TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

Functionality is short-lived without security

Securing tomorrow's Connected, Intelligent, and Autonomous Vehicular Ecosystem

Akwasi Adu-Kyere

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. F OSA – TOM. 77 | TECHNICA – INFORMATICA | TURKU 2026

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

FUNCTIONALITY IS SHORT-LIVED WITHOUT SECURITY

Securing tomorrow's Connected, Intelligent, and Autonomous Vehicular Ecosystem

Akwasi Adu-Kyere

TURUN YLIOPISTON JULKAISUJA ANNALES UNIVERSITATIS TURKUENSIS
SARJA SER. F OSA TOM. 77 | TECHNICA INFORMATICA | TURKU 2026

University of Turku

Faculty of Technology
Department of Computing
Information and Communication Technology
Doctoral Programme in Technology

Supervised by

Adjunct Professor, Ethiopia Nigussie
University of Turku

Professor, Jouni Isoaho
University of Turku

Reviewed by

Professor, Juha Röning
University of Oulu

Associate Professor, Gaurav Choudhary
Technical University of Denmark

Opponent

Professor, Vasileios Gkioulos
Norwegian University of Science and Technology

ISBN 978-952-02-0547-8 (PRINT)
ISBN 978-952-02-0548-5 (PDF)
ISSN 2736-9390 (PRINT)
ISSN 2736-9684 (ONLINE)
Painosalama oy, Turku, Finland, 2026

To my Father and Mother

UNIVERSITY OF TURKU
Faculty of Technology
Department of Computing
Information and Communication Technology
ADU-KYERE, AKWASI: Functionality is Short-lived without Security: Securing tomorrow's Connected, Intelligent, and Autonomous Vehicular Ecosystem
Doctoral dissertation, 88 pp.
Doctoral Programme in Technology
September 2026

ABSTRACT

Vehicles are increasingly becoming fully functional complex computers on wheels, primarily driven by automation as social "things" while presenting various security challenges. As cyber-physical objects, the current vision of transitioning to fully connected, intelligent, and autonomous vehicles has introduced unique requirements that emphasize the importance of security dynamism, adaptiveness, self-awareness, context-awareness, and continuity. However, current security solutions are static and inadequate in addressing all these unique requirements. As functionality without the appropriate security measures is short-lived from a security perspective, which are influenced and shaped by its interactions security-wise.

This dissertation develops a dynamic security architecture and investigates the impact of interaction resulting from security dependencies, inter-dependencies, and relationality within the vehicular ecosystem. In addition, it presents the findings from a series of experiments conducted with a real-world heavy-duty truck, exploring the role of existing quantum technologies in the next generation of vehicular security and their integration. This includes the creation of a framework based on relational dependency chains and a self-aware system-level architectural design. Furthermore, this research enhances existing security measures and advances the state-of-the-art by examining, assessing, and demonstrating the significance of vehicular security while addressing the complexities within the vehicular ecosystem.

The first contribution demonstrates decision-making and security impacts in multi-sensing environments, particularly focusing on object tracking for heavy-duty trucks with extended trailer dynamics in urban traffic scenarios. Intrusion Detection System/Intrusion Prevention System (IDS/IPS) is developed and tested in real-time with a custom in-vehicle design within a multi-sensing environment. The second contribution introduces Seaming Security Dependency-Chains (SSDC), which arise from security interconnectedness by examining the individual and collective effects of dependency, interdependency, and relationality within vehicular security and its ecosystem. The third contribution presents a security architecture featuring a hierarchical self-aware security that effectively establishes accountability at the system-level through an integrated security-specific black-box. The final contribution is twofold: first, it includes a proof-of-concept regarding the necessity of quantum key distribution for securing in-vehicle and external transactions and communications. Second, it proposes a Quantum Vehicular Ecosystem (QVE), exploring quantum-like modeling

in the vehicular domain from the perspectives of design, implementation, simulation, impact, and society's role in service and security demands.

It is evident that increasingly intricate in-vehicle security systems with their complex hybrid architectures and automation-driven features are here to stay. As a result, security seams and chains will continue to develop, each evolving in response to specific domains and advancements. Therefore, without dynamic, adaptive, and self-aware security solutions that extend beyond in-vehicle interactions and communications, the benefits of dynamic features and functionalities will not align with the vision of intelligent mobility. The contributions of this dissertation can be applied beyond the vehicular ecosystem and its networks. Over time, more security seams and chains will be established due to increasing dependencies and inter-dependencies.

KEYWORDS: *Security, Cybersecurity, Vehicular Security, Autonomous vehicles, Connected vehicles, Intelligent vehicles, Security architecture, Self-Aware architecture, Security accountability, Security Analysis, in-vehicle Security, In-vehicle IDS/IPS, Security-chains, Security-seams, Seams, Dependencies, Dependency-chains, Inter-dependency, Relationality-chains, Eavesdropper detection, Quantum key distribution, Quantum mechanics laws, Right-Turn, multi-sensing, Trailer dynamics, Object-tracking, Freighting trucks, Heavy-duty trucks*

TURUN YLIOPISTO
Teknillinen tiedekunta
Tietotekniikan laitos
Tietotekniikka
ADU-KYERE, AKWASI: Functionality is Short-lived without Security: Securing tomorrow's Connected, Intelligent, and Autonomous Vehicular Ecosystem
Väitöskirja, 88 s.
Teknologian tohtoriohjelma
Syyskuu 2026

TIIVISTELMÄ

Ajoneuvoista on tulossa kattavilla toiminnoilla varustettuja, monimutkaisia renkailla liikkuvia tietokoneita, jotka ovat pääasiassa automaattisesti ohjattuja sosiaalisia "esineitä" ja joihin liittyy erilaisia tietoturvahaasteita. Koska ne ovat kyberfyysisiä kohteita, nykyinen visio siirtymästä täysin yhdistettyihin, älykkäisiin ja itsenäisiin ajoneuvoihin on tuonut mukanaan erityisiä vaatimuksia, joiden mukaisesti tietoturvan olisi oltava dynaamista, mukautuvaa, itsetietoista, kontekstisidonnaista ja jatkuvaa. Nykyiset tietoturvaratkaisut ovat kuitenkin staattisia, eikä niiden pohjalta kyetä vielä vastaamaan kaikkiin näihin erityisiin vaatimuksiin. Toiminnallisuudet ilman asianmukaisia turvatoimia ovat tietoturvan kannalta lyhytikäisiä, ja niihin vaikuttavat ja niitä muokkaavat tietoturvaan liittyvät vuorovaikutukset. Väitöskirjassa kehitetään dynaamista turvallisuusarkkitehtuuria ja tutkitaan tietoturvariippuvuuksien, keskinäisten riippuvuuksien ja suhteellisuuden aiheuttamien vuorovaikutusten vaikutuksia ajoneuvoekosysteemissä. Lisäksi siinä esitellään raskailla kuorma-autoilla tehtyjen kokeiden tulokset ja tutkitaan olemassa olevien kvanttiteknologioiden roolia seuraavan sukupolven ajoneuvoturvallisuudessa ja niiden integrointia. Tähän kuuluu suhteellisiin riippuvuusketjuihin ja itsetietoiseen järjestelmätason arkkitehtuurisuunnitteluun perustuvan viitekehyksen luominen. Lisäksi tämä tutkimus parantaa olemassa olevia tietoturvatoimenpiteitä ja vie uusinta tekniikkaa eteenpäin tutkimalla, arvioimalla ja esittelemällä ajoneuvojen turvallisuuden merkitystä sekä käsittelemällä ajoneuvojen ekosysteemin monimutkaisuuksia. Ensimmäisessä osassa havainnollistetaan päätöksenteon ja turvallisuuden vaikutuksia monianturisissa ympäristöissä, erityisesti perävaunulla varustettujen raskaiden kuorma-autojen kohteiden seurannassa kaupunkiliikenneskenaarioissa. Tutkimuksessa kehitetään ja testataan reaaliajassa tunkeilijan havaitsemisjärjestelmää/tunkeutumisenestojärjestelmää (IDS/IPS) räätälöidyllä ajoneuvon sisäisellä mallilla monianturisessa ympäristössä. Toisessa osassa esitellään saumauksen tietoturvan riippuvuusketjuja (Seaming Security Dependency-Chains, SSDC), jotka perustuvat tietoturvan keskinäisiin yhteyksiin, ja tarkastellaan riippuvuuksien, keskinäisten riippuvuuksien ja suhteellisuuden yksilöllisiä ja kollektiivisia vaikutuksia ajoneuvon tietoturvaan ja sen ekosysteemiin. Kolmannessa osassa esitellään tietoturva-arkkitehtuuri, jossa on hierarkkinen itsetietoinen tietoturva. Se parantaa tehokkaasti järjestelmätason vastuullisuutta integroidun tietoturvaan keskittyvän mustan laatikon avulla. Viimeinen osa on jaettu kahteen: ensiksi siinä esitellään soveltuvuusselvitys kvanttiavainten jakelun tarpeellisuudesta ajoneuvon sisäisten ja ulkoisten tapahtumien sekä viestinnän turvaamiseksi. Toiseksi siinä esitellään Quan-

tum Vehicular Ecosystem (QVE) -ekosysteemiä ja tutkitaan ajoneuvojen kvanttityyppistä mallinnusta suunnittelun, toteutuksen, simuloinnin ja vaikuttavuuden näkökulmista sekä yhteiskunnan vaikutuksia palvelu- ja turvallisuusvaatimuksiin. On selvää, että yhä monimutkaisemmat ajoneuvojen tietoturvajärjestelmät ovat tulleet jäädäkseen monimutkaisine hybridiarkkitehtuureineen ja automatisoituine toimintoineen. Näin ollen myös tietoturvasaumat ja -ketjut kehittyvät edelleen yksittäisten käyttökohteiden ja edistysaskelten innoittamina. Ilman dynaamisia, mukautuvia ja itseohjautuvia tietoturvaratkaisuja, jotka ulottuvat myös ajoneuvon sisäisen vuorovaikutuksen ja viestinnän ulkopuolelle, dynaamisten ominaisuuksien ja toiminnallisuuksien hyödyt eivät kuitenkaan vastaa älykkään liikkuvuuden visiota. Tämän väitöskirjan sisältöä voidaan soveltaa myös ajoneuvoekosysteemin ja sen verkkojen ulkopuolella. Ajan myötä tietoturvasaumojen ja -ketjujen määrä tulee lisääntymään riippuvuuksien ja keskinäisten riippuvuuksien lisääntyessä.

AVAINSANAT: Tietoturva, kyberturvallisuus, ajoneuvojen tietoturva, autonomiset ajoneuvot, yhdistetyt ajoneuvot, älykkäät ajoneuvot, turvallisuusarkkitehtuuri, itsetietoinen arkkitehtuuri, tietoturvan vastuullisuus, tietoturva-analyysi, ajoneuvojen sisäinen tietoturva, ajoneuvojen IDS/IPS, tietoturvaketjut, tietoturvasaumat, saumat, riippuvuudet, riippuvuusketjut, keskinäinen riippuvuus, suhteellisuusketjut, salakuuntelun tunnistus, kvanttiavainten jakelu, kvanttimekaniikan lait, oikealle kääntyminen, monianturisuus, perävaunudynamiikka, kohteen seuranta, kuorma-autot, raskaat kuorma-autot

Acknowledgements

First and foremost, I would like to express my heartfelt gratitude to Almighty God for the protection, grace, and wisdom bestowed upon me. I am therefore sincerely thankful to Adjunct Professor Ethiopia Nigussie and Professor Jouni Isoaho as my research supervisors for their guidance, support, and mentorship, as well as the opportunities provided by the University of Turku. I would also like to extend my appreciation to Professor Juha Röning from the University of Oulu and Associate Professor Gaurav Choudhary from the Technical University of Denmark for serving as my reviewers, and to Professor Vasileios Gkioulos from the Norwegian University of Science and Technology for acting as my opponent.

My thanks go to the University of Turku for supporting my research through employment, to the Finnish Cultural Foundation for a research grant, to the University of Turku Graduate School (UTUGS) for research funding, and to the PRYSTINE project for supplying research resources and experimental equipment. I would also like to thank LanguageWire Oy for their assistance in translating the abstract into Finnish.

Finally, my father, John Nana Otchere, for his wisdom and motivational support throughout my education, and Margret Otchere. My siblings and Samuel Akpe for not only showing their interest in my well-being, but also being there when things got tough.

7th January, 2026
Akwasi Adu-Kyere

Table of Contents

Abbreviations

ACSP Automotive Cybersecurity Protection

ADAS Advanced Driver Assistance Systems

AI Artificial Intelligence

AI artificial intelligence

API Application Programming Interface

CAM Cooperative Awareness Messaging

CAN-FDs Flexible Data-Rate

CAN Controller Area Network

CIAE Connected, Intelligent, and Autonomous Ecosystems

CIAVs connected, Intelligent, and Autonomous Vehicles

CIA Confidentiality, Integrity, Availability

CPS Cyber-Physical Systems

CSEF Cybersecurity Evaluation Framework

CSSMS Cybersecurity and Safety Management System

CVs Connected Vehicles

DBIR Verizon Data Breach Investigation Report

DCP Data Control Plane

DDoS Distributed Denial-of-Service

DNS Domain Name System

DoS Denial-of-Service

ECUs Electronic Control Unit

EIR External Infrastructural Resources

FLcM Full Life-cycle Management

GPS Global Positioning System

GSM Global System for Mobile

H2M Human-to-Machine

IDS/IPS intrusion detection system and intrusion prevention system

IoT Internet of Things

KG$_b$ Key Generator

LiDAR Light Detection and Ranging

LIN Local Interconnect Network

LSTM Bidirectional Long Short-term Memory

LTE Long-Term Evolution

M2M Machine-to-Machine

MiTM Man-in-The-Middle

ML Machine Learning

NIST National Institute of Standards and Technology

OEM Original Equipment Manufacture

OTA Over-the-Air

PE/D$_b$ Photon-Base Encoder/Decoder

PG$_b$ Photon-Base Generator

PQC Post-Quantum Cryptography

PRYSTINE Programmable Systems for Intelligence in Automobiles

QaaS Quantum as a Service

QB Quantum Block

QKD Quantum Key Distribution

QVE Quantum Vehicular Ecosystem

RSA Rivest-Shamir-Adleman

RSUs Roadside Units

SAE Society of Automotive Engineers

SAS Self-Awareness Security

SDVs Software-Defined Vehicles

SHDP Software and Hardware Data Pipeline

SoSDD Security-Oriented Software-Defined Deployment

SSDC Seaming Security Dependency-Chains

SSH Secure Shell

TEE Trusted Execution Environment

TLS Transport Layer Security

V2C Vehicle-to-Compute

V2I Vehicle-to-Internet(V2I)

V2P Vehicle-to-Pedestrian

V2RI Vehicle-to-Road Infrastructure

V2T Vehicle-to-Things

V2V Vehicle-to-Vehicle

V2X Vehicle-to-Everything

VANET Vehicular ad hoc Network

List of Original Publications

Original Publication List:

I **Akwasi Adu-Kyere**, Ethiopia Nigussie, and Jouni Isoaho. Seaming Security Dependency-Chains (SSDC) in the Vehicular Ecosystem. Status: Manuscript.

II **Akwasi Adu-Kyere**, Ethiopia Nigussie, and Jouni Isoaho: Quantum vehicular ecosystem: Analysis of emerging applications and security implications. World Congress in Computer Science, Computer Engineering & Applied Computing, Springer, 2025; status: Accepted and to be published in conference proceedings.

III **Akwasi Adu-Kyere**, Ethiopia Nigussie, and Jouni Isoaho. Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design. Procedia Computer Science, 2024, 238: 175-183.

IV **Akwasi Adu-Kyere**, Ethiopia Nigussie, Jouni Isoaho, Jukka Ronkainen, and Arto Kyytinen. Validating multi-sensor object tracking in Heavy-Duty Trucks with extended trailer dynamics for road traffic situations. Procedia Computer Science, 2024, 238: 167-174.

V **Akwasi Adu-Kyere**, Ethiopia Nigussie, and Jouni Isoaho. Self-Aware Cybersecurity Architecture for Autonomous Vehicles: Security through System-Level Accountability; Sensors. 2023; 23(21):8817

VI **Akwasi Adu-Kyere**, Ethiopia Nigussie, and Jouni Isoaho: Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3. Sensors. 2022; 22(16): 6284.

1 Introduction

The global economy has used, relied on, and created additional opportunities through technological advancements over the past decades. Transportation has been a key driver of these advancements, with several variations of vehicular ecosystems catalyzing the journey toward leveraging today's technological advancements in the vehicular realm. Particularly as vehicles increasingly integrate into Cyber-Physical Systems (CPS). This potential increases as we progress beyond level 3 in the levels of the Society of Automotive Engineers (SAE). Thus, vehicles will evolve into complex computers on wheels [1], fully functional, with the ability to foster advanced fleet management [2], in-vehicle compute with advanced driver assistance routines, and routing optimizations. In addition to vehicular telemetry and bidirectional data and information exchange [3]. Such vehicular capabilities will extend to network traffic transactions handled via embedded systems [4]. Hence, exhibiting characteristics and properties through functionalities that make these vehicles with such capabilities social "things." Coupled with collections of evolving sensor platforms for in-vehicle and their periphery, enormous amounts of data will be generated by these vehicles. Comparatively, serving as intelligent mobile objects and virtual data sources on wheels [2]. The seamless communication with each other, resource infrastructures (in-vehicle and external), the Internet of Things (IoT), intelligent devices, and other domains within vehicle-to-everything (V2X) is further evidenced. The emergence of machine learning and computing capabilities accelerates the advancement of transportation in terms of potential and possibilities.

Society and the general public enjoy an array of benefits, including the proliferation of hardware sensors for driving assistants [5] and their software associates [6]. In particular, advanced driver assistance systems (ADAS) have substantially improved pedestrian and road safety with vehicle sensor deployments such as radars, LiDAR , and cameras. These ADAS-capable vehicles utilize machine learning [7] attributes, catalyzing assistive hardware and software sensing. With confidence in the identification and detection of stationary and moving objects, including pedestrians, most passenger vehicles have gained advantages from these assistive functionalities and situational awareness in recent years. These hardware driving assistant sensors provide accurate data delivery with efficient and precise back-end ADAS executions. Alleviating the split-second decision-making accountability onus in traffic situations that are beyond the control of drivers and commuters. In terms of responsiveness,

dynamism, and consistency, more research has also demonstrated that these benefits can be extended to freight trucks for logistic purposes in terms of trailer dynamics on right turns [8] in urban environments. Figure 1 based on [8] shows a combined 76-ton heavy-duty truck and its extended trailer in a traffic scenario, of length 25 meters and in some cases beyond. The ADAS-capable truck in this scenario exemplifies the benefits of multi-sensing in an intricate and diverse environmental element, including their dynamic factors [9], driver perception, and collision [10]. This emphasizes how fast, intelligent, and accurate decision-making is needed in such traffic scenarios where the driver has a blind spot during a right turn.

(a) Approaching a Right-Turn **(b)** Making a Right-Turn

Figure 1. Simulation of a Right-Turn scenario under a controlled environment with side mirrors visibility

1.1 Background

Trends in automotive security-related issues have emerged as part of the current progress toward the goal of a fully connected, intelligent, and autonomous regime and are here to stay. These trends are corroborated by the research community, as authors such as [11] take the perspective of safety and acceptance, [12] from risk mitigation and user protection, and [13] from cybersecurity threats and assessments. As such, ensuring vehicle security characteristics, traits, and properties is a critical challenge that demands our utmost attention. Although Trusted Execution Environments (TEEs) [14], Access control [15], Tamper-proofing, White-listing, and others [16] security measures exist in vehicles, there are still critical security challenges that need to be resolved. Security is essential to the basic existence of fully connected, intelligent, and autonomous vehicles. These challenges are evident in the vehicle security frameworks and concepts proposed by various researchers. For example, [17] on the secure authentication and attestation scheme, [18] on deep learning-centered intrusion detection, and [19] discussion on the functional safety of embedded automotive systems. Their roles are crucial in influencing and shaping associated technologies within the corresponding ecosystems. Therefore, the

challenges of vehicular security gradually and persistently impact the automotive landscape as an influential factor. As a result, such associations through relational functionalities exhibit cascading security complexities. Thus, there has never been a time for researchers to explore this realm, as there is still anticipation and expectation that artificial intelligence (AI) will play a vital role.

Amid these contributions from the research community, emphasis of this research is placed on automobile security challenges such as dynamism, adaptiveness, dependencies, and self-awareness, which emerge as a research gap. Factoring complexities and challenges [20; 21] fostered by increasingly complex and vital groups of heterogeneous hardware and software, and platforms [22]. Thus, with the belief that the resolutions in the fluidity of technological transitions in automotive security and life-cycle management, in particular, should consider an accompanying set of security requirements. Requirements that are systematically entrenched in the exhibition of security self-management. From this dissertation's point, vehicles geared towards SAE level 5 must display self-configuration and self-adoption, coherent error recovery, and survivability security characteristics and properties. Underscoring the importance of dynamic, adaptive, and self-aware in-vehicle security solutions and measures in this transition to address the following challenges in the vehicular ecosystem and its networks.

- Lack of a dynamic, adaptive, self-aware, and context-aware security solution for the in-vehicle infrastructure: dynamic interactions with a dynamic environment create fluctuating security characteristics, parameters, and requirements, compounded by legacy and external devices and infrastructures.

- Lack of systematic method for analyzing the impact and influence of security dependency-chains, inter-dependency-chains, and relationality-chains: The interconnectedness of interactions that create intricate and complex interwoven security layers of in-vehicle to external communications. Research into this area in the context of vehicular security is lacking in the vehicular ecosystem.

1.2 Aim and Objectives

The work aims to strengthen the security of the connected, intelligent, and autonomous vehicular ecosystem. Following recent projections suggesting an estimated 115 million increase of connected vehicles (CVs) from the year 2025 [23] and beyond. The attack frequency on regular vehicles endured a staggering increase of 225% between 2021 and 2024 [24]. A significant portion of the 225% spike in attacks is proportionally distributed, with 84.5% from remotely conducted attacks [25] and the rest through physical means. As the vehicle-to-everything (V2X) philosophy gains strength, security interactions contribute to these attack causes and effects.

Because vehicular networks are based on complex interactions between vehicles, intelligent gadgets, the Internet of Things (IoT), people, and external infrastructures in an in-vehicle or external context. There is also the anticipation that artificial intelligence (AI) will impact the landscape of vehicular security threats as well as new security solutions.

Hence, the dissertation's objectives are as follows:

1. To propose a security architecture that effectively establishes accountability at the system-level.

2. To design, implement, and simulate a communication architecture model that utilizes quantum cryptography to facilitate secure communication.

3. To examine security interconnectedness between security measures and propose a method to capture its complex interactions within the context of a connected, intelligent, and autonomous ecosystem.

This research would comprise the design of a self-aware system-level architecture and its development, with the study of security relations within its security interactions and their associated chains. The work also improves current security measures and advances the state-of-the-art by examining, assessing, and showcasing the significance of vehicular cybersecurity while highlighting security intricacies within the vehicular ecosystem. It is clear that vehicles are gradually turning into complex computers on wheels and are predominantly going to be driven by automation. As such, this will affect and influence vehicular life-cycle management, continuity support, and the effects of technological advancements on security sustenance in the amid of quantum technologies, Artificial Intelligence, and machine learning on vehicular security postures. Therefore, this dissertation advocates that without having dynamic, adaptive, context-aware, and self-aware security solutions that extend beyond in-vehicle interactions and communications, the impact of dynamic features and functionalities does not align with the vision of intelligent mobility.

1.3 Research Questions

RQ1: What are the security challenges and problems in the move towards a fully connected, intelligent, and autonomous vehicular regime?

With an undeniable vision for the transition towards fully connected, intelligent, and autonomous vehicles, research, study, and interest in this progression continue to grow. In particular, the evolution and systematic evaluation of the security challenges and problems associated with this change will be of interest in the coming

years. To this end, the goal is to address this question by examining the parameters and attributes of in-vehicular systems' security. Hence, directing the investigation towards security measures and compliance, adaptive and real-time dynamism, and security threat mitigation in the current vehicular context.

RQ2: What are the components of a security system and their architectural requirements for securing the next generations of fully connected, intelligent, and autonomous vehicles and their ecosystem?

The extended role, responsibilities, and operations of autonomous vehicles in vehicle-to-everything communications and interactions are expected to evolve with each climb of autonomousness. For that matter, there would be much emphasis on the security complexities and requirements that this form of transition toward a fully connected, intelligent, and autonomous vehicle would introduce. As such, the roles within the security architecture realm are significant. Therefore, this question intends to facilitate an investigation that reveals these components and their unique security roles.

RQ3: How do the potential and limitations of quantum-based security influence future vehicular ecosystems and their security?

Cryptography has demonstrated its relevance in several use cases, including the vehicular ecosystem. In-vehicle and external communications and transactions have relied on encryption and decryption through various means to securely ensure privacy, data confidentiality, integrity, availability (CIA), authenticity, and non-repudiation in its protection. As quantum computing and informatics expand, the research community is increasingly interested in the security relationship between quantum systems and vehicular security. Thus, this work aims to answer this question, factoring considerations from research question **RQ2**, by investigating quantum-based security solutions for vehicles and their ecosystems.

RQ4: How to systematically analyze the security dynamics and interactions in a vehicular ecosystem?

As far as technological advancements go, the security posture, maturation, and evolution of devices, systems, and infrastructures, or groups of security-related entities, have been subjected to or tied to the security and expansion of other devices, systems, infrastructures, etc. This has been possible because of the security interactions among devices, systems, and infrastructures within ecosystems. In addressing these, the research community has been investigating security requirements and their attack-to-defense strategies. Other factors in the security situation and scope in the

vehicular environment that provide a comprehensive understanding of the vehicular cybersecurity and its related systems have also seen relative interest. However, the impact and influence of security interactions on attacks, data protection, and privacy are inadequately addressed in relation to the causalities of interacting components. Therefore, the focus and hope in answering this question is that this security interactions analysis leads this investigation to a different perspective, advantageous to shaping and influencing connections, and the impact these security interactions have on the development and deployment of technological solutions.

1.4 Research Contributions

This section presents the contributions of this dissertation to reflect the compiled publications, aim, and objectives. They are grouped into paragraphs to illustrate each contribution based on the research, experiments, simulations, and all other activities performed.

The first contribution demonstrated the **societal benefits** of multi-sensing and securing the heavy-duty freight trucks towing an extended trailer in a combined length of 25 meters and weight of 76 tons and beyond in an urban traffic environment. The intricate and diverse elements, including dynamic environmental factors, driver perception, and transportation accidents which emphasize the importance of decision-making and security impact.

The second contribution proposed a **security architecture** as it was evident that there is a need for appropriate security measures that match the dynamic nature of the vehicular security landscape through **a hierarchical self-aware security that effectively establishes accountability at the system-level**. This further illustrates why such a proposed security architecture is relevant to connected, intelligent, and autonomous vehicles and their sub-components, intricate architecture, algorithms, and the integration of a security-specific black-box.

The third contribution provided a **proof-of-concept** on the necessity of security in-vehicle and external security transactions and communications with quantum key distribution, and the vision of a **quantum vehicular ecosystem (QVE)**. Exploring quantum-like modeling for vehicular security from the perspective of a quantum vehicular ecosystem. **Designed, implemented, and simulated** a communication architecture model that utilizes quantum cryptography to facilitate secure communication via the BB84 protocol in Python.

The fourth contribution provided an overview of **security interconnectedness** in the connected, intelligent, and autonomous ecosystem by examining the individual and collective effects of dependency, interdependency, and relationality in the context of vehicular security and its ecosystem. Leading to the proposal of **the concept of Seaming Security Dependency-Chains (SSDC).**

1.5 Thesis Organization

The subsequent structure of the thesis is grouped under four parts, signaling transitions and themes to facilitate systematic cohesion. Each part presents an overall focus that embodies the theories and concepts discussed. The conclusion then follows to summarize the whole research work, with the parts illustrated as follows:

Part I: Research Method and Problem Introduction - Two chapters in this part cover materials and research methods, and the theoretical foundations of this dissertation.

- **Chapter 2: Materials and Research Methods -** This Chapter presents the compilation of materials and research methodologies associated with the dissertation. The components of the compiled publications are systematically explained with a detailed breakdown of each aspect that contributed to the completion of the work.

- **Chapter 3: Theoretical Foundations -** This chapter and its subsequent sections offer a theoretical foundation for the vehicular security challenges the dissertation intends to address.

Part II: Dissertation Results and Outcomes - This part presents the findings of the dissertation and its associated discussions.

- **Chapter 4: Results and Findings -** This chapter delves deep and addresses the findings and results from the investigations, experiments, simulations, and real-world tests that the dissertation undertook. Three crucial results presented covered self-awareness security architecture, the role of quantum in a vehicular ecosystem, and the effects, impact, and influence of the two, as seaming security dependency-chains.
  - **Section 4.1: Self-Awareness Security with System-Level Accountability -** Presents a hierarchical vehicular security architecture that focuses on security accountability at the system-level, emphasizing real-time security monitoring, analysis, fallback mechanisms, and virtual operation center operations.
  - **Section 4.2: The Role of Quantum in the Vehicular Ecosystem -** The findings in this section present the trajectory, trends, and technological advancements interplay between quantum technologies and automotive cybersecurity from a proposed quantum vehicular ecosystem.
  - **Section 4.3: Seaming Security Dependency-Chains -** The section presents results and findings that relate to complex and intricate

security dependencies, inter-dependencies, and relationalities pertaining to their influence, impact, and role in shaping in-vehicle and external security interactions and their postures.

Part III: Discussion - As a summarization chapter with the intention of bringing to focus the impact of the dissertation results, it consists of a single chapter that summarizes the compiled works in terms of beneficial impacts and influences.

- **Chapter 5: Discussion -** This chapter presents a summary of the dissertation perspective from all presented findings, arguments, and concepts in three significant sections: Theoretical implications, practical implications, and reliability and validity. The discussions under these sections provide additional perspectives related to the impact of the dissertation outcomes.

Part IV: Concluding Remarks - As the final part, it consists of two chapters concluding the dissertation with publication summaries of the compiled works and the concluding chapter of this work.

- **Chapter 6: Publication Summary and Author Contributions -** This chapter presents a summary of published articles that are included in this dissertation, with a detailed account and breakdown of the author's contributions in each research work.

- **Chapter 7: Conclusions -** This is the concluding chapter that summarizes all the findings and results with the rationales and constructs addressed through the research question answering.

2 Materials and Research Methods

Figure 2 represents the visual compilation workflow in this dissertation, on which the methodology is based. It starts with the experiments and implementations tied to an EU-funded project with the name ”Programmable Systems for Intelligence in Automobiles” (PRYSTINE). What follows is the data collection phase, while the subsequent parts of Figure 2 show a distributed account of each compilation within this dissertation. In the following sections, each of the research methods associated with each account will be explained in detail, starting with the Literature review. It is the starting point of this research, delving into the state-of-the-art of security solutions, concepts, and best practices. Practical design methods in the literature review were also examined to assess several factors in achieving the optimal security design and implementation adopted in this work. Three experimental designs consisting of multi-sensing in a traffic scenario and its impact on security interaction [8], which is extended by using an intrusion detection system and intrusion prevention system(IDS/IPS) implementation for real-time dynamic security evaluation [26] were conducted. The last experiment is a simulation that covered quantum key distribution [27] from the perspective of a quantum vehicular ecosystem and its networks. The experiments and simulations conducted used real-life testing scenarios that cover sandbox, on-road, and iterative simulation in each implementation process, except the quantum one. In all experiment scenarios, algorithms, custom scripts, and applications were developed to fulfill data collection and intended results, which were tested and verified using hardware sensors and network traffic flow devices in a real-world implementation in a Heavy-Duty truck. The experimental setup involving the hardware resources was aided by the use of a custom compute unit configured and housed in a Renault T520 freight truck with carefully placed multi-sensor arrays. Custom script and open-source libraries implemented in the experiment testbed also helped to interpret, transform, and visualize the raw data, along with proprietary applications from in-use hardware. The majority of the research-specific code was written in Python 3. A detailed and systematic breakdown of the research methodology is given below.

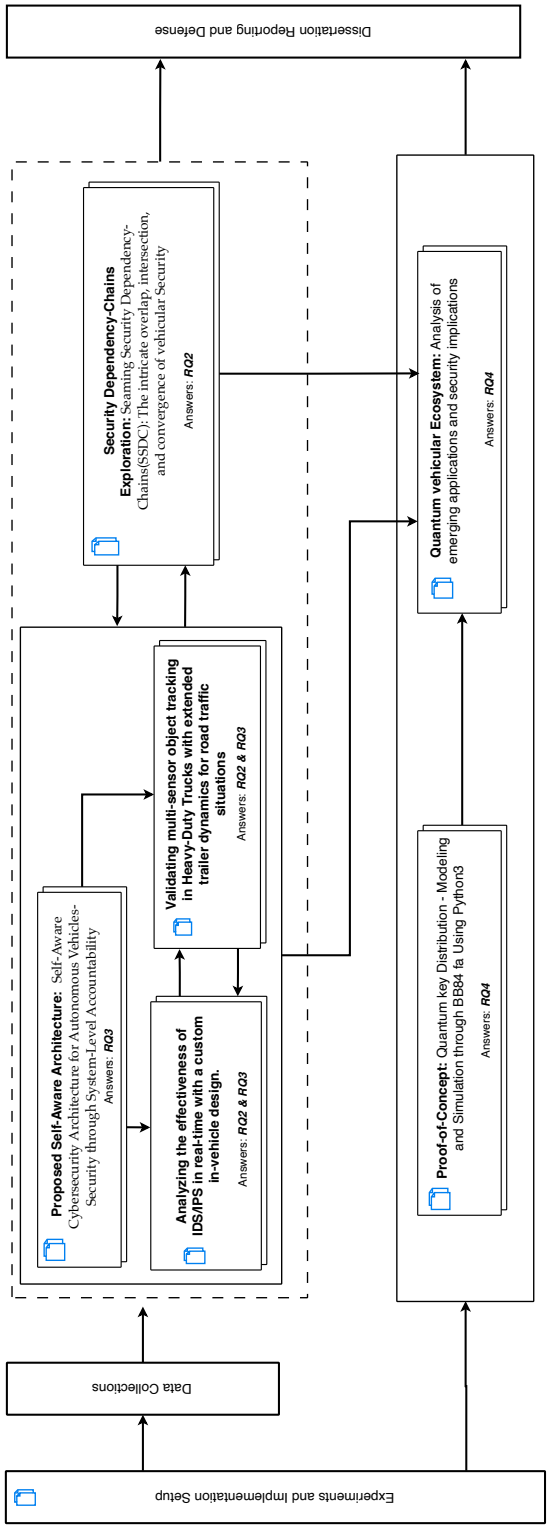


Figure 2. Illustration of Research cohesion and integration of sections and parts.

2.1 Literature Review Method

The review covered data, experiments, scientific methodologies, practical implementations in the literature, and followed trends and projections within the scope of the research.

In the case of the self-aware cybersecurity architecture for autonomous vehicles: a systematic overview and exploration of security dynamism, self-awareness, and adaptiveness in the vehicular ecosystem was conducted. The exploration further considered how and the impact of security in this context, in a holistic infrastructure with security accountability at the system-level. The literature review on the existing state-of-the-art was also extended by a self-aware architecture that addresses security complexities and challenges concerning dynamism, adaptiveness, and self-awareness.

For the quantum aspect, the review focused on the future trend in the transition to a fully autonomous vehicle as "Things" and their diversification of role, application, and responsibility. In addition to the researched security applicability and deployment in the literature review stage, the research on the appropriate and chosen security implementation needed to re-stand technological advancements. Accounting for mathematical and computational cryptographic attack complexities and intricacies.

In terms of the multi-sensing in a traffic scenario and its security interactional impact, and its extension by using IDS/IPS implementation, the initial review and experiment had already been covered by the Self-Aware Cybersecurity Architecture for Autonomous Vehicles. Therefore, subsequent literature reviews on this aspect delved more into the vehicular multi-sensing implementations and their security challenges, to support the actual components of the architecture, particularly with the analysis process controller and the related decision controller. This particular method of deep dive allowed and generated further resources that were useful in the later stages of the research.

The last literature review occurred when the first three were completed. Further unique observations had been made, and questions arose on the security dependencies, inter-dependencies, and relationalities observed within the security interactions and their characteristics and properties. Thus, an extensive review on complex and intricate security interactions was conducted, dynamically evolved, and how they contribute to the overall security posture in the three literature reviews.

2.2 Developing Algorithms, Protocols, and Architectures

The development of algorithms, protocols, and architectures began, following best practices to consider resource heterogeneity and complex transactional relationships between components based on the research logic. Laid out in the dissertation with respect to the aim, objectives, and research questions.

In the case of the self-aware cybersecurity architecture for autonomous vehicles, the sub-components of the architecture were developed. Each of the main modules, including analysis, fallback, fail-over, and report/support, was designed as a process module-based controller. Their associating algorithms were also developed as decision module-based controllers, which included system incident, criticality, and resolvability with the integration of a security-specific black-box. Decision controllers and process controllers are used to achieve a dynamic, adaptive, and self-aware in-vehicle security infrastructure.

For the quantum aspect, the methodology centered on developed algorithms and protocol architecture geared towards using the laws of quantum mechanics to generate a secure key by manipulating light properties for secure end-to-end communication for vehicular applications. This methodology used a proof-of-concept via a simulated model relying on the BB84 protocol. Two scenarios were designed, developed, and simulated for communicating parties to simulate the interception-resend attack model from a theoretical and practical perspective. A quantum channel is used in this case for polarized photon transmission after a pre-agreed configuration over a classical channel with parameters. The data from the algorithm used in the simulations were then interpreted. The method is also extended to cover vehicular quantum applications and quantum-like approaches.

In terms of the multi-sensing in a traffic scenario and its security interactional impact, the method used relied on a custom software environment that was set up to accommodate the developed algorithms and custom scripts. The same environment was also used in its extension with the use of an IDS/IPS implementation that stemmed from the self-aware cybersecurity architecture. With multi-sensor object tracking emphasizing trailer dynamics, outcomes from the experiments were used to evaluate and validate the extended trailer dynamics in road traffic situations. Back-end parameters and characteristics were also used as a method and a means to study security interactional influence and decision-making strategies concerning overall security posture, pedestrians, and other road commuter dynamics. However, the IDS/IPS aspect of the methodology incorporated the resources behind the main gateway as the primary ingress and egress, fully aware of all traffic transactions, including plug-and-play streams, external resource requests, and system updates, because vehicles are traditionally composed of modular compute units.

This developmental process, as a result of the first three above, involved the method of capturing security interactions of dependencies, inter-dependencies, and relationalities intersecting, overlapping, and converging within a dynamic security interaction and context. This method is predicated on developing a principle that assesses the impact of these dynamic security interactions and interconnectedness from the individual and collective perspectives in the vehicular ecosystem using case studies. The case studies drew from four scenarios: vehicle-to-vehicle, vehicle-to-pedestrians, vehicle-to-roadside units, and vehicle-to-compute infrastructures, to re-

veal the significant role of security-chains and security-seams.

2.3 Data Collection and Interpretation

Experimental data is collected and described according to the research workflow in Figure 2, with further preparation and processing guided by the security architectural design and algorithms developed and driven by the concepts, principles, and framework proposed.

The data collection scope covered real-life implementation strategies, physical on-site testing, calibration, and on-road testing combined with remote testing. The raw data were prepared and visualized using language-specific coding libraries such as OpenCV, hardware-specific APIs, and the rest were predominantly available through the Anaconda library. Data preparation was also tied to the applications and custom scripts used, along with open-source libraries. A detailed flow of data collection to the interpretation phase is illustrated in Figure 3, while the additional information is offered via Table 1.

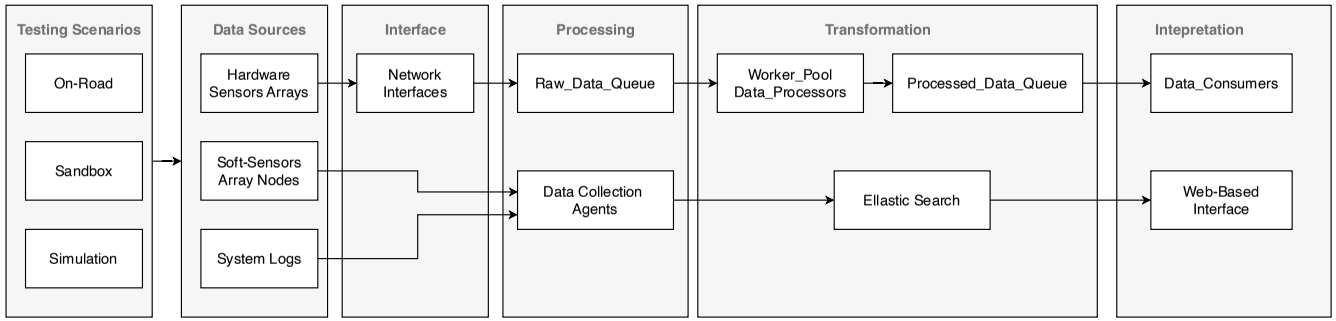


Figure 3. Data collection and preparation phases in the dissertation

Soft-Sensor Data Sources	File Beat	Audit Beat	Metric Beat	System Beat	Hardware-Sensor Data Sources	CAN Interface	Ethernet Interface	Collection Phases	Transformation
Integrity Checks	✓	✓	✓		Basler Camera		✓	OpenCV API Scripts	✓
System Audit Checks		✓			Mobileye 6	✓			
Configuration Checks	✓	✓			Ouster 32 Lines Lidar		✓	Ouster API Script	✓
Sysctl Ckecks	✓	✓			Continental Radar	✓		Continental API Script	✓
Firewall Rule Ckecks	✓	✓			Hokuyo Lidar		✓	Hokuyo API Scripts	✓
System Health			✓		Brigade Radar	✓		Brigade API Script	✓
System Logs				✓					

Table 1. Hardware-sensors and soft-sensors security nodes and their data collection flow paths

2.4 Development and Proposal of Concepts

Self-Aware and Adaptive Security Architecture: The interpretation, evaluation, and verification using the collected data led to the development and proposal of a hierarchical self-aware security architecture that effectively establishes accountability at the system-level with a security-specific black-box [28]. Further illustrating why such a proposed security architecture is relevant to fully connected, intelligent, and autonomous vehicles. The proposed work offered a systematic exploration of the landscape of security dynamism, self-awareness, and adaptiveness in the vehicular ecosystem.

Quantum Vehicular Ecosystem (QVE): As an outcome of both the quantum-related literature review and experiment, a quantum vehicular ecosystem is proposed based on the comprehensive investigation conducted on quantum and its advancements. Specifically focusing on automotive cybersecurity and its numerous applications. The proposed work emphasizes the critical need for enhanced security measures and specialized quantum applications in the context of vehicles. It also addressed a significant gap in the existing literature by shedding light on QVEs by providing valuable insights, including the importance of quantum-like modeling approaches and solutions that can improve vehicular security and its relevant applications.

Evaluating Security Interactions: In reference to section 2.1 and section 2.2. Seaming Security Dependency-Chains (SSDC) is introduced as an enabler to assess the impact of these dynamic security interactions and interconnectedness on individual and collective perspectives. Thus, highlighting the significance of capturing security dependencies, inter-dependencies, and relationalities as they intersect, overlap, and converge within a dynamic security interaction and context.

2.5 Testing, validating, and Integrating security solutions with real-life use cases

The experiments conducted in association with the multi-sensing, IDS/IPS, and security interactions in this dissertation were tested, verified, and validated using a real-world Renault T520 freight truck with a custom-built compute unit. Based on the initial review of the literature and further development of algorithms, protocols, and architectures, leading to the developed and proposed concept, architecture, and framework. Each of the proposed works underwent testing, verification, and validation using experimental approaches and practical test beds.

3 Theoretical Foundations

This chapter and its subsequent sections offer a theoretical foundation for the vehicular security challenges the dissertation intends to address. It is presented systematically, starting with a brief introduction on vehicular security and its associated technologies. Vehicular state-of-the-art security is covered in its present in-vehicle security infrastructure, the threat landscape with its consequences, challenges and limitations, and vital emerging technologies with the potential to influence vehicular security in the near future.

3.1 Vehicular Security

Vehicular security used to be one-dimensional on a single plane, without a combinatorial matrix of security characteristics and properties. Security concerns were quantifiable and attributed to the physical protection of each automobile. Decades have gone by in an evolution that currently produces numerous multi-dimensional security characteristics and properties beyond that single plane. Hierarchies of combinatorial security characteristics and properties of traits, complexities, and concerns are now discussed in automobile cybersecurity across a matrix of thriving, accomplished, and emerging technologies.

Today, society is confronted with a new generation of vehicles in a new paradigm of artificial intelligence (AI) and quantum capabilities. Capabilities that could advance the potential security and safety for vehicles across homogeneous and heterogeneous sectors. Just as the traits, characteristics, and properties of these advances and capabilities are critical to society's development and the global economy. Security has maintained its long-standing impact and benefits regarding challenges and issues that progressively shape the vehicular landscape. It has predominantly become a persistent, influential, and prime mover and contributor to the success and failure of the vast percentage of critical infrastructures on which the interplays of society and the global economy rely.

Security is the critical differential characteristic in the relationship and transition between traditional driving and driverless autonomy. A differential resonates from the perspective that functionalities need appropriate security measures. Thus, there are implementation security requirements that need consistency across diverse vehicular ecosystems and their networks for the safety of society. Infrastructures that

include security measures, such as automotive cybersecurity architectures and their hybrid multi-faceted components, such as decision-making on the part of the in-vehicle nerve systems and their analytical layers, have now introduced security concerns. It also extends to real-time security monitoring and visualization layers that give feedback to both in-vehicle occupants and remote virtual operations analysts. The characteristics and properties attributed to these layers report and present information at each stage as authentically as possible. Therefore, these layers need not only to perform their functions and operations optimally but must exhibit a vast comprehension of context awareness across a variety of domains. Hence, self-awareness through dynamism and adaptiveness, maximizing security, is the next significant security paradigm in the automotive cybersecurity architecture and its ecosystem with hierarchies of system-level accountability.

3.1.1 Security Technologies

Today, cloud platforms account for the vast implementations that entail on-demand services such as data retrieval, automation, analysis, machine learning (ML), and others that society is accustomed to. Thus, solving relevant and technological challenges across these service domains on a day-to-day basis for individuals, organizations, and industries via intelligent processes and environments involves several Internet services. Cyber-physical systems and the Internet of Things, of which connected, intelligent, and autonomous systems are counted as part, rely on these service infrastructures through cryptographic technologies. As such, challenges and issues regarding privacy and data integrity on the part of society have relied on numerous hardware-to-service nodes from heterogeneous devices to facilitate communication secrecy. This secrecy extends to versatile interactions in human-to-machine (H2M), machine-to-machine (M2M), vehicle-to-things (V2T), and vehicle-to-Internet(V2I)[29]. Furthermore, the *"science of secrets"* [30], through cryptography, is still studied and investigated for advantages [31; 32] on how to efficiently and securely protect critical systems. Researchers and governing bodies in the field have impacted the current cryptographic infrastructures, as they benefit a wide range of technologies, such as in-vehicle and outbound vehicular communications. Public-key cryptographic schemes and infrastructures such as Rivest-Shamir-Adleman (RSA) algorithms have been the de facto infrastructure across internet communications, while private-key systems have synonymously been popular with vehicular security. Between the inability to factorize larger integers of the form $n = PQ$ efficiently [33] in polynomial time [34] and the computational complexity in s-box matrix operations, several variations of the cryptographic infrastructure today rely on these fundamental principles. Symmetric and asymmetric algorithms as post-quantum resistance schemes gradually undergo experimental transitions and are the underlying system infrastructure in such communications. However, unique and highly sensitive in-

frastructures across multi-dimensional organizations and industries already employ quantum-related cryptographic schemes and algorithms such as quantum key distribution.

3.1.2 State-of-the-Art

Throughout human history, specific phases of technological development have led to significant advancements that have had both beneficial and detrimental effects. Technology has also evolved through competition, the presentation of solutions, and a shared commitment to address both the pressing challenges currently faced and those that may arise in the future. There is a strong correlation between the rapid advancement of technology and the many benefits society enjoys. Hence, researchers, practitioners, and organizations continue their efforts to uncover the potential breakthroughs that technology has to offer. For instance, the current state of automobile security infrastructure has prompted further research in various security sectors to meet the increasing demand for vehicular services [35], vehicular network deployments [36], and in-vehicle electric infrastructure [37].

Trends in vehicular security are diversified based on the field of study and the domain of concern. However, five trends predominantly recur in this research field: security from the perspective of personal safety and factors influencing acceptance[38; 39; 40; 41; 11] form the first category. Including other contributing insights on topics such as safety protocols, risk mitigation, and user protection [39; 42; 38; 43; 12].

Further research and investigation indicate the second category focuses on cybersecurity threats and assessing the extent to which corresponding attack-to-defense implementations exist concerning challenges and evaluations [44; 45; 46; 13; 47; 48; 49; 50; 51; 52]. Substantial literature and exploratory investment from theories, concepts, frameworks, and experimental proposals demonstrating vulnerabilities with sophistication and susceptibility across processes and sensors [53; 49; 54]. Assessing the security of connected and autonomous vehicles by [55] covered a range of cyberattacks, including intrusion detection, data breaches, and system vulnerabilities, highlighting the importance of robust security measures. This study further divided the security and vulnerabilities into three main categories: in-vehicle, V2X, and digital infrastructures. It also highlighted the inter-dependence of vehicular (ECUs), illustrating the cascading implications of attacks where one infection can affect others.

In the third category, much emphasis is on the cybersecurity risk management approaches and frameworks that follow such approaches. For example, cybersecurity and safety management system (CSSMS) [56] approach that relies on the ISO 26262 and ISO/SAE 21434 for integrated safety and cybersecurity process management in vehicles. In a different perspective on practical security examination tailored from a cybersecurity evaluation framework (CSEF) on asset identification, threat ex-

amination, risk assessment, and security testing [15].

The fourth category emphasizes proposed frameworks and concepts that significantly dwell on methodologies and operational techniques, with the inclusion of AI and ML. For example, a lightweight and secure authentication and attestation scheme for attesting dynamic transit vehicles in the line of sight [17; 57]. A real-time intrusion detection framework based on normal state-based and a deep learning-centered bidirectional long short-term memory (LSTM) architecture [18]. Similarly, there have been proposed remote diagnosis and maintenance (RD&M) systems [58] that are made up of different layers.

The final category surveys a wide range of research focal views that incorporate the combinations of the first four categories. For example, the discussion of security and functional safety of automotive embedded systems [19] focuses on AI challenges. They position their contributions by emphasizing the integration of safety systems and process viewpoints, highlighting the transformative impacts of machine learning (ML) on automotive embedded systems. A survey on attack and defense on intelligently connected vehicles [59] noted that cybersecurity in these vehicles is made up of two components: the security of inter-vehicular communications and in-vehicle security. They are further classified into four categories: cryptography, network security, software vulnerability detection, and malware detection. Others offer a comprehensive survey on AI through the advancement of autonomous vehicular technologies and their use of ML, deep learning, reinforcement learning, statistical techniques, and usefulness [60] in IoTs for vehicles from safety and security concerns related to risk examination. Table 2 illustratively summarizes these vehicular security approaches from the literature.

Proposed Approaches	Dynamism	Self-Awareness	Adaptiveness	Context-Awareness	Focal Point	Security Characteristics	Dependency	Inter-Dependency	Relationality
Regulation-Based Mitigation [45]	✓	×	✓	×	Risk management and regulation-based automotive cybersecurity approach	Security requirement Check-list	×	×	×
Risk Assessment-based Framework [46; 13; 47; 48; 49; 50; 51; 52]	✓	×	✓	×	Risk mitigation via systematic layout framework	Rely on risk assessment and security controls	×	×	×
Cybersecurity Risk Framework[56; 15]	✓	×	✓	×	Rely on ISO standards (ISO 26262 and ISO/SAE 21434) as bases	Security asset identification and threat examination	×	×	×
Cybersecurity Frameworks [17; 57; 18; 58; 19; 60]	✓	×	✓	×	Cybersecurity methodologies and operational techniques	Deploys Machine Learning, Real-time, and Attestation Mechanism	×	×	×
Dissertation Approach	✓	✓	✓	✓	Focus is placed on automotive cybersecurity dynamism, adaptiveness, self-awareness, and context-awareness	Utilizes various security approaches in its formulations with emphasis on impact, influence, and relational interplays	✓	✓	✓

Table 2. Table covering the vehicular security state-of-the-art solutions from the literature.

3.1.3 Research Gap

The vehicular security landscape is transitioning towards a paradigm that embraces autonomy across several layers of automotive cybersecurity. It is also apparent from the above sections that (1) security requirements attributing to vehicles have evolved, (2) Traditional security measures that deploy static mechanisms are no longer sufficient to drive the evolving security parameters, characteristics, and properties, and (3) this transition is envisioned towards SAE level 5. Meaning, security complexities and their intricacies are also compounded towards reaching the ultimate autonomous vehicular infrastructure and all that it would influence, impact, and shape. Considering all these avenues along with trends and organizational security transitions, there are research gaps that arise from the necessity vehicular security architecture has to offer via self-awareness, dynamism, adaptiveness, and context-awareness. Thus, more research is needed in the systematic exploration of security dynamism, self-awareness, and adaptiveness with an in-depth examination that balances appropriate security measures.

3.2 Threat Landscape

The propositional value and prolificacy of the technological leap in Connected, Intelligent, and Autonomous ecosystems (CIAE) is a double-edged sword in its intricacies and complexities. The prolificacy of CIAE is beneficial to both the Blue and Red Teams, White and Black hats, enablers, and experts. This implies that its security challenges and issues can be a bullwhip transversal diversification in its application sectors and organizations, catalyzed by transcendental attack vectors and surfaces. Therefore, the analysis and correlation between these security challenges and the interaction of external technologies and advancements with connected, intelligent, and autonomous vehicles are correlations mapping to associated security challenges. Hence, it presents a complex attack mapping of interaction with interconnecting technologies within the vehicular ecosystem threat landscape. This threat landscape is, therefore, categorized in a taxonomy of attack types comprising five distinct categories: Identity, Application, Network, Platform, and Hybrid-based.

3.2.1 Identity-Based Attacks

Communication security among various infrastructures has been enhanced by the capability to identify, verify, and attest to the integrity of devices, nodes, entities, and platforms involved in the communication process. However, challenges and complexities related to identity verification persist, as noted by cybersecurity experts [61]. In the transition to a cloud-based infrastructure for numerous organizational processes, platforms, and services, Identity-based attacks are significant as they en-

compass both human and non-human entities [62]. For example, connected, intelligent, and autonomous vehicular identity security issues persist, per findings from the research community, due to the rise of identity and cloud infrastructure migrations. The proliferation of Internet of Things (IoT) devices and gadgets in public and private spaces has also contributed to the growing complexity of vehicular networks, particularly in their deployment and utilization in vehicular domains. According to the Verizon Data Breach Investigation Report (DBIR) of 2022, a significant proportion of web application breaches (80%) and all breaches (40%) relate to identity-based attacks [63]. Therefore, ensuring the security and reliability of authentication attacks and associated processes among interconnected and communicating devices poses a significant challenge to credibility and integrity. There are multiple methods for achieving the concealment of device identities. In instances such as connected, intelligent, and autonomous vehicles (CIAVs) are susceptible to spoofing and other attacks. The GPS spoofing [64] technique uses devices or software to manipulate GPS signals that can lead to unintended actions, for example, the perception of false localization or route injection. Vulnerabilities such as these could be compounded by the expected high number of roadside units (RSUs), pedestrians, and vehicles. It can include other nodes and devices expected to be present in this identity-based attack scenario. In a comparable vein, networks may contain concealed rogue gateways and access points that give rise to man-in-the-middle (MiTM) attacks for further intelligent vehicle impersonation. It involves employing a fake self-driving car to mimic the behavior of a real one. Attacks like these can be furthered and extended by tricking other vehicles or systems into making incorrect decisions or exposing sensitive information.

3.2.2 Application-Based Attacks

Security interlocks with the security architecture and parameters on board, attached, or embedded in intelligent vehicles through seams. Most often, each vehicle deployment ships with its own set of security infrastructure, either on the software or hardware side. These include the design phase security, firmware, operating systems, diagnostics, embedded instructions, and others as default security features. Application-based attacks seek to explore the vital underlying characteristics, properties, parameters, and metrics of these in-vehicle networks, security environments, and interacting ecosystems. Besides the malicious intent, some outcomes arise from security compromises via unintentional interactions.

Current vehicles have extendable software applications, hardware, and platforms with in-vehicle interactions through hot spots, plug-and-play, Bluetooth, WiFi, and many others. Application-based software exploits find and exploit vulnerabilities of outdated characteristics, properties, and parameters to gain unauthorized access or control. These unauthorized scenarios can be of several avenues, for example,

misleading maps to invoke inaccurate decision-making and unsafe routes, in-vehicle malware injection to inhabit a security environment, and ransomware.

3.2.3 Network-Based Attacks

There are two distinct network infrastructures related to connected, intelligent, and autonomous vehicular ecosystems: the in-vehicle and external network infrastructures. In-vehicle network infrastructure, for example, has facilitated society's convenience with the aid of wireless communication for peripherals and in-vehicle core networks. The wireless communication infrastructure has been in support of vehicular nerve Controller Area Network (CAN) Buses with Electronic control units (ECU), Local Interconnect Network (LIN), and Flex-Ray. Meanwhile, external vehicular networks over the years have gradually been integrated across a vast range of vehicles with operational modems, GSM, LTE 5/6G, and others. As these vehicular networks aid Over-the-Air (OTA) communications, the impact of network traffic transmission on networks is a significant factor in the increasing number of attacks that occur through remote interventions.

Routine and unforeseen continuous process of repair and replacement in the maintenance of user vehicles also necessitates using brute-force security strategies. However, such measures may leave vulnerabilities for subsequent attacks, including Bot and SSH exploits. As the technological components integrated into these vehicles age in a rapidly evolving vehicular market, their capacity to manage security vulnerabilities within a complex network of dependencies, inter-dependencies, and relationalities diminishes and becomes increasingly critical and constrained. These risks are not limited to the vehicle perspective but extend to users and interacting nodes. Legacy systems pose security risks related to connectivity that are susceptible to exploitation due to discrepancies in security integration of variations in heterogeneous hardware [65] and software sourced from various manufacturers, vendors, and suppliers, which may result in network-based security breaches.

Vehicular attacks, specifically Denial of Service (DoS) in the form of VANET DDoS [64] and other variations, have consistently demonstrated high success rates in passive and active contexts. The excessively overwhelming influx of Denial-of-service attacks on vehicular communication systems can make it difficult or nearly impossible to perform in optimal operation. Thus, potentially disrupting intended targets such as networks, services, sensor arrays, and others, eventually rendering targeted vehicles unavailable and inoperable. Side-channel attacks [66] using information leaked, such as power consumption, electromagnetic radiation, or timing data, to infer or extract sensitive information or compromise the vehicle's security. Sniffing [66] attacks, as preliminary scouting, lead to injecting malicious code, data, and the attachment of other devices to rogue nodes and shadow networks. The constant reiteration of vehicles' life cycles by the rapid evolution of perennial vehicles

from production conveyor belts to security updates and upgrades makes it challenging to mitigate remote malware cyberattacks, network intrusions, unauthorized access, stealing sensitive information, manipulating vehicular behavior, and disruption of operations.

3.2.4 Platform-Based Attacks

Platforms have been the core infrastructure that application-based infrastructures utilize to facilitate communications, on which identities are verified via network-based infrastructures. With new generations of in-vehicle networks capable of higher throughput, such as 10 Mbps for CAN-FDs and beyond, for automotive Ethernet applications. Platforms exist as containers on which hybrid, homogeneous, and heterogeneous sub-containers co-exist as they share resources, connectivity, operational parameters, and security characteristics and properties of the primary platform, and those of co-inhabiting sub-containers, which might represent services, nodes, components, hardware, and software. Hence, platform-based infrastructure interactions are formed on single and multiple interconnected platforms locally and remotely, which enables intelligent mobility platform communication between various platforms and endpoint node infrastructures. Therefore, platform-based attacks of these characteristics and properties leverage the susceptibilities inherent in a platform-based sub-interconnecting component, employing either an active or passive approach. These approaches include the injection of false bits into the Controller Area Network (CAN) [66; 64], manipulation of sensors by altering value perception or introducing additive noise, and impacts on adversarial deep neural networks specifically targeting [67; 68] sensory platforms. Deliberate malicious data is introduced into the training process, modeling inputs, data intake endpoints, and nodes to result in erroneous decision-making, render them susceptible to exploitation, and exhibit abnormal behavioral tendencies under specific circumstances. Distinct attributes and qualities of different hardware and software platforms have necessitated the utilization and hosting of several services and operations. The wide range of flexibility, scalability, and ease of deployment of these platforms has been the backbone of the current boost in cloud transitions and migrations. Devices that operate on these platforms have a variety of customizations based on targeted tasks, characteristics, and properties with diverse proprietary skills entrenched in dependencies, inter-dependencies, and relationalities. The fundamental portion of these platforms is governed by firms, industries, companies, and enterprises that commonly employ platforms to facilitate, relay, interface, and interact with diverse sub-systems.

Platform-based attacks leverage the importance of accurate data interpretation as a core component of intelligent mobility decision-making, with its dependency, inter-dependency, and relationality in several ways. Perception attack accomplishes this by deliberately disseminating inaccurate information to the sensory platforms

by manipulating GPS signals, modifying road signs, and fabricating artificial objects within the perceptive environments to induce confusion or deceive connected, intelligent, and autonomous vehicles. Attacks of this nature exploit the human aspect to compromise websites, online resources, and frequently accessed infrastructure. It is to affiliate and infect vehicles in watering hole attacks, while in-transit tampering elicits sensitive information and inflicts vehicular damage directly or through maintenance activities.

V2V and V2I inter-dependencies and relationality of data sharing in a vehicular ecosystem possess the ability to enable rogue vehicles to conduct attacks such as jamming or interference, amplification attacks, and electronic warfare. Amplification attacks utilize an intelligent vehicle as a medium to amplify or disseminate malware, rogue networks, target and compromise other systems or networks, and other electronic devices to impede or disrupt communication systems such as GPS, Wi-Fi, or cellular network platforms. Connected, intelligent, and autonomous supply chain platforms can utilize attack staging by compromising various stages during production, assembly, or distribution.

3.2.5 Hybrid-Based Attacks

The amalgamation of diverse attack bases leverages a combination of cross-identity, application, network, and platform into a unified hybrid-based attack. Inter-connectivity of security seams presents an attack vector that expands and exploits the potential scope dependencies, inter-dependencies, and relationality. Attack categories ranging from identity to platform take several variations and forms to materialize compromised data, unauthorized acquisition and access, and manipulation of information in vehicular platforms. For example, confidential unlawful information acquisition from in-vehicle systems or related cloud-based interfaces and data storage, passenger identities, travel history, and payment details requires several attack paths. Social engineering is an attack path that relies on psychological tactics and deceptive techniques. It exerts influence over assets such as operators, developers, and consumers to undermine security systems. Human-in-the-loop as a social engineering attack variation influences the human operator of an autonomous vehicle towards erroneous decisions with hazardous consequences. Credentials are also divulged by invoking the installation of malicious software onto their devices with full knowledge of its usage in a connected, intelligent, or autonomous vehicle via phishing. Insider threats from individuals with authorized access to the systems would take advantage in the same manner as employees, contractors, or other insiders to enact physical tampering or deliberate manipulation of components such as sensors, actuators, control systems, and others.

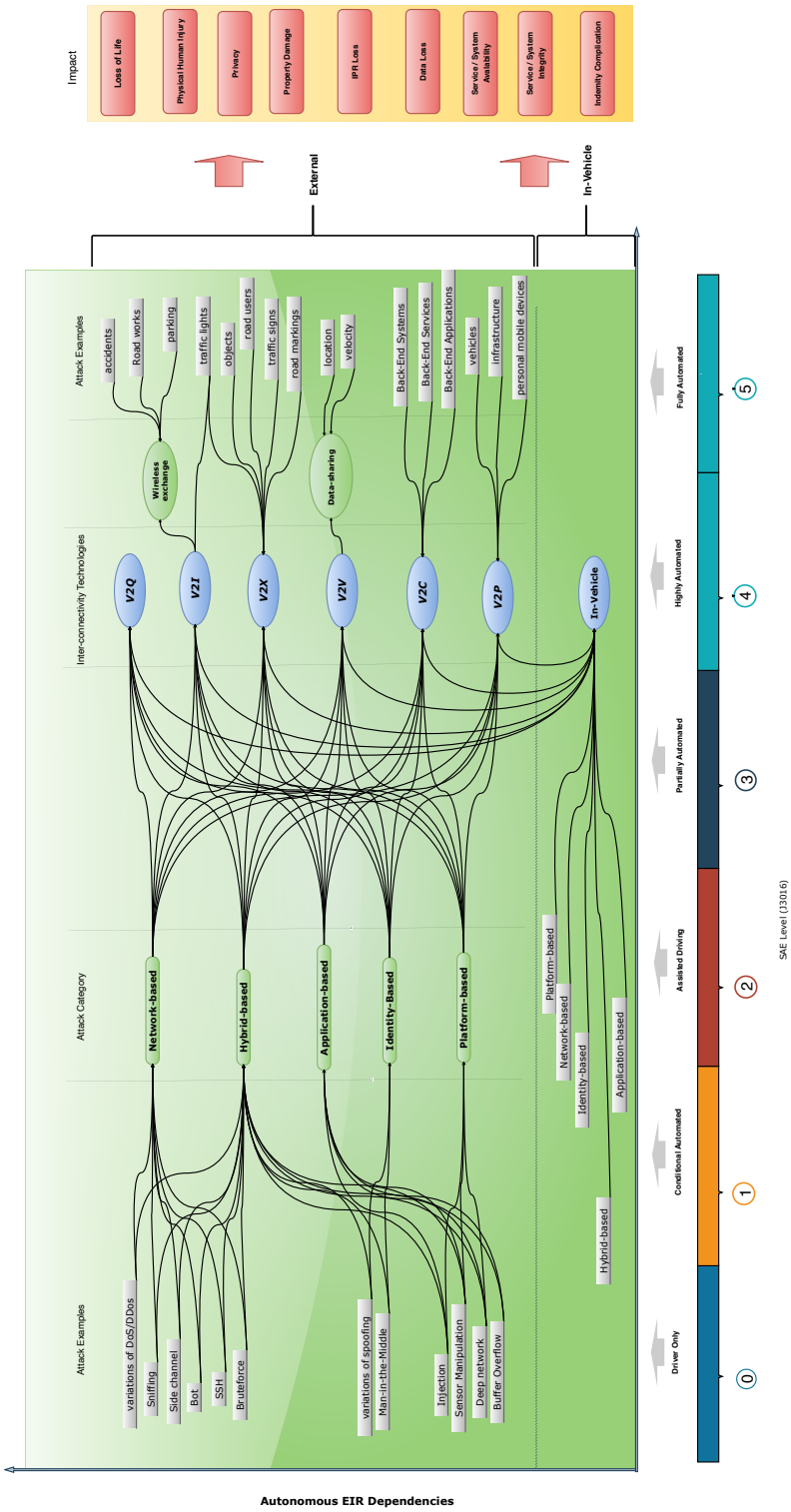


Figure 4. Examples of attack-based outcomes with their realm interplays

3.2.6 Research Gap

Extensive research from this literature review and beyond has demonstrated that investigating security requirements, attack-to-defense strategies, vulnerability susceptibility, and other factors provides a comprehensive understanding of the security scope in the vehicular environment and its related systems. Figure 4 illustrates such insights with associated impacts and influence on society's part. Nonetheless, there is a research gap on how these comprehensive insights are often analyzed on the relational interplay of security dependency, inter-dependency, and relationality of vehicular automotive characteristics and properties, individually and collectively.

3.3 Challenges and Limitations

Society has become more aware of vehicular security flaws, challenges, and issues over the past few years. The literature has also collaborated further on the significance of vehicular security in the present era of AI and ML dominance, as vast research demonstrates the challenges and limitations associated with security. Several technological approaches and proposed techniques, with surveys, have provided comprehensive and reliable insights into these issues. However, this thesis extends the attack-to-defense causalities in regards to research questions to investigate correlations and propose its outcome on solutions, concepts, and practical perspectives to the fulfillment of the research goals. For that matter, answering the research questions is instantiated into three categories focused on the research contributions this thesis is trying to accomplish. The three identified problems (lack of dynamic and adoptive system-level security accountability, the impact and influence of dependency, inter-dependency, and relationality, and quantum communications and applications for the vehicular realm) are illustrated in the following subsections taking into account vulnerability susceptibility, evolution of technological advancements in quantum and AI, practical security implementations, existing standards, protocols, and justifications consistent with real-world applications of this work.

3.3.1 Security Trend

The advances in artificial intelligence (AI), quantum computing, machine learning, and other technologies have also ignited several research avenues in the vehicular realm. One such avenue is the vehicular security complexities of associated issues and challenges regarding the growth of coded instructions with autonomy. Decision-making on our highways has the potential to be shaped and influenced by these advancements as the trajectory starts to converge with vehicular functions and operations, taking advantage of the perspective that:

- Vehicles are becoming increasingly computerized and automation-driven, with

features and functions that extend beyond in-vehicle interactions and communications.

- Several vendor infrastructures and in-vehicle architectures are starting to rely on a bi-directional external infrastructure for resources and transactions, making security and safety two sides of the same coin.

- The sustainability of vehicular life-cycle management, continuity support, and the effects of technological advancements such as quantum technologies on security posture (for example, updates, maintenance, and repairs) are critically important to vehicular ecosystems and their security infrastructures.

3.3.2 Security Accountability

The continuity and consistency of security in the life cycle of traditional vehicles contributed little empirical evidence to the security of the vehicles we use today. It also left an ominous assurance of future security in the hands of the user [69]. With the advent of vehicle-to-any (V2X) and the above highlight in the vehicular ecosystem on the horizon, the convergence paradigm of the technological surge necessitates a substantial investment in Automotive Cybersecurity Protection (ACSP). Hence, factoring in the life-cycle and longevity of vehicles on our roads, the underscoring challenge and limitation in these explorations has been the prioritization of security dynamism, adaptiveness, and self-awareness.

Prior research from the literature has noted this importance in the convergence paradigm and has also attracted several research perspectives. Further literature also shows that the demand for in-vehicle cybersecurity-to-defense mechanisms is significantly critical as it relates to findings such as acceptance, the protection of data, risk management, assessments, frameworks, and many others. Others have also argued that certain aspects of a network's security depend on the security of the individual devices and systems connected to the network and the functionality of various software applications and systems. With this evidence, one underscoring characteristic and property of these observations is the evolution of addressing security context-aware dynamism, adaptability, and self-awareness. Context-aware security dynamism, adaptiveness, and self-awareness are significant as vehicles would depend on each other and the external infrastructure in a vehicular network within a vehicular ecosystem. The security of software components operating on vehicular hardware can affect the hardware's security and vice versa. A vulnerable component can have a cascading effect on the entire network or compromise an entire vehicle's security within an ecosystem.

3.3.3 Dynamic Security Interactions

Security context-aware dynamism, adaptability, and self-awareness are critical for vehicular security evolution over time. As such, evolutions in quantum computing and cryptography, post-quantum equivalent, and AI would impact and influence vehicular security as we know it. For that matter, dynamic interactions of security and activities related to vehicles and their networks, ecosystems, and external infrastructures would share characteristics and properties such as security dependency, inter-dependency, and relationality. A growing interest has prompted the research community to investigate this role in cybersecurity threats and corresponding attack-to-defense implementations. This is because dynamic interactions and associative security of diverse technologies interlock through integrations and complementary associations, resulting in developments that significantly heighten security dependence, inter-dependence, relations, and complexities. Given this, several discussions have expressed notable perspectives across vast research. However, in this case, the discussion on how their mentioned points and perspectives relate to security dependency, interdependency, and relationality independently and as a collective lacks from the perspective of the vehicular ecosystem. Therefore, to the best of our knowledge, the literature has not addressed the collective impact of security dependency, interdependency, and relationality in the vehicular ecosystem holistically. Thus, one advocacy of this research is that analysis of security complexity with increased automation and other related security factors and contributors must encompass security complexity with seaming security dependency-chains perspectives. In addition, the security landscape in the vehicular ecosystem is evolving in dynamism, self-awareness, and adaptability, and with the growth of AI adoption, SSDC is of paramount significance.

3.4 Quantum Technologies

The term ”quantum” has been closely linked with the field of quantum mechanics [70; 71], as Steve Wiesner’s paper Conjugate Coding considerably ignited quantum cryptography realization [72]. Sparking discussions and adding depth to conversations regarding quantum computing [73], informatics and communications [74], Max Planck’s discovery[75], Einstein’s 1905 prediction, and Sir Isaac Newton’s interpretation of light as a wave, other than an energy source with millions of elementary particles [76] were significant. However, with Arthur Compton’s work leading to photons in 1923 [77], Quantum also brings to mind cryptographic implications and espionage. In addition, cutting-edge research on its applications and integrations. Thus prompting the post-quantum initiative by the National Institute of Standards and Technology (NIST) [78] on post-quantum cryptography (PQC), quantum-safe random number generation, and other relational algorithms. As modern-day tech-

nology shapers, quantum cryptography and computing have sparked various security evolutions in communication and applicational integrity on traditional security infrastructures [79]. Quantum cryptography, more specifically quantum key distribution, makes use of the fundamental laws of quantum mechanics to construct encryption keys between two parties in a secure manner. This makes it easier to encrypt and decrypt data for the persons involved in the communication to identify and counteract any attempts to eavesdrop on their conversation [27]. As a method, it ensures secure communication by leveraging the inevitability of altering the quantum states as a security premise. Therefore, any attempt to eavesdrop on the transmission of the key will invariably be discovered and halted.

This is a significant development in the field of information security, as the unavoidable cascade of effects on operators to evolve and pivot towards other emerging security solutions and infrastructure is being triggered. All because several classical security infrastructures are beginning to evolve around quantum cryptography and computing [80]. These two technologies use the principles of quantum mechanics [81] as the primary basis on which both computational supremacy and secure communication are achieved.

Security deployments and implementations depend heavily on cryptographic systems and their infrastructures, setting the stage for the subsequent exploration of mathematical complexities and quantum computation. Noticeably, how mathematical complexities play a crucial role in existing applications across various fields and organizational sectors, in this, mathematical complexities [27]. However, classical computation infrastructures have been deemed insurmountable when it comes to proportional parameter scaling in exponential complexity. Unlike quantum computation infrastructure, this constraint is particularly relevant when considering time-bound polynomial instances of mathematical problems and application utilization. The pressure is even mounted further with QKD protocols, devices, and systems making technological strides in the market [82; 83] based on current market demand, with prominent companies leading the surge [84].

The trends in challenges and limitations in this domain include how quantum variational methods can enable the execution of exploitable tasks in a manner that bears a distinct resemblance to quantum mechanics [85], also known as quantum-like modeling. Quantum-like modeling demonstrates the application principles of quantum formalisms extended beyond the realm of quantum physics [86]. Therefore, aim to comparatively analyze how quantum-like modeling of vehicular ecosystems can advance the field of vehicular security toward fully connected, intelligent, and autonomous mobility. QVE Compared to existing vehicular security architectures (e.g., ISO/SAE 21434, AUTOSAR Secure Onboard Communication), QVE encompasses the whole vehicular ecosystem and its network, which includes security architectures and relatable quantum communications solutions for vehicles.

4 Results

At the beginning of this thesis work, four research questions were established to be investigated. The outcome of the questions is presented in this section, with each section answering a research question except research question **RQ1**. The first research question **RQ1** is answered in Chapter 3, where it is introduced in a wider scope with respect to the societal impact. Before delving deep into the question and providing a systematic structure of the problems, challenges, and the research gap. The structure and approach of how the rest of the questions are answered are presented in the following descriptions.

RQ2: What are the components of a security system and their architectural requirements for securing the next generations of fully connected, intelligent, and autonomous vehicles and their ecosystem?

- **Section 4.1:** This section answers the question by proposing a hierarchical self-aware security architecture in vehicular security and its characteristics, security-wise covering automotive cybersecurity through system-level accountability with the integration of a security-specific black-box. This architecture is implemented in a real-world vehicle by focusing on the security analysis aspect in an experiment that uses IDS/IPS with the purpose of securing the truck and multi-sensors utilized as a safety mechanism.

RQ3: How do the potential and limitations of quantum-based security influence future vehicular ecosystems and their security?

- **Section 4.2:** The section answers this question from the perspective of a proposed quantum vehicular ecosystem, after experimentally proving that quantum key distribution can play a role in vehicular security through a series of simulations.

RQ4: How to systematically analyze the security dynamics and interactions in a vehicular ecosystem?

- **Section 4.3 -** This section explores unique observations, security characteristics, and properties security-wise, in the interplay of security interac-

tion with research questions **RQ2 and RQ3**. Thereby, proposing a seaming security dependency-chains to answer this question as the individual and collective capturing of security dependencies, inter-dependencies, and relationalities as they intersect, overlap, and converge.

4.1 Self-Awareness with System-Level Accountability

To comprehensively analyze the concept of self-awareness, it is pertinent to consider a systematic array of terms that encapsulate its essence: consciousness, traits, capabilities, persistence, accuracy, perception, presence, self-knowledge, and competencies. These terms are particularly relevant in the context of the security challenges faced by connected, intelligent, and autonomous vehicles (CIAVs) and systems.

In the framework of hierarchical architecture, there exists a critical necessity for a system to be cognizant of its own security traits and capabilities. This awareness should be characterized by a continuous and accurate perception of its operative presence, alongside a thorough understanding of both its knowledge and abilities. Consequently, the notion of self-awareness security (SAS) evolves through the application of dynamic monitoring, comprehensive analysis, informed decision-making, visualization, and other advanced capabilities, which collectively facilitate the integration of multifaceted security solutions.

The security paradigms of connected, intelligent, and autonomous vehicles and systems stand to gain significantly from the implementation of a holistic SAS infrastructure. This transition emphasizes the imperative to move away from static or, in certain instances, partially hybrid approaches toward a fully dynamic self-aware security architecture, underscored by principles of system-level accountability.

4.1.1 System-Level Accountability Architecture

The proposed hierarchical Self-Aware Cybersecurity Architecture through System-Level Accountability, with the integration of a Black-Box, answers research question **RQ2**. The architecture consists of (1) distributed monitoring agents, monitored components, and a data feeder at the monitoring layer, (2) process controllers at the analysis layer, and decision controllers at the decision layer, (3) visualization controllers at the visualization layer, and (4) a black-box illustrated as the database visible in Figure 5 in an upper abstraction. The process-based module controller has four module-based deployments: the Analysis module, the Fail-Over mechanism module, the Fall-back mechanism module, and the Report/Support module. The Data intake feeders are the shippers of various metrics and incidents, such as measurements, status monitoring, and extracting data from controllers for scrutiny.

Delving a layer deeper below Figure 5 is the illustration of Figure 6, which is used to illustrate the systematic flow sequence. It introduces four main modules as

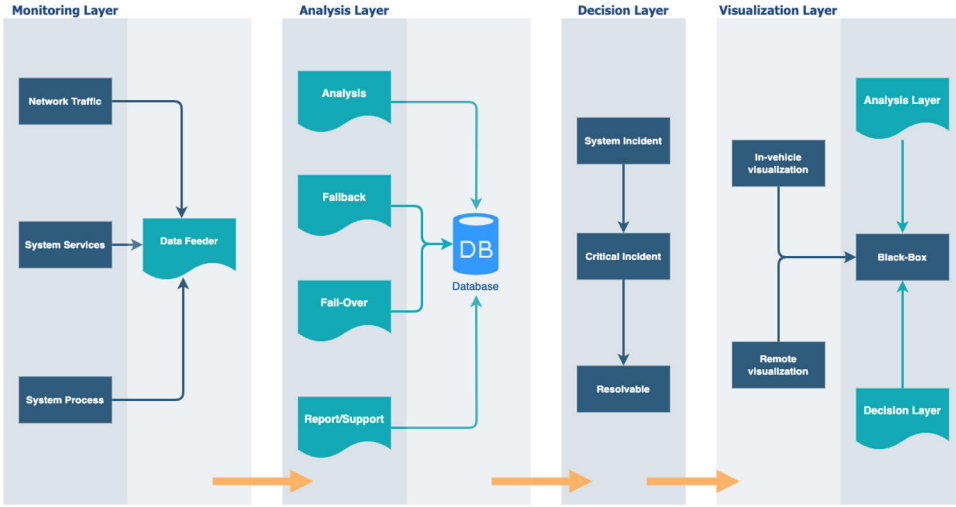


Figure 5. Overview of self-aware security architectural design for autonomous road vehicles.

controllers: monitoring, analysis, decision-making, and visualization, with a deeper sense of security organization. In a complex system, for example, with a security focus, processes and applications perform their routine operations by making changes and fulfilling requests, besides other critical interactions and activities. They interact with other processes and request to perform specific actions on behalf of other processes and applications, translating to external and in-vehicle security interactions. The security system-call interactions in routines follow this perspective, deducing that the self-aware system-level security accountability instantiates these system-calls to respective integrity levels.

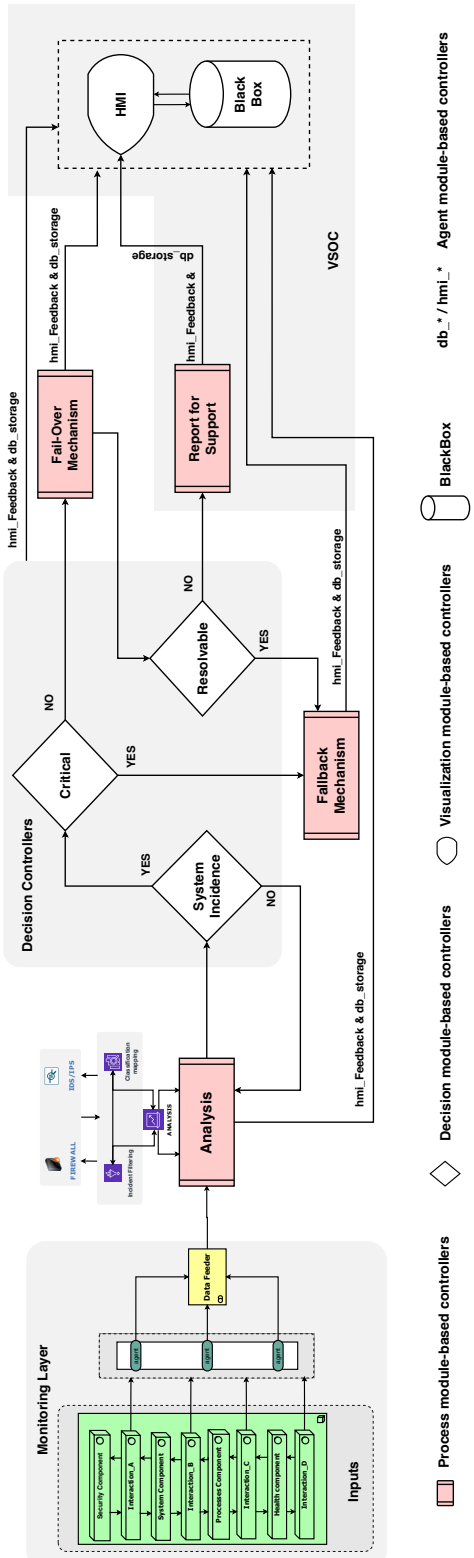


Figure 6. Overview of self-aware security architectural design for autonomous road vehicles.

Thus, the **Analysis controller's** functionality, for example, is to handle and analyze security-specific instances and incidents reported through the data feeders by the agents. As shown, analysis from the data intake feeders in the form of security interactions and activities (security, health, services, etc.) is sent to the analysis layer. The **fail-over controller** envisions an optimization management role responsible for compensating for security failures. This is to achieve and retain operational status if needed without entirely compromising the decision-making process and its related outputs. There are three **Decision module-based controllers** in the decision layer: **system incident, critical incident, and resolvable controllers**. The decision modules' operation follows each other and carries the identifier decision phases, respectively, from each associated analysis controller within the whole decision-making chain. The outputs include decision-related modules, evaluation nodes, devices, and components. On the other hand, the **fall-back controller** mechanism's primary premise is a secondary system or procedure that is designed to be activated if the primary system fails or malfunctions. Its existence, security-wise, for a connected, intelligent, autonomous vehicular in-vehicle infrastructure, networks, and ecosystem contributing facets is critical. **The reporting / Support controller** is the last in the chain before the outputs are sent to the visualization layer. For example, critical instances of in-vehicle interaction with external instances report an answerable justification upon system-calls, attestation, and investigations made by applications and processes of interest through a systematic flow. This accountability is extendable to the System, User, and specific pre-defined space within the decision module-based controllers. For example, the three decision modules evaluate security actions to permissions-related, processes-related, and predefined-related against pre-defined reporting incidents and rules (i.e., incidents, user, model, or within the model that triggered the rule). Command executions in a defined space enable the assessment of events from the analysis phase to the resolvable decision module. Furthermore, queries relating to specific instances of command executions and the support module mechanism visible in Figure 6 also relate to recording, keeping, and tracking summarizations.

4.1.2 Experimental Studies on Accountability

For the implementation and validation of the hierarchical self-aware security architecture via system-level accountability, the analysis aspect is studied further through an experiment. The experiment of the analysis sub-module of the architecture is performed on the same software and hardware platform in Figure 7 and 8, with all of its characteristics, properties, and implementation requirements. The experiment examined and analyzed the application of a dynamic Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) with a custom in-vehicle software and hardware implementation and design catalyzed by three distinct security decision controllers

through developed algorithms. In the experiments, a Renault T520 heavy-duty truck is utilized to house computing hardware integrated into the system as the DealComp ABOX-5200G4 compute-unit shown in Figure 8. Furthermore, on the developed security algorithms and architectures at the back-end implementation strategies, coding language-specific libraries are visible in Figure 7 as the software implementation layer. The physical on-site testing, calibration, and on-road testing, combined with remote testing and its attributing flow, are discussed further in the experiment.

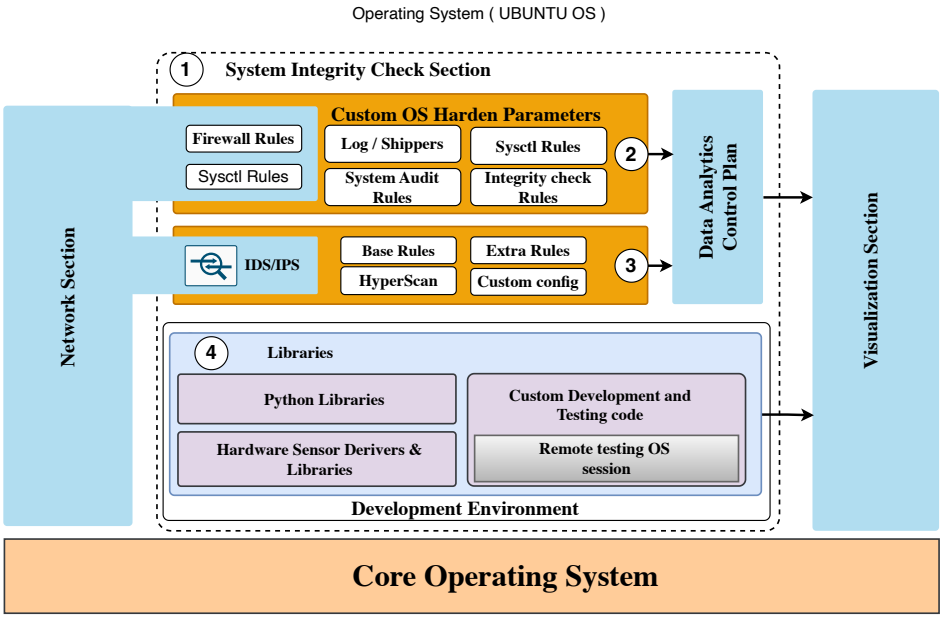


Figure 7. Software implementation of components hosted by the ABox-5200G4

Experiment I: Real-time Dynamic Security Analysis

Figure 9 illustrates two halves of the experiment that studied the dynamic in-vehicle security system. The first part shows the integration of the analysis sub-module, while the second part shows the data flow and stream of transactional relations within the compute-unit and its implemented testbed. A primary emphasis is placed on the analysis dimension of in-vehicle security infrastructure using a real-time intrusion detection system (IDS) and intrusion prevention system (IPS) in vehicles.

Because security has several facets of causality and contributors, the experiment focused on security accountability of system-level analysis by examinations, precise identification, and differentiation of legitimate and unauthorized traffic transactions, system calls permission, audits, and the effective optimization of algorithm imple-

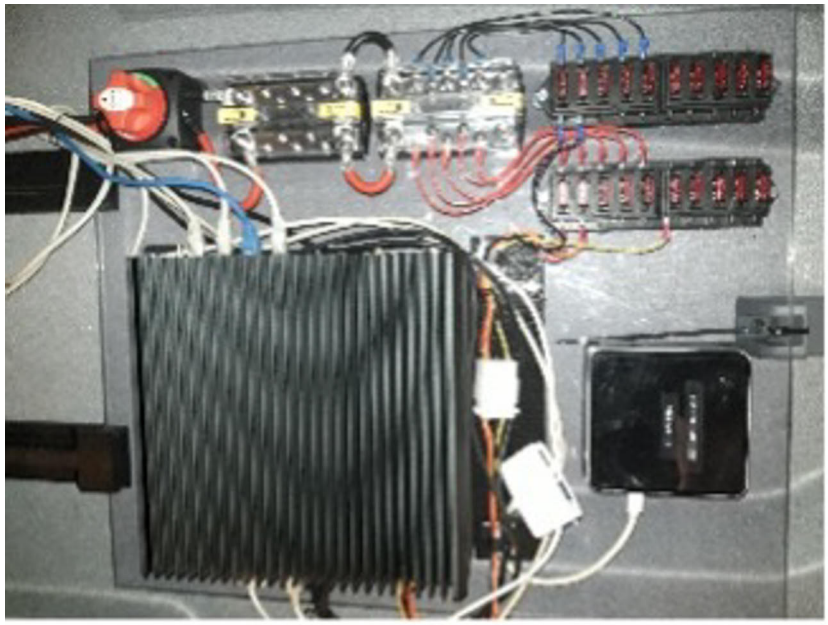


Figure 8. ABox-5200G4 Compute Unit

mentation over a broadband connection. The analysis utilized diverse data acquisition influx in both the software and hardware data pipeline in the data flow part. Characteristics and properties were observed among system health metrics during a testing instance, with illustrations in Figure 10. For example, the average comparative Suricata process CPU utilization and memory consumption of the data processing, which contributed approximately 54.9 percent. Processes related to sensors like the Ouster Studio and Team-viewer used in remote tests contributed a range of approximations from 0.2 percent to 2.337 percent, as illustrated in Figure 11. Background processes of native, custom, and hybrid tasks were also periodically examined to verify that all of their critical nodes, including the sensing nodes, are operational and that the rules are in effect and functional.

In the span of the experiment duration, the truck's operational routines generated several login attempts recorded in the time frame with their corresponding geographical locations for root and admin users, respectively, in Figure 12. Execution rules and custom configurations generated were also tracked to their executor, time frame, User counts, process counts, started and stopped processes with detailed accountability on their external interactions from DNS, TLS, successful and failed attempts, and others. For example, in-vehicle authentication results assessment, while simultaneously monitoring the resources linked to these procedures and their associated system-calls and processes, with a clear illustration from the back-end evaluation of processes matching the network traffic certificate legitimacy and associated critical

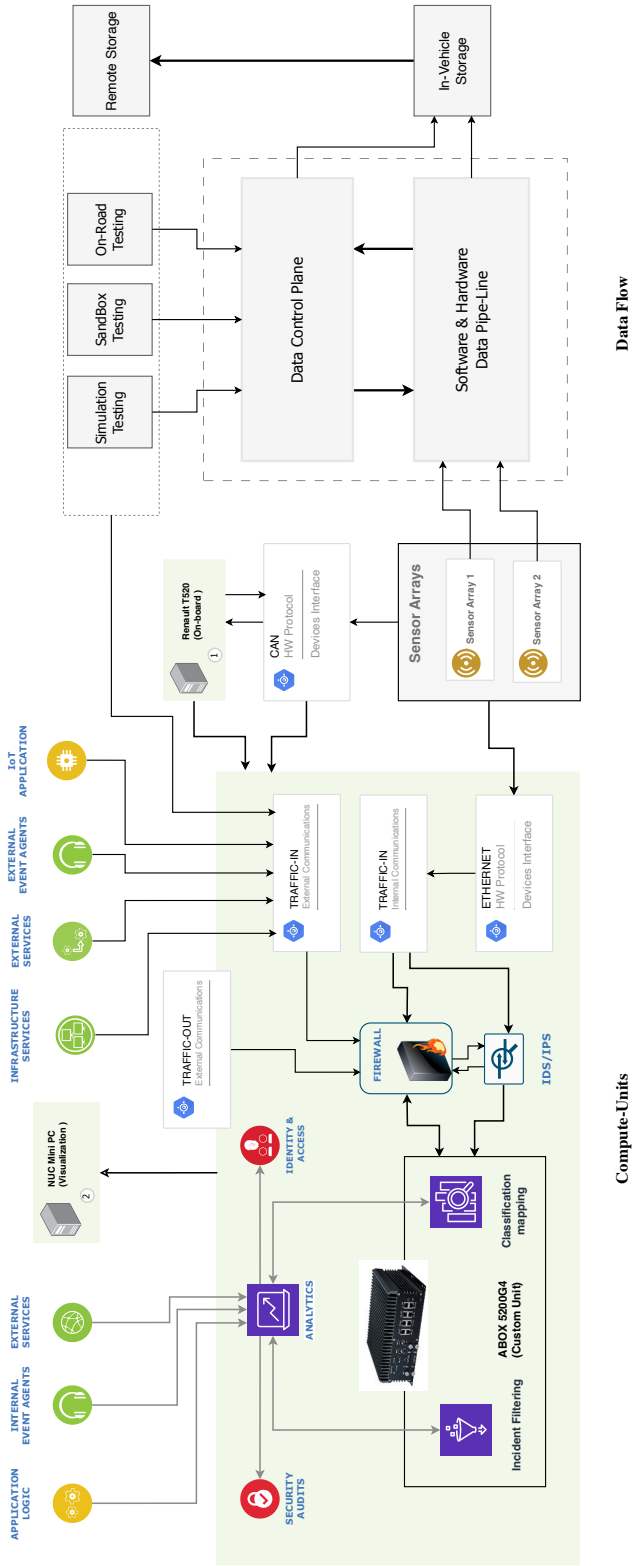


Figure 9. Real-time dynamic security interactions and SSDC perspective using an IDS/IPS.

parameters, such as the TLS validation.

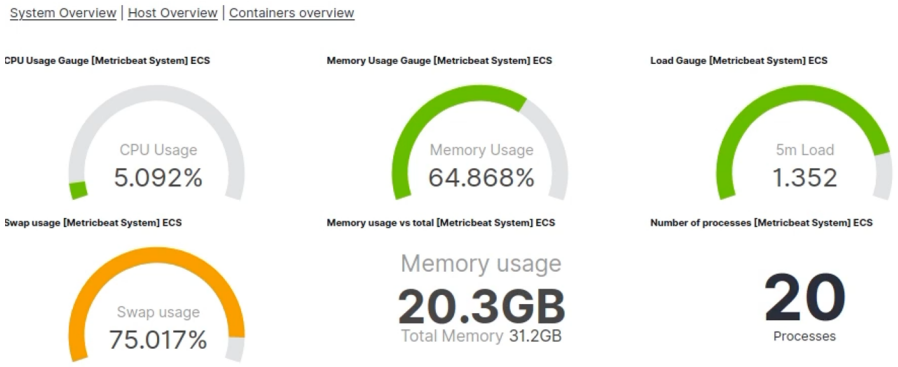


Figure 10. System Health Statistics

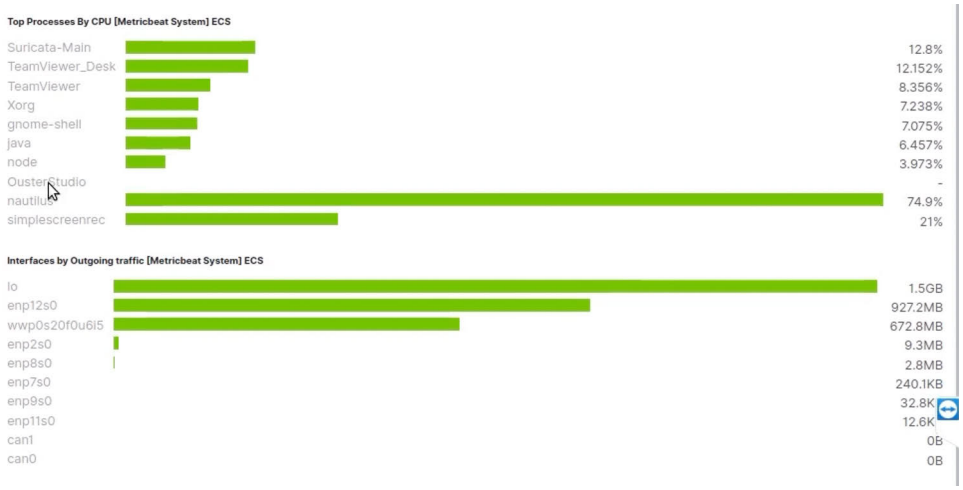


Figure 11. Process-specific Health Statistics Sample

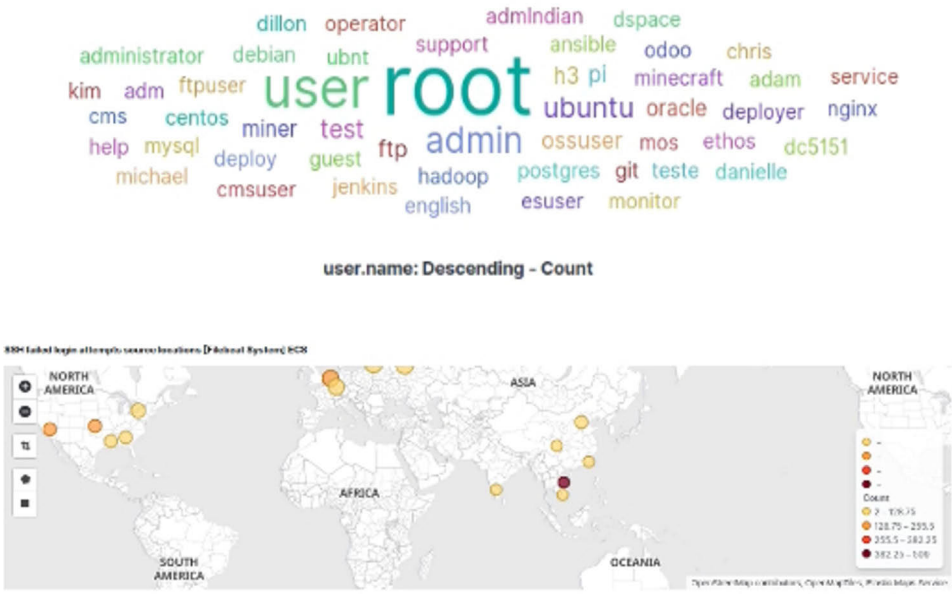


Figure 12. SSH Attempts with its geographical origination

4.2 The Role of Quantum in the Vehicular Ecosystem

In the answering research question **RQ4**, the findings are presented in two aspects. The quantum informatics aspect that plays a significant role in the proposed quantum vehicular ecosystem is the part that pertains to the experimental simulation. The other is the stance taken, through the proposal of the quantum vehicular ecosystem (QVE). The convergence of quantum technological applications and quantum-like modeling for the benefits of the vehicular ecosystem, with security serving as the focal point, was found to have entrenched in quantum sensing, quantum annealing, and quantum communication. An observed theme in the literature was the indication of the potential of quantum. Corroborated in diverse publications as well as its applications in the vehicular context, particularly in quantum annealing and communication. Besides these two, the principle of applying polarized single-photon emission characteristics and properties to maximize their use in the context of vehicular security and associative infrastructures is predominantly growing in the research community through quantum sensing.

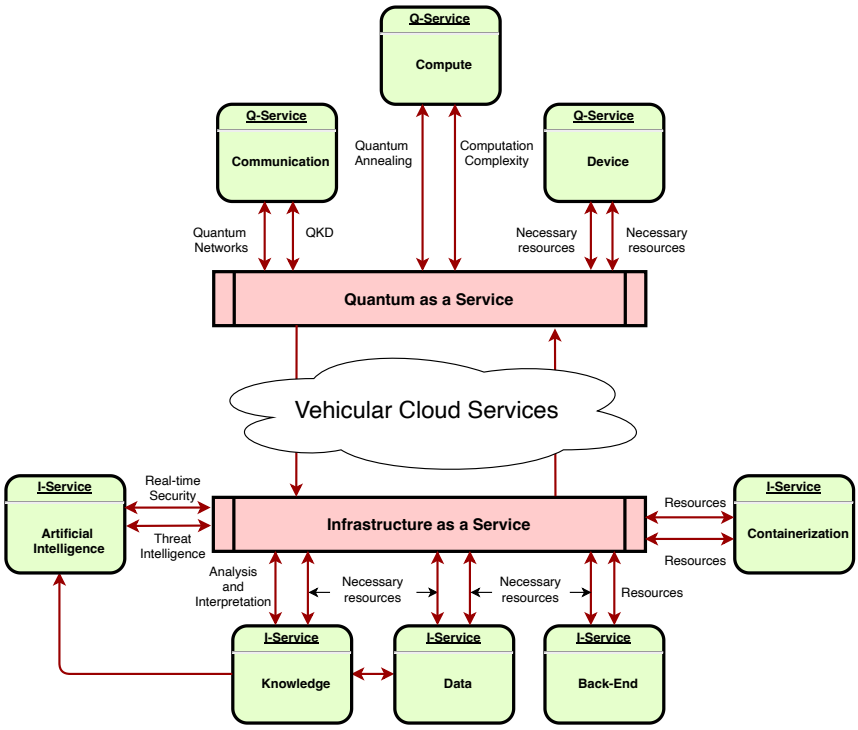


Figure 13. Quantum as a Service

4.2.1 Quantum Vehicular Ecosystem

The proposed QVE envisions the accommodation of quantum simulations via a quantum-like modeling approach that not only offers opportunities to resolve vehicular optimization problem complexities but also extends to classical problems and challenges in machine learning and artificial intelligence. As the justification for the necessity of a QVE, observations were made that indicated the trajectory of demands and service offerings. These service offerings are extended and elaborated in Figure 13, seeing Quantum as a service(QaaS) advantageous in this context. A quantum platform that offers the availability of services such as bridging infrastructure as a service and quantum as a service, tailored for vehicular needs in computation overheads and security complexities. Constructing or possessing quantum capabilities is improbable for a wide range of organizations and industries in the automobile sector. Thus, the primary inquiry in the vehicular domain, particularly in this dissertation, is what quantum as a service contributes to the QVE, and how its potential can be realized.

With the aim of establishing a quantum vehicular ecosystem as proposed in Figure 14, an inference in the literature also reports a strong relationship between quantum key distribution as a communication medium and the security of current vehicular communications. Upon reviewing the applications of quantum-oriented technologies related to fully connected, intelligent, and autonomous mobility, keeping post-quantum in mind, this study found that the communication aspect dominates the literature in a variety of cases. Thus, with respect to the concept of a quantum vehicular ecosystem (QVE) and the exploration of quantum-like modeling for vehicular security, these cases fall into a wide range of significant clusters. These clusters involve the integration of quantum key distribution (QKD) into the existing infrastructure and its use as a communication channel, complementing traditional channels. Another extrapolation on the QVE is concentrating particularly on quantum applications in the vehicular ecosystem, which revealed the focus on the impact of quantum in emerging software-defined vehicles, their function demands, and vehicular security via subscription models.

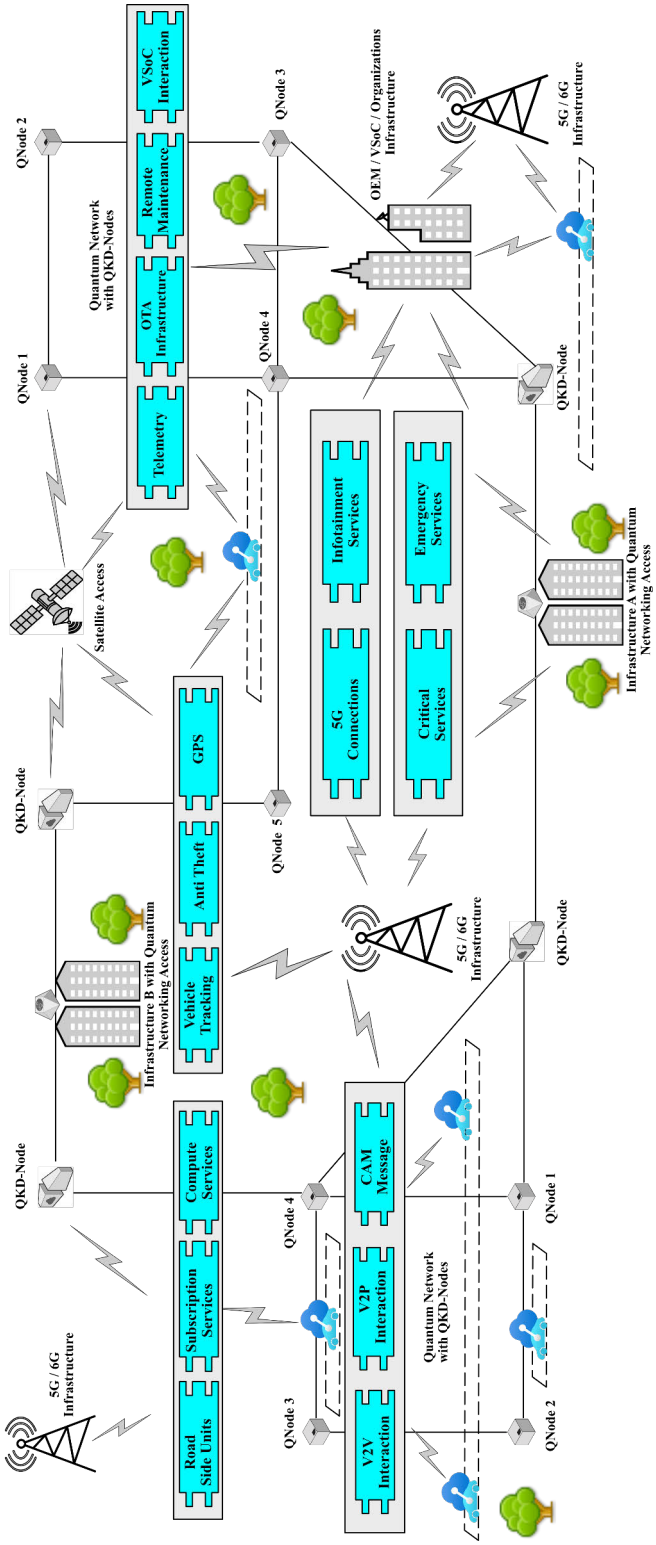


Figure 14. Quantum Vehicular Ecosystem.

4.2.2 QVE Deductions

The demand for vehicular security improvement in the transition to fully connected, intelligent, and autonomous vehicles has prompted the need for enhanced security dynamism, adaptability, and awareness [87]. Furthermore, the gradual dynamics and emergence of software-defined vehicular solutions will evolve and traverse further in the future years. Hence, the importance of security-oriented software-defined deployment (SoSDD) in software-defined vehicles (SDVs) increases as we approach the quantum vehicular era. From a QVE, it is deduced that quantum technological applications and quantum-like modeling come together to enhance the vehicular ecosystem, with security as the primary focus. Due to security features, full life-cycle management (FLcM) in a quantum vehicular ecosystem necessitates security characteristics and properties that can be flexibly managed in a decoupled in-vehicle configuration and external security infrastructure. Thus, software containerization plays a crucial role in ensuring FLcM security, bridging the gap between OEM infrastructure and external resources required for an SDV to transition to a service-oriented model. This specifically evokes services such as personal data and privacy protection, creating opportunities for organizations to explore. For example, autonomous vehicles would collect a large amount of personal data, such as the driving behavior and habits of their users. Manufacturers, service providers, or other entities often need to manage and monitor these vehicles remotely. Intelligent vehicles in recent years have also seen emergency services and other convenient services becoming a critical component in the case of accidents or other emergencies. When combined with other avenues, these not only present a multifaceted vehicular ecosystem that is entrenched in security challenges but also provide reasons to utilize them in a wide range of situations and avenues that align with service orientation. Thus, these challenges could also present different opportunities for organizations and OEMs, given that the signs are visible with each vehicle shipped, as are the features associated with remote management applications and eSIM capabilities.

As we transition from coupled monolithic software and hardware, a flexible in-vehicle applicational interaction with external resources could aid in the integration of diverse functionalities, potentially extending vehicles' FLcM. As discussed in [88] and others in previous sections, decoupled software and hardware have a higher probability due to limited hardware dependency, which makes integration more flexible and requires fewer changes to different hardware. A software-defined vehicular network often operates with a centralized model governed by a central controller. It illustrates an emphasis on ring in-vehicle topology, contrary to a mesh that offers much redundancy and multiple security access points at the same time. Nonetheless, a central controller in software-defined vehicular security is also not ideal without any form of redundancy, as it then becomes a single point of failure. Furthermore, losing security-beneficial features and traits of coupled hardware and software brings

up some problems, as shown by [89]. Coupled software and hardware often necessitate the verification and confirmation of changes and modifications, thereby potentially enhancing security.

In that aspect, the application of quantum key distribution in autonomous vehicles offers significant benefits in terms of security, privacy, and trust. By ensuring the authenticity, integrity, and confidentiality of the information being exchanged and stored in autonomous vehicles, quantum key distribution can play an important role in the development of a safe and secure autonomous vehicle ecosystem. We can increase the reliability of these communication channels by using quantum key distribution to encrypt the communication between autonomous vehicles and other entities. This is due to the fact that quantum key distribution guarantees the integrity of the transmitted information, preventing any corruption or compromise during transmission. In the proposal [90], for example, the changed SDN scheme lets the main SDN controller hand off the job of managing and checking keys for the Electronic Control Units (ECUs). This process could include switches and the distribution of quantum keys. The authors of [91] also expressed similar examinations in a quantum-aware SDN.

Another dimension of all this is the utilization of the above through a service-oriented infrastructure where KaaS and DaaS, for example, could be a service offering that caters to data related to the security and privacy of systems, on one side, and the safety of users, on the other side [92]. The data involved could play a significant role in developing novel analytics solutions, as well as serving as a catalyst for marketing, AI prediction, and forecasting engines that drive organizational decisions and investments. However, as acknowledged in [92], security requirements that fulfill these forms of interactions must be robust. Lin et al. [93] describe this best by saying that people are no longer only satisfied with raw data as a service. Instead, people want to gain the insights behind the data.

4.2.3 Experimentation of Quantum Key Distribution

The designed architecture for this experimental implementation is based on two communicating parties: party **A: Alice** and party **B: Bob**. A third party **E: Eve** is introduced in proving the premise of the unconditional cryptographic secrecy and the effects of tampering. Thus, two communication channels and an error detection channel were used in this context. The error detection channel was for the purpose of summing up the estimates of errors on the two channels. A classical channel is used for communication characteristics and properties that pertain to initial communication parameters, while the second channel, which is a quantum channel, is used for a similar purpose. However, on the quantum channel, two simulation scenarios were used: the presence and the absence of an eavesdropper, referring to simulation models in Figure 15 and Figure 16 respectively.

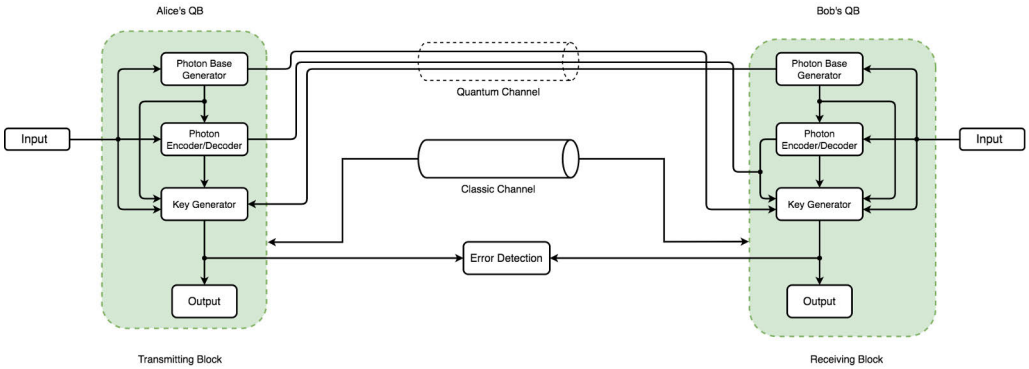


Figure 15. Simulation model design used for simulating an instance with the absence of an Eavesdropper (Eve's Quantum Block)

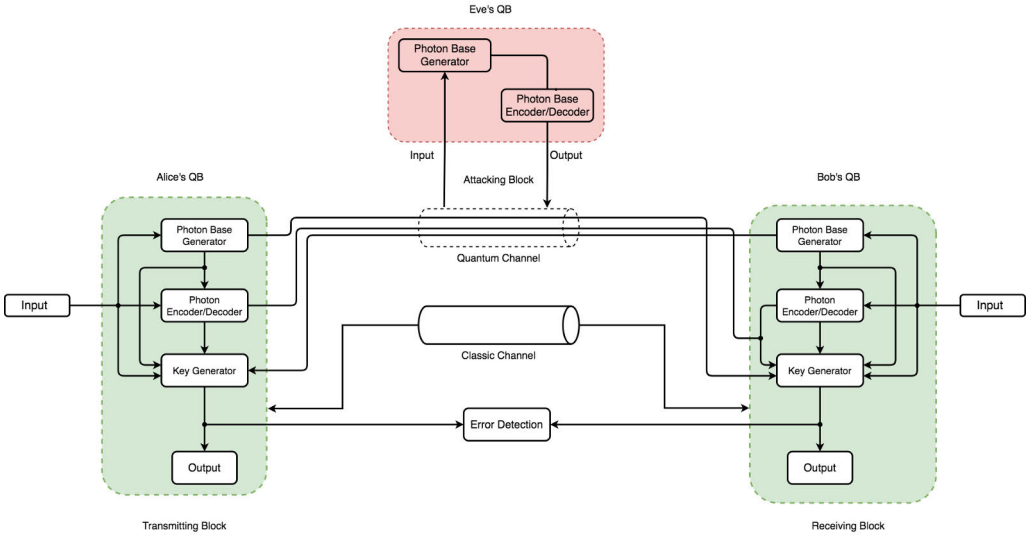


Figure 16. Simulation model design used for simulating an instance with the presence of an Eavesdropping(Eve's Quantum Block)

Experiment III: Proof-Of-Concept

The simulation models in each scenario in Figure 15 and Figure 16 depict Alice and Bob, referred to as a quantum block(QB). Depending on who is sending or receiving, either party can fulfill these roles. In this specific instance, Alice is the sender, and Bob is the receiver, representing the transmitter and receiver, respectively. In each QB, there are code-based specific functionalities designed and developed in Python 3 on a Linux-based platform. Alice and Bob have a Photon-Base Generator(PG_b), Photon-Base Encoder/Decoder (PE/D_b), and a Key Generator(KG_b) component

with an output in their quantum block except for **E: Eve** in simulation model II of Figure 16. On that same model, the purpose of Eve and its QB is to mimic an intercept and re-transmission attack over the quantum channel. This is to fulfill the requirement of an eavesdropper, as the purpose of the model requires eavesdropping (Eve's Quantum Block) on transmission tempering.

Table 3. Initial parameter used in the simulation.

Parameters	Values	Units
Qubit length	256	bits
Sender's bit probability	0.5	percentage
Receiver's bit probability	0.5	percentage
Attacker's bit probability	0.5	percentage
Error threshold	0.11	percentage
Error detection sample length	128	bits

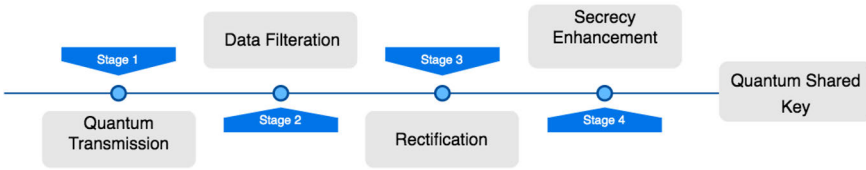


Figure 17. Main simulation procedure.

Alice and Bob agree on initial parameters in Table 3, on which their communication would be based. The sender **A** begins an encoding process by preparing a random bit (photons) stream sent to PG_b in choosing a polarization for each single-photon (quantum state) to begin the communication process within its QB. With the output received by **B** on the quantum channel, its QB undertakes the required operations illustrated in Figure 17. A communication is then initiated to **A** from **B** on the classical channel to relay the QB outputs. Both parties now make known to each other their polarization bases measured from the photon pulses sent with total secrecy and elimination of any leakage. Communication is re-established on the classical channel to confirm each other's results after comparing each other's qubits and polarization states. The results of this comparison are shown in Table 4 to represent the simulation scenarios and their attributing error threshold and single-photon base measurement mismatch. It is apparent from Table 4 that the result on both sides is then the final shared-key, which both parties had equal key length and matched polarization photon bases with a cumulative error rate less than the error threshold for the eavesdropper's absence. However, the opposite happened with the presence of the

eavesdropper as a mismatch and error rate greater than the error threshold indicated that Heisenberg's theorem and the no-cloning principle are breached (presence of an eavesdropper). Resulting in unequal key length as shown in Figure 18.

Table 4. Comparison of base parameters used and obtained results from the two main simulation instances.

Parameters	Normal	Eavesdropping
Initial bits – (**bits**)	256	256
Final key length – (**bits**)	54	36
Error correction rate – (**%**)	0.2421875	0.265625
Eavesdropper rate – (**%**)	0.04296875	0.125
Party A, B bit probability – (**%**)	0.5	0.5
Eve bit probability – (**%**)	0.5	0.5
Base mismatch – (**%**)	0.546875	0.5234375

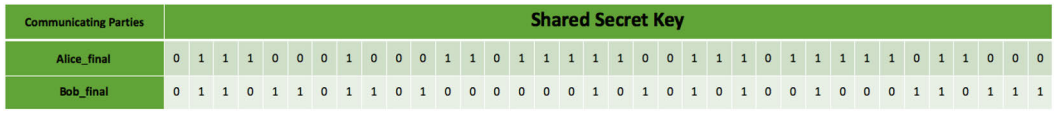


Figure 18. Sender and Receiver final shared key mismatch with Eavesdropper presence.

4.3 Seaming Security Dependency-Chains (SSDC)

In the previous chapters, research question **RQ1** systematically explicated the problems, challenges, and limitations in automotive cybersecurity. Research questions **RQ2 and RQ3** addressed the answers to these challenges through experiments, simulations, real-world tests, and scenarios. In answering these research questions, certain characteristics and properties were observed that led to further investigation and experiments. Leading to research question **RQ4** and its answers presented in this section as a result. This section explored these challenges and limitations, which were investigated further with an emphasis on comprehending the observed security interactions and relationships within and between attributing causalities associated with these challenges and limitations. To do so, the experiments performed in previous sections were revisited with associated data reanalyzed for security interactional relationships. The answers to research question **RQ4** are therefore systematically broken down into segments. The underlying premise of these security causalities is first presented to build hypotheses. These hypotheses are clarified in the subsequent sections of this result.

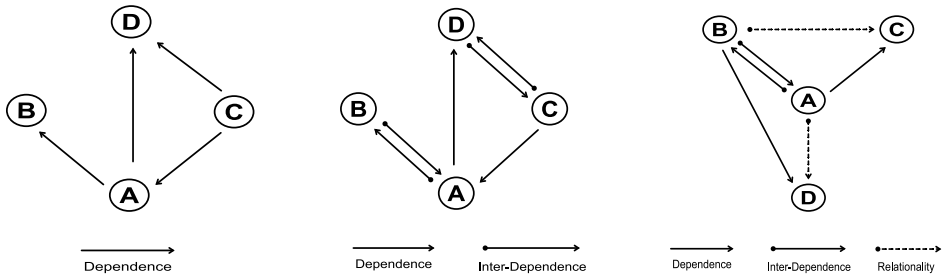
4.3.1 Fundamental Premise

Interactions are fundamental to the universe in every aspect, from how society operates to the fabric of all that exists within. Interactions are dynamic due to several facets constituting the how, the manner in which they occur, and the attributing characteristics and properties that shape the interaction itself. Technology is not new to interactions, and neither are advancements on which society is built. There exist borders, boundaries, sections, and segments that characterize each technological advancement as either a homogeneous, heterogeneous, or hybrid functional entity on which interactions can be categorized as ecosystems. Ecosystems with diverse interests that may or may not share similarities, characteristics, and properties then act as the building blocks by which internal and external interactions are governed. One such interaction that keeps privacy, safety, and isolation amid all these dynamic and adaptive evolutions of these interactions is security. Thus, interactions influence and shape the manner in which security as a gatekeeper is implemented and designed, as interactions by themselves can be influenced and impacted in the same manner. Influencing or impacting how technological advancements interact can be used as a double-edged sword for either the betterment or detriment of society due to the inherent dependencies, inter-dependencies, and relationalities within associations, attributions, and beyond. For that matter, the concept of **Seaming Security Dependency-Chains** (SSDC) is introduced while answering the research question **RQ4**. The building blocks - dependency, inter-dependency, and relationality are classified as the fundamental premise of this concept with emphasis on security, and

are addressed through security-seams and security-chains.

Security-Seams and Security-Chains

All interactions begin or originate from one point and terminate at one specific point. Multiple interactions in a sequence or series follow this form of perspective, but are joined to form a chain. Such a chain can also be joined into chains of interactions in any proportion of length or width. Thus, in the context of security, interactions associated with or attributed to the characteristics and properties of this scope form a security-chain. In a security-chain, the interactions within meet to create a seam, differentiating the characteristics, properties, and behavioral tendencies of each interaction. Therefore, a ”seam” refers to where interaction between entities and edge-to-edge interwoven elements meet across various dimensions. ”Seams” are evident in diverse security circumstances, scenarios, and contexts. Although they retain the same fundamental principle of interaction, security-seams then becomes the edge or the junction at which two or more security contexts meet or interact. Consequently, security-chains fundamentally derive from seams and interactions, define, impact, and influence security postures across various aspects. For example, vehicular security in their ecosystems, interactions, and associated technologies through dependence, inter-dependence, and relationality. Thus, security-seams are essential, influencing quality and performance, which rely on security properties, characteristics, infrastructure types, and situations, encompassing seam strength and efficiency. These are referred to as the security traits from this section onward.



(a) Dependency dynamics.

(b) Inter-dependency dynamics.

(c) Relationality dynamics.

Figure 19. Security interactions and relationships through seams and chains from dependencies, inter-dependencies, and relationalities.

Dependency is a circumstance in which the security maturation and evolution of an entity or groups of security-related entities are either subjective or tied to the growth and expansion of another [94]. Unlike dependency, where the flow of influence is a one-way function to the benefit or detriment of the dependent, inter-dependencies have two dependency instances flowing in both ways. Indicating that

both parties are dependent on the security maturation and evolution of each other. With dependency and inter-dependency interactions closely linked with each other, the concept of relationality extends these interactions. Thus, two security contexts or entities can be dependent or inter-dependent on each other without necessarily having direct interactions, but through relationality. Relative interactions in the form of security-seams and security-chains become complex and intricate when relationalities are meshed with overlapping, intersecting, and converging dependencies and inter-dependencies across multidimensional security contexts, as shown in Figure 19. Therefore, with referencing seams, specific terms such as dependency-chains, inter-dependency-chains, and relationality-chains exist within such complex and intricate relationships, denoting several overlapping and converging security-seams within each respective domain.

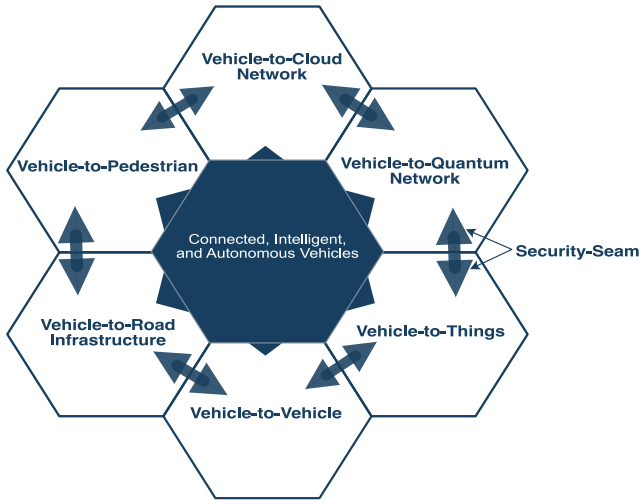


Figure 20. Illustration of interactions creating security-seams in a connected, intelligent, and autonomous vehicular ecosystem and its network.

For example, in the transition to fully connected, intelligent, and autonomous vehicular infrastructures and ecosystems with varying degrees of security autonomy, the impact, influence, and significance of dependency, inter-dependency, and relationality are vital to the holistic vehicular security. As the future of transportation envisions fleets of networked and managed connected, intelligent, and autonomous vehicles [95] on road networks, the security complexity and reliance on these created seams would advance. Complex in-vehicle hardware and software will interact independently and across networks with various technological domains in Figure 20. Vehicles capable of operating and participating in such networks will experience and exhibit dependence, inter-dependence, and relationship interconnectedness. The advent of the security effect in strong, relational, interwoven dependencies extends beyond connected, intelligent, and autonomous vehicles. Such dependencies, inter-

dependencies, and relationalities occur in communications and transactions between homogeneous, heterogeneous, and hybrid security postures and infrastructures.

4.3.2 Hypotheses and Definitions

Dynamic interactions with associated security traits and behavioral tendencies, in the connected, intelligent, and autonomous systems and their environments, would adapt and evolve. Adaptations would include attaining the new and evolving features, operational tendencies, the way and manner interactions are handled, and overall, security metamorphosis across and beyond, relative to smart, intelligent, and other autonomous devices, systems, and ecosystems. By so doing, it creates and maintains security characteristics, requirements, and external interactions. Some already visible with examples encompassing traffic conditions [96], collision awareness [97; 98], and pedestrian interactions [97; 99], safety [98] and security [100]. However, there are other characteristics and properties, such as fault tolerance [101], survivability [102], self-configuration and self-adoption [103], and coherence fault-recovery [104] significant in fully connected, intelligent, and autonomous ecosystems. Some elements of these characteristics and properties necessitate resources and access that surpass local vehicular engagements. Requiring External Infrastructural Resource management to address, process, and attain these traits while overseeing specific interrelations and dependencies among distinct assets. Thus, imposing contingent security requirements on one another yields both positive and negative security implications. Therefore, the first and second hypotheses state:

***Hypothesis* 1** (H1)**.** *Security-seams and security-chains in this transition increase in the move from the Society of Automotive Engineers level (SAE) 2 to 5 in a fully connected, intelligent, and autonomous vehicular ecosystem shown in Figure 21. Thus, influencing factors such as the demand for External Infrastructural Resources (EIR), security interactions, services, policies and legislation, security requirements, etc.*

***Hypothesis* 2** (H2)**.** *Seaming Security Dependency-chains (SSDC) occur when dependency, inter-dependency, and relationality overlap, intersect, or converge within a security context or framework, whereby the security posture is dependent on and relatively influenced by other security components due to inter-dependence or inter-relations or both, as depicted in Figure 22.*

***definition* 1.** *Thus, Seaming Security Dependency-Chains is the capturing of security dependencies, inter-dependencies, and relationalities as they intersect, overlap, and converge within a dynamic security interaction and context, individually and collectively, to advantageously enhance a security context.*

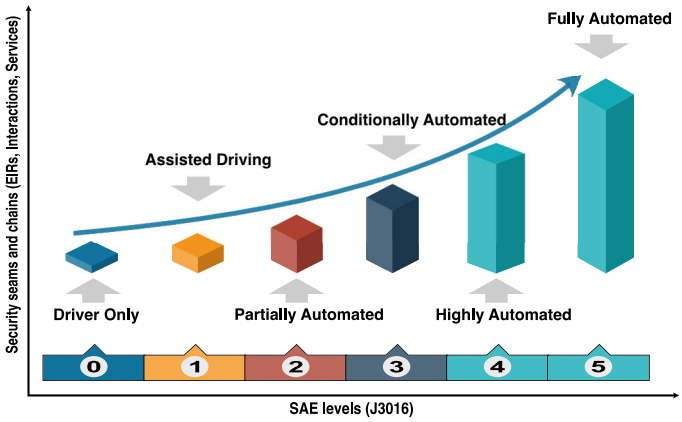


Figure 21. Progressive increase of External Infrastructural Resource (EIR) demands as a function of SAE levels.

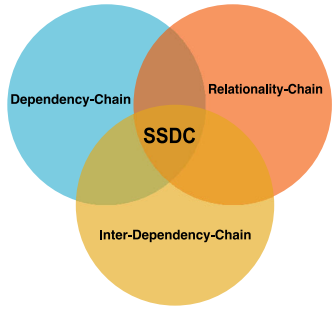


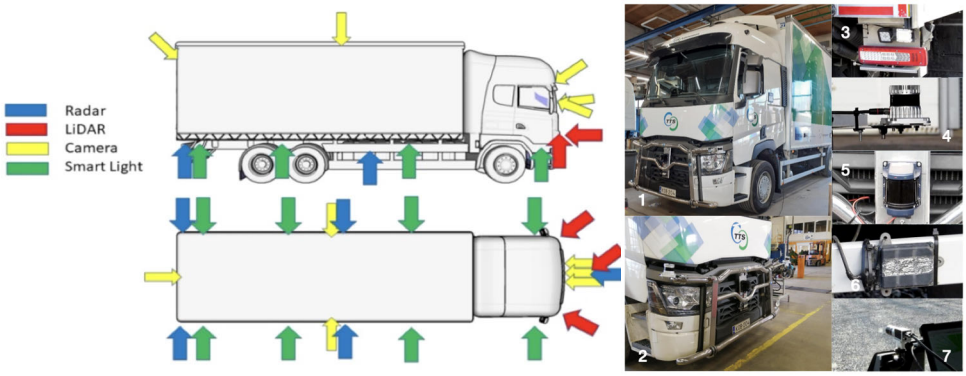
Figure 22. Illustration of overlapping and converging SSDC components from a security context.

Technologies evolve and mature, for example, those depicted in Figure 20. It is also certain that in this evolution, the automotive sector will adopt them upon their availability, usefulness, and security benefits. Establishment of vehicle-to-applicable technology across diverse domains, including pedestrian, cloud, peripheral, IoT, infrastructure, and quantum, will yield advantageous results for the transportation ecosystem in the long term, while introducing new dependency-chains, inter-dependency-chains, and relationality-chains fused in security-chains towards security-seams. Thus making the necessity of capturing security-chains related dynamics, of the three premises, significant as it comprises external infrastructure resources, including bi-directional telemetry, real-time security event monitoring, remote diagnostics, interfaces with remote operation centers, and additional components. Moreover, functionalities that utilize in-vehicle infrastructure, such as streaming, eSIM capabilities, and IoT devices that synchronize with vehicles and other apparatus, may require external resources. As they remain connected to the vehicle's network and ecosystem for consumer convenience or OEM-related purposes, they

also influence EIR enhancement.

4.3.3 Experimental Studies on Interconnectedness

In the re-visiting of the experiments, simulations, real-world tests, scenarios, and their associated data collected, the approach to answering the research question aimed to identify the critical components of security attributes that significantly impact, influence, and affect connected, intelligent, autonomous vehicle networks and ecosystems emphasized by the hypotheses. Security-seams and security-chains are in any ecosystem, and its infrastructure plays a role in the holistic security posture. For that matter, the self-aware cybersecurity architecture for autonomous vehicles, analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design, validating multi-sensor object tracking in Heavy-Duty Trucks with extended trailer dynamics for road traffic situations from a security perspective, quantum key distribution, and quantum vehicular ecosystem were approached from the perspective of the hypotheses.



(a) Multi-sensor mount positions **(b)** Sensor orientation

Figure 23. Hardware and sensor orientations with compute unit.

Experiments II: Multi-Sensor Security Interactions

With the IDS/IPS experiment already presented in Section 4.1.2, the multi-sensing from the security interaction perspective is discussed in this section. However, both of these experiments shared the same platform and resources. Therefore, all the software, hardware, and architectural details apply to this experiment. Thus, the primary objective of this experiment was to demonstrate the societal advantages of utilizing multi-sensor object tracking, emphasizing trailer dynamics, back-end parameters, and characteristics that influence decision-making strategies to improve safety. However, due to the result data and the dynamics of security interactions observed,

the study in the experiment now focuses on the interactions and sequences of security impact in each of the stages while drawing from hypothesis II and its definition. Thus, there are three blocks in this sequence of interactions: the data flow block, the compute-unit block, and the sensor-array block. Figure 24 showcases these blocks critical to the security operational parameters and characteristics using data flow as the means of path tracing analysis, while Figure 23 illustrates the positional orientations of the used sensor arrays. There are dependence, inter-dependence, and relationality chains that merge into security-seams in this experimental workflow within and among the blocks. The sensor arrays from Figure 24 with their orientation in Figure 23 operate independently and are not dependent, nor inter-dependent, on each other from an installation perspective. However, there are two main interfaces for the sensor arrays on which both sensors depend for configuration and settings that are pushed to individual sensors from the algorithms and custom applications developed to specifically operate unique tasks.

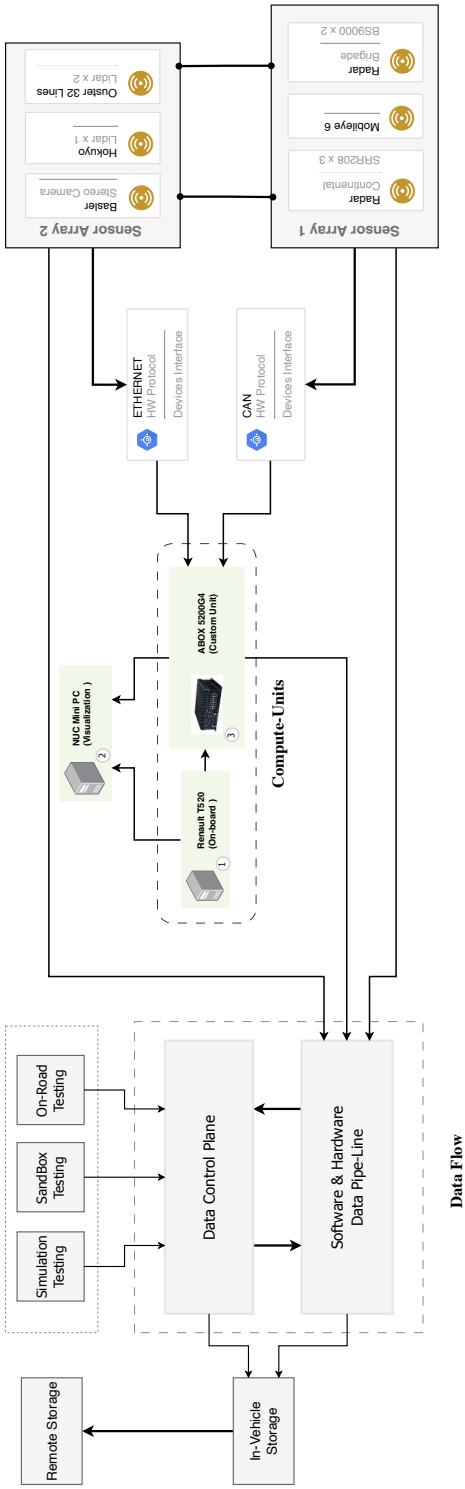


Figure 24. Multi-Sensor Security Interaction Observations

The data analyzed in this experiment are from the multi-sensor arrays based on three testing scenarios: simulation, sandbox, and on-road under both controlled environment and on-road traffic scenarios. Data accumulation and processing procedure follows the dataflow block in Figure 24 with details illustrated in Figure 25. It has a software and hardware data pipeline (SHDP) and a data control plane (DCP) interdependent on each other's actions and operation. In the SHDP, there is a DCP subcontrol plane ***data_source*** and ***raw_data_queue*** coordinating the data preparations, transformations, and queue-specific allocations with the ***worker_pools***. Interactional observations indicated the overlapping, converging, and intersection of specific interactions, which enacted and confirmed hypothesis II, indicating the presence of SSDC. With data consumers located in the DCP subscribing to the ***raw_data_queue***, the subsequent operations from that specific chain also meant that dependencies and inter-dependencies are created and are tied to that specific data pool. There are three decision-event blocks, **D1, D2, and D3**. The processed data queue plane (PSQP), depending on the subscriptions, dynamically shifts the dependencies, inter-dependencies, and relationalities that were visible across the data trace path for security interaction impacts. For example, a queue request such as **Q1 and Q2** via subscriptions from tracking consumers and fusion consumers feeds into the decision-event block **D3**. Further critical implications and influences were observed as well, security-wise. For example, fusion outputs feeding the decision-event blocks that the driver is dependent on during a right-turn are influenced and impacted by chains of dependencies and relationalities. Operational flow constraints such as latency, ***raw_data_queue*** bottle-necks, and others' security not only influenced the security interactions, but also shaped the actual interactions on which the processes are built.

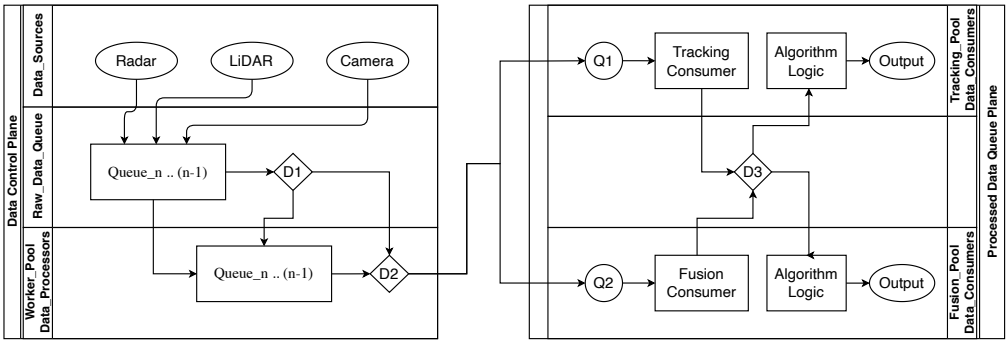


Figure 25. Multi-Sensor Data sequence and Consumption allocation

5 Discussion

In this chapter, the dissertation is approached as a complete perspective upon each research question answered in previous sections. It is presented in three main sections: Theoretical Implications, Practical Implications, and Reliability and Validity of the research results. The theoretical implication uses four case scenarios reflecting the consensus of proposed works and perspectives from the literature in the scientific community. Thus, reflecting on the theoretical foundations presented in Chapter 3 and the results as an outcome. However, the practical implications cater to society, organizations, companies, and all stakeholders to whom the results presented in this dissertation may concern. On the reliability and validity, the section delves into the degree to which the results reflect the underlying research construct, as to whether the results indicate what the dissertation purports to address.

5.1 Theoretical Implications

”Functionality” from the dissertation title in this context denotes the attributes and features of a vehicle that are intentionally crafted to achieve a particular objective or fulfill an intended design. Currently, automobiles possess numerous intrinsic and extrinsic functionalities that enhance passengers' comfort and convenience. With additional advancements anticipated in the future, and supporting the presented hypothesis 1, need for dynamic self-aware security accountability, robust security infrastructure such as QKD, and other security necessities within a quantum vehicular ecosystem. Functionalities may also encompass security features, infotainment, and interaction with the environment and its elements. For that matter, in the transition from the current SAE level to SAE level 5, the case scenarios used indicate the justification that these selected areas represent and capture the envisioned purpose in this transition.

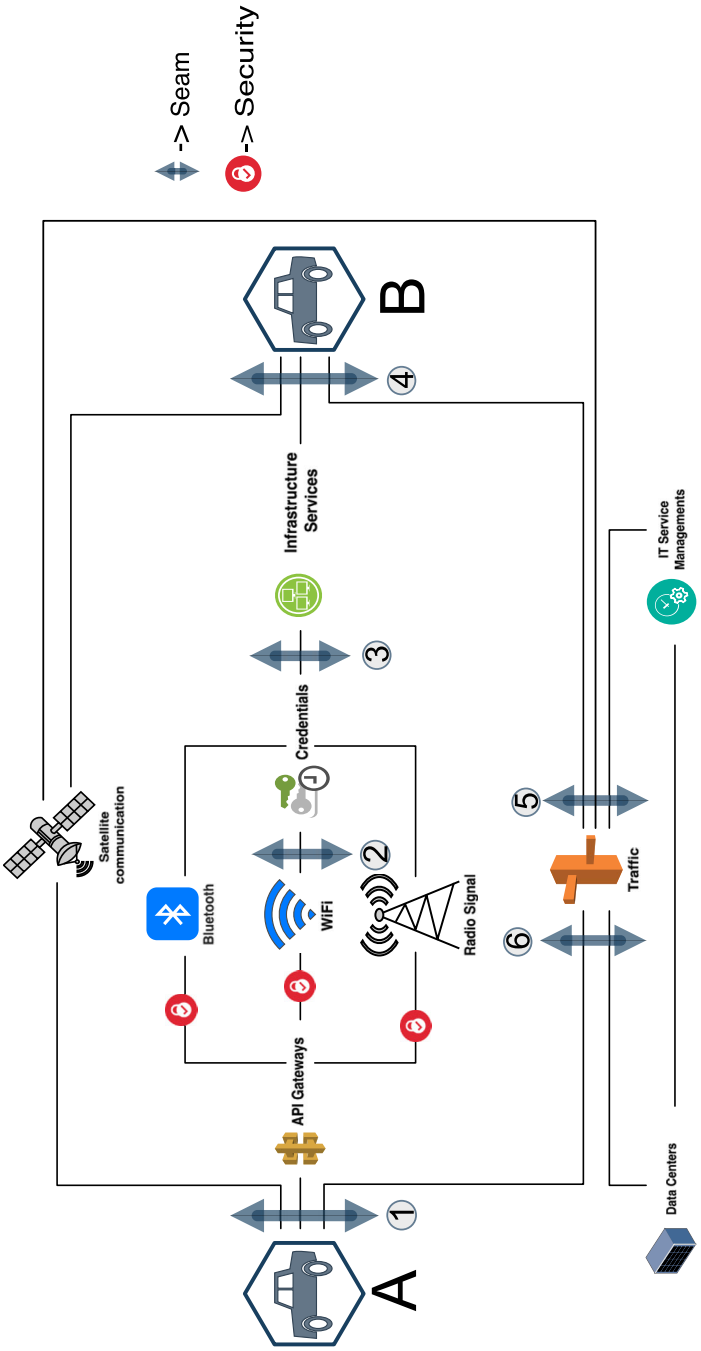


Figure 26. Case scenario I: Vehicle-to-Vehicle Communication (V2V).

Case Scenario I: Vehicle-to-Vehicle Communication (V2V)

The observations and results from experiments, simulations, and real-world tests from this dissertation have already established the potential impact, influence, and effect on other aspects of security in its totality. Thus, the significance of security interactions shows that technologies employing peer-to-peer transactions and node data exchanges enable seamless interaction between internal and external applications. Figure 26 depicts this peer-to-peer transaction via vehicle-to-vehicle communication featuring two vehicles that can interact as part of a fully integrated, intelligent, and autonomous vehicular network or ecosystem. There are six security-seams with any combinatorial matrix of security characteristics and properties from which a single-dimensional vehicular security plane infrastructure would not be beneficial. This is because technological evolutions over the past years have produced numerous multi-dimensional and yet beyond a single plane with hierarchies of combinatorial complex attacks, vulnerabilities, and security issues across each of these matrices of security-seams. The API gateways connecting to the access points, for example, are located between seams (1) and (2). The credentials associated with access points, including satellite communication, Bluetooth, WiFi, and radio transmissions, with communicating vehicles, if applicable, are situated between seams (2) and (3). The lower section includes a traffic light, which is essential to this specific communication scenario. Because the literature and the research community perceive it as a vital instrument in V2V communication. Seams (5) and (6) interface with vehicle A and the data center on the left and with the IT system management satellite communication on the right. The vehicle (B) establishes a connection with the infrastructural services through seams (3) and (4) in this instance.

In a vehicle-to-vehicle communication that uses the communication mediums located between the API gateway and credentials, the security infrastructural perception analysis has to comprehensively be self-aware and conscious of its in-vehicle and external environment on threats, not based on a static pre-defined security structure, but dynamically evolve and adapt to its environment context-wise and dynamic interactions-wise. Thus, the proposed hierarchical self-aware architecture with system-level accountability offers a foundational premise on which further extension can be derived by the research community as to the implementation of the process controllers and decision controllers.

In an ideal scenario, vehicle-to-vehicle communication envisions fully connected interactions between vehicles with no restrictions on the vehicular brand or model. Implying vehicles from various brands and models equipped with the capability to participate in such interactions are capable of doing so. This is where the results pertaining to security interactional dynamics and a reliable security accountability from the system-level, with a black-box for archiving security interactions and interplays, come into play, even beyond ideal situations. In addition to original equipment

manufacturer (OEMs) building ecosystems that can co-exist perfectly in their homogeneous context, security from the effects of security dependence, inter-dependence, and relationality is influential in such situations. As such, OEMs' in-vehicle security infrastructure discrepancies with hybrid, heterogeneous, and homogeneous vehicular models can result in security challenges without a dynamic security solution that puts real-time monitoring, analysis, reporting/support into effect.

When vehicle A tries to communicate with another vehicle through sending or receiving, it is, first of all, dependent on the security of the message sent, and vice versa. Hence, both are interdependent on each other's security implementation and posture. Vehicle A is also dependent on the security of the implemented APIs, while the security sanity of the access points is dependent on the API security and framework. In contrast, vehicle B receiving is not dependent on the API of vehicle A, but because the security of vehicle A relies on its API security, vehicle B is relatively dependent on the security of vehicle A based on attack transversal propagation. Signaling vehicle B may not be dependent on A's APIs, but attacks could be initiated on B due to vehicle A's weak or inadequate security implementation. For example, attacks such as GPS spoofing, VNET DDoS, and other network-based and vision-based attacks found in [64] and further classifications are also indicated in [105].

Given the heterogeneous nature of vehicles, communicating vehicles may require a common network, an identifier, credentials, and, if applicable, authentication aside from the ones indicated in Figure 5.1. One unique infrastructure that has been proposed in the literature to handle such security instances is traffic light infrastructures. They are stationary and easily accessible to vehicles within such communication ranges and radii. In such an instance, the broadcast information is sent to the traffic light system, and other vehicles can then receive the relayed information or message. Therefore, the vehicle's security level relies on the relayed messages, while the traffic light system relies on the broadcast messages and, if factored in, the satellite communication. There has also been proposed work on the use of quantum key distribution for the security of V2V communication, and one possible avenue is the combination of satellite communication and traffic light infrastructures.

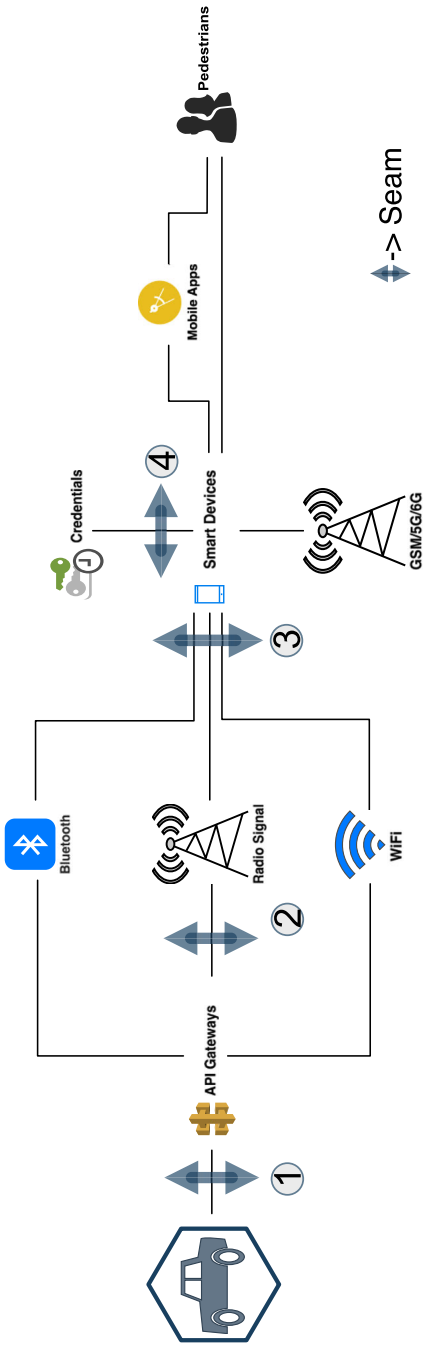


Figure 27. Case scenario II: vehicle-to-pedestrian (V2P).

Case Scenario II: Vehicle-to-Pedestrian (V2P)

The concept of vehicle-to-pedestrian (V2P) interaction and communication centers on enhancing pedestrian safety in many situations, including those outlined in [8]. The concept entails interactions between pedestrians and vehicles that are devoid of bias or discrimination. Therefore, collision avoidance between automobiles and pedestrians can be accomplished by the utilization of cooperative awareness messaging (CAM), corroborated by [97; 106]. V2P aspires to improve pedestrian vigilance and cautious awareness in crucial situations, applicable to both drivers and all road users capable of utilizing CAM, as exemplified in Figure 27. However, this form of interaction has security challenges that span across privacy, authenticity, non-repudiation, and others. With the first segment numerically designated security-seams analogous to case scenario I on seams (1) through (3), APIs and other vehicular infrastructures have exhibited security challenges in recent years, as far as mobile applications and pedestrians' involvement is concerned.

In the second segment, pedestrians' reliance on smart devices might require a mobile application to interface, enable, and facilitate such connectivity. The smart device operates independently of the pedestrian and the mobile application, as the pedestrian depends on the precision of the messages they see or interpret. Thus, from a security standpoint, that functionality is short-lived without its appropriate security; the smart device and pedestrian emerge as intersecting, overlapping, and converging security contexts. For that matter, the research community does not only have to focus on functionality, but also on an appropriate dynamic solution that stems from accountability and limits static solutions addressing attacks such as Side-channel attacks, Sniffing [66], and adversarial deep neural networks specifically targeting [67; 68]. This form of communication in the scenario so far has accounted for a wide range of occurring interactions that dynamically evolve based on the security characteristics and properties of the parties involved. Without downplaying the security challenges each party attributes to, passengers and pedestrians alike will continue to use diverse heterogeneous devices to achieve their personal and corporate outcomes. As such, research into dynamic security solutions and conditionally secure communication channels pertaining to automotive cybersecurity for societal benefit falls within the research community.

These designed and presented case scenarios, based on the results, observations, and lessons learned throughout this research, are to systematically elaborate on various avenues the research community can extend these results and the dissertation. The case scenarios are also used as an advocacy to emphasize the need for a dynamic self-aware security with system-level accountability.

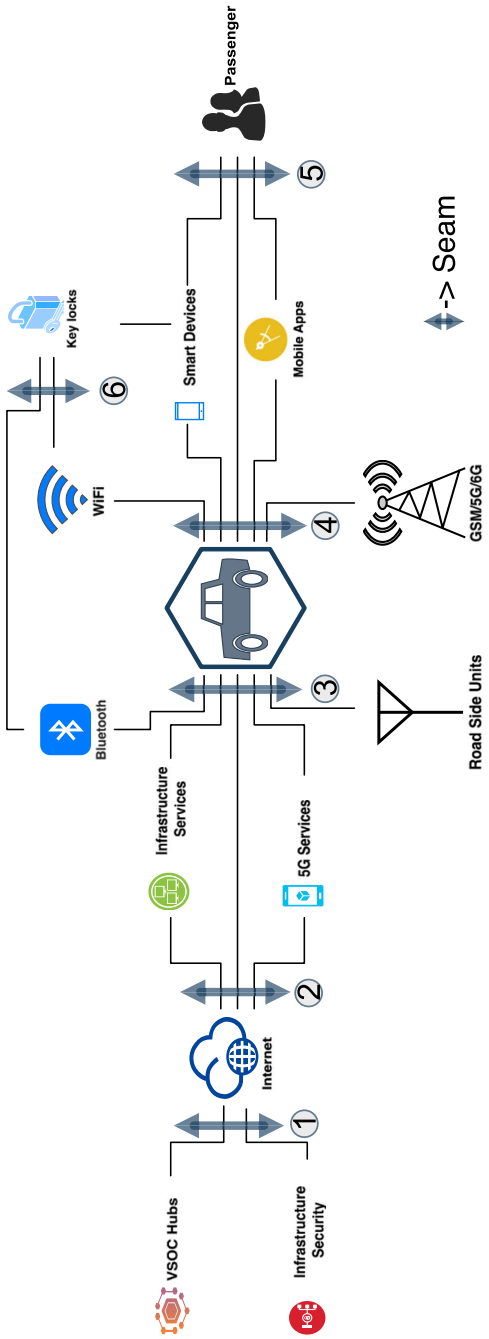


Figure 28. Case scenario III: Vehicle-to-Road Infrastructure (V2RI).

Case Scenario III: Vehicle-to-Roadside Infrastructure (V2RI)

Attack susceptibility and vulnerability landscape are widened in scope in the concept of vehicle-to-road infrastructure (V2RI) and external infrastructures. As it involves the interplay between vehicular communication and roadside units (RSU) [107], as well as infrastructures beyond the in-vehicle framework. This interaction involves vehicle-based ad hoc networks (VANETs) utilizing transmission broadcast and the IEEE 802.11p spectrum for communication, as depicted in Figure 28. It considers the vehicular interaction with external infrastructure resources, together with the two hypotheses, services, and other devices. This V2RI scenario additionally illustrates essential elements of vehicle-to-roadside infrastructures categorized with seams from (1) to (6). One aspect of V2RI communication in the transition to SAE level 5 is the increase in the security intricacies and complexities that arise. Evidence from the literature in contribution to the results of this dissertation has also shown that security seams and chains will always be created and evolved. Implying there will always be vulnerabilities for other researchers to discover, not forgetting that all these scenario instances are double-edged swords in the technological realm. Indicating as virtual operation center hubs and security infrastructures, among other unspecified instances, derived from seam (1) monitoring security interactional characteristics and properties, so would attackers.

The two service-oriented architectures existing at the seam (2), 5G and 6G mobile services, together with infrastructure services, are essential elements of today's vehicle communication. Between seams (1) and (2), internet access is denoted by direct connectivity to vehicles at seams (3), signifying changes in vehicular internet access. Beginning at the seam (4) on the other side of the case model to the right, mobile applications, smart devices, and the vehicle key fob at the seam (6) constitute a crucial component of vehicular interactions with external infrastructures. These are the principal entry points directly interfacing with both the in-vehicle security framework and external security elements. Nevertheless, the security context and posture of the vehicle are contingent, despite the application being independent of the vehicle. Smart gadgets equipped with intelligent features for automobiles have become integral to the passenger experience, akin to the scenario described in case scenario II, beyond seam (3). Automotive security is interdependent and relationally contingent upon smart gadgets and the security behaviors of passengers and owners. Likewise, key fobs possess security chains that link in-vehicle access points, electronic control units (ECUs), and connections to mobile applications, functioning interchangeably as electronic key fobs. Therefore, the premise for this reasoning is utilizing the results from Chapter 4 to aid introductions, developments, and management of security resources when designing dynamic, adaptive, and self-aware in-vehicle security infrastructures, advantageous in the way and manner SSDC components are structured. Emphasized by Seam (6, 3, and 4) in recent years, being

essential to vehicular security has caused numerous vehicular thefts. Other security incidents in the form of attacks may include attack types I and II described in [105] for flooding attacks, replay, etc. There are additional attacks based on communication and interactions from [108], including DoS, MiTM intercepts, Eavesdropping, etc.

Case Scenario IV: Vehicle-to-Compute (V2C)

To this point, a variety of case scenarios have already been used to demonstrate the impacts, benefits, and significance of security interactions, system-level accountable self-aware security design, and associated secure communication platform via QKD in various security contexts. This final case scenario considers the future perspective of fully connected, intelligent, and autonomous vehicular networks and their ecosystems. The security perspective of this scenario is extended to reflect the case scenarios I, II, and III, and the associated attack examples given.

The vehicle-to-computing infrastructures depicted in Figure 29 delineate three segments: quantum integration and computing, cloud computing infrastructure, and resources from both internal and external computing infrastructures. In the dissertation process, these three areas proved to play a significant role in a fully connected, intelligent, and autonomous ecosystem and its networks. Beginning on the left: Seam (1) pertains to internet access, data center access, and the virtual security operations center. A backbone to the communication infrastructure that can benefit from the use of quantum key distribution to conditionally guarantee communication secrecy among in-vehicle and external transactions. Seam (2) integrates with resources and infrastructure services. Seams (3) and (4) have virtual security operation centers, focusing on interactions with infrastructural security services, 5G/6G services, and IT service management infrastructures, which are critical to remote management of autonomous vehicles. Seam (6) emphasizes the influential seams, including mobile applications tailored to individual vehicle models, intelligent devices, resources, and quantum technologies. Satellite communication is evident in an overlapping security context in seam (5), whereas seam (8) addresses cloud interface API interactions. Seam (7) subsequently integrates with cloud computing systems, in-vehicle data, and information attributes concerning storage, interpretation, usage, and intelligent devices equipped to use these resources through specialized mobile applications. Quantum computing and its associated technologies also overlap at seams (4), (6), and (7).

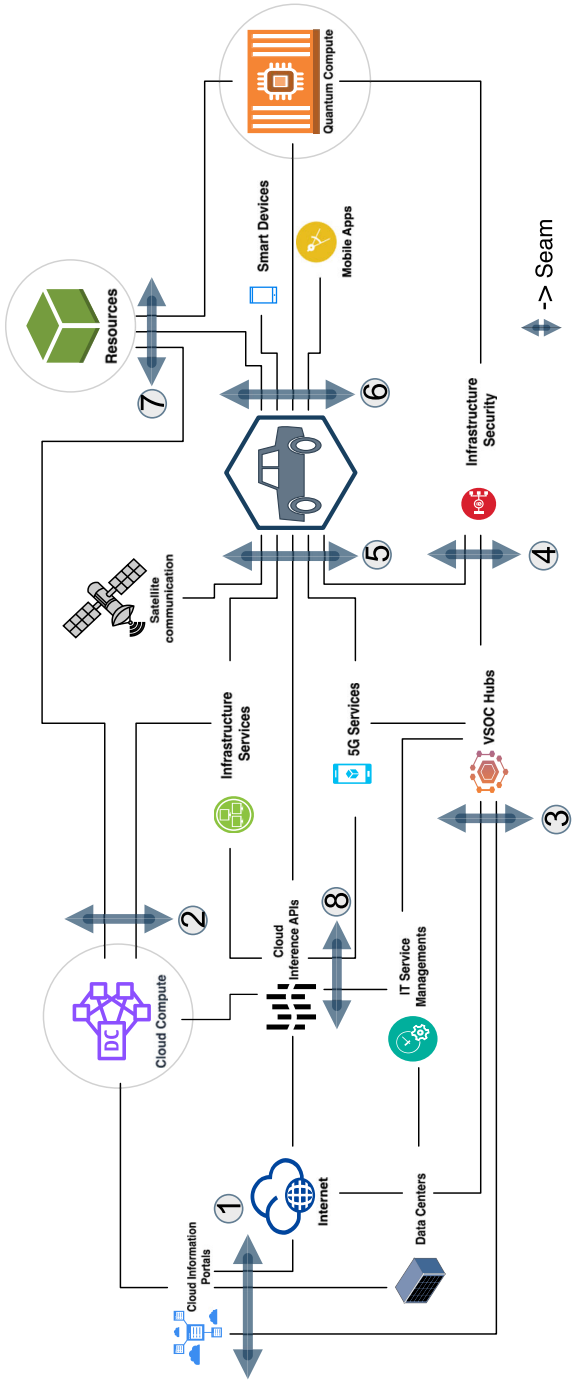


Figure 29. Case scenario IV: Vehicle-to-Cloud Compute (V2C).

A divergent perspective in this case scenario is that the research community has different views on the classification of cloud computing in the vehicular context. These divergences are built on where the computation tasks occur. Others argue that the vehicular cloud compute would reside in-vehicle, while others are of the view that it would reside externally. Nonetheless, the fundamental results of this dissertation have demonstrated that regardless of where vehicular computation resides, there is always going to be the need for a hierarchical system-level accountability security infrastructure, dynamic, adaptive, and context-aware to address the evolving threat landscape, focusing on vehicular security instances, contexts, and beyond. Security resource demand falls within relationality and inter-dependence based on how the resource is utilized, pulled, or pushed. In the case of a security-based subscription service to improve the overall security posture of a particular vehicle, the vehicle creates a security-seam that is dependent on that specific service. It also applies to security updates of operating systems or firmware, but not unidirectional telemetry. With resource transactions including data, information, subscription services, and many others in vehicles as virtual data centers on wheels, there are several critical impacts and influences on security dependencies, inter-dependencies, and relationality in contexts such as insurance claims, privacy, safety, and rights to generated transactions and streams of interactions, where the security-specific black-box is of significant necessity.

5.2 Practical Implications

As vehicular technologies progress and their related systems converge, the automotive industry will make use of diverse technologies to improve and enhance vehicles function-wise and capability-wise. Particularly in security, the intricacy of these security seams, chains, and interactions will become increasingly complex, due to increasingly computerized and automation-driven systems, with features and functions that extend beyond in-vehicle interactions and communications. Several vendor infrastructures and in-vehicle architectures are starting to rely on a bi-directional external infrastructure for resources and transactions, making seaming security dependency-chains offer an avenue for organizations, industries, vehicular security experts, researchers, and stakeholders to address security interactional impacts, influence, and effects to advantageously maximize security-related tasks that fall under such context and realm. For that matter, bring clarity to the implementations of a self-aware security in-vehicle accountability with the view that if stakeholders have much comprehension of their own security processes and operations in terms of security dependencies, inter-dependencies, and relationalities, a hierarchical system-level security emphasizing SSDC is more conscious to apply.

The sustainability of vehicular life-cycle management, continuity support, and the effects of technological advancements such as quantum technologies on secu-

rity posture (for example, updates, maintenance, and repairs) are critically important to vehicular ecosystems and their security infrastructures. Thus, prompting the stakeholders to start approaching vehicular security with a dynamic, adaptive, and self-aware perspective, which can be furthered in collaboration with AI to achieve context-awareness for all three critical perspectives presented in this dissertation. Dynamic interactions with a dynamic environment create fluctuating security characteristics, parameters, and requirements, compounded by legacy and external devices and infrastructures, which in a V2V, V2P, V2RI, and V2C, are critical. Vehicular interconnectedness is now clearly the trajectory and vision. As such, interactions that create intricate and complex interwoven security layers of in-vehicle to external communications need to be comprehended in terms of security seam series and sequence, and chains' hybridity and metamorphoses. Research into this area in the context of vehicular security is lacking in the vehicular ecosystem.

In a nutshell, vehicles have undergone steady advancements in terms of computing controllers and electronic safeguard units. Various areas, including security activities and events, have properties, characteristics, and operations that will always allow homogeneous and heterogeneous types of interactions within the vehicular ecosystem and its networks. Therefore, evident that the vehicle security aspects related to software development processes and techniques are crucial, of which APIs play key roles in facilitating various procedures and operations, including communication and transactions between the in-vehicle infrastructure and external resource needs. Thus, a dynamically self-aware security capable of adapting to the threat environment is essential when positioned as the in-vehicle security infrastructure.

5.3 Reliability and Validity

Societal norms dictate that accountability is often used when the clarity of resource distribution is in play. It is also employed to systematically distinguish interactions of various avenues clusterable for ease of traceability and flow pattern analysis. Accountability for society symbolizes transparency and precision associated with the perceived context. Thus, allow such a perceived context domain or realm to be classified as it is self-aware of its ins and outs. Ins and outs, being interactional complexities and the intricate flow dependencies, inter-dependencies, and relationalities. Being accountable in a security context in the cybersecurity space and spectrum does not necessarily translate to security self-awareness in the context of discussion for society, but it does establish a pathway to achieving such context-awareness security that people could appreciate amid the proliferation of technologies such as driving assistive hardware sensors [5], vehicles as social things, software and hardware associative [6], and as an extension to people's homes. For example, classification of roadside pedestrian safety impacted by the perceptions of hardware and software sensing ascribed to modules via Machine Learning [7] might be cautionary when

they malfunction, but not as significant as an in-vehicle security breach. As it is not as confined as the security parameters and characteristics that embody interactions related to several aspects of people's lives. It is so because society itself is considered a primary contributor to security, often clarified through the human element of security. Therefore, self-awareness security through system-level accountability coupled with SSDC is a derivable advantage for the security threat landscape, automotive cybersecurity challenges and limitations, and the future promises in cryptography, security design, security interaction analysis, etc., and the evolution of ecosystems.

The era of ubiquitously interconnected, intelligent, and self-driving automobiles approaches, and society will not only rely on its transportational benefits but also on its security. Thus, a catalysis that sees the security issues addressed via analysis in various modules, algorithms, operating systems, software, and hardware nodes. For that reason, vehicular security dynamics would still be a highlighted subject in research studies. Additionally, with the advocacy that numerous methodologies and implementations would subject security accountability in all aspects, with SSDC consideration in ongoing research. Particularly, concerning the parameters and attributes of in-vehicle systems that enable adaptive and dynamic compliance with security threats for societal benefit. Leading to impactful benefits on security challenges such as privacy risks, data thefts, road safety and life threats, sensor manipulations, risk management violations, infotainment system escalations, and many more.

6 Publication Summary and Contributions

The publication summary and author contributions in this chapter provide a summary of each publication within this compilation dissertation. The chapter breaks down the author's contributions from the original draft preparation, including the conceptualization and investigation, formal analysis and methodology, and associated details such as visual illustrations, review, and editing.

6.1 Publication I:

This publication examines the complex interactions of security dependence, interdependence, and relationality within various security contexts. These interactions create dynamic security chains and seams that influence development trends toward a fully connected, intelligent, and autonomous vehicular ecosystem. However, the existing literature has not adequately addressed the overall impact of security dependency, interdependency, and relationality within the vehicular ecosystem.

Therefore, the paper assessed these dynamic security interactions from both individual and collective perspectives. It introduces the concept of Seaming Security Dependency Chains (SSDC), which captures the intersections of security dependencies, inter-dependencies, and relationalities within a dynamic security context.

The work also employs case studies consisting of four scenarios: vehicle-to-vehicle, vehicle-to-pedestrians, vehicle-to-roadside units, and vehicle-to-compute infrastructures. These case studies highlight the crucial role of security chains and seams in identifying and understanding influential security factors. The SSDC concept is designed to be independent and can be scaled or adapted for any ecosystem involving multiple dynamic interactions. This adaptability can significantly enhance security design, optimization, implementation, and its evolution within the vehicular ecosystem.

Author Contributions: Akwasi Adu-Kyere introduced the concept of Seaming Security Dependency-Chains and undertook a formal analysis to examine the influences, impacts, and implications of security dependencies, inter-dependencies, and relational dynamics within the context of vehicular systems. His investigation into the SSDC was further developed through a focused analysis of interactions among

security nodes, predicated on three foundational premises.

The research methodology included a series of empirical experiments designed to explore multi-sensing security interactions and the implications of real-time Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), grounded in two proposed hypotheses. Throughout the original manuscript, Akwasi Adu-Kyere employed various visual aids to effectively illustrate, document, and elucidate the comprehensive nature of his work.

6.2 Publication II:

This publication systematically explores contemporary security deployments and implementations that are fundamentally reliant on cryptographic systems and their underlying infrastructures. Of particular significance is the emerging application of quantum principles, which is positioning itself as a transformative paradigm in secure communication.

The manuscript presents a comprehensive investigation into quantum technologies, with a concentrated focus on automotive cybersecurity and its myriad applications within a proposed Quantum Vehicular Ecosystem (QVE). It underscores the imperative for advanced security measures and tailored quantum applications specifically designed for the automotive context.

This work addresses a critical gap within the current literature by elucidating the concept of QVEs. We provide substantial insights, including an examination of quantum-like modeling approaches and innovative solutions poised to enhance vehicular security and its pertinent applications.

Author Contributions: Akwasi Adu-Kyere conceptualized a quantum vehicular ecosystem and initiated an in-depth analysis of quantum applications, informatics, and quantum-like modeling approaches pertinent to the domain of vehicular systems and their associated networks. His investigation encompassed the implications of quantum technology within the automotive sector, employing a comprehensive methodology aimed at addressing a spectrum of security applications. These applications focus on securing vehicular transactions and communications, both within vehicle systems and external infrastructure.

As the main contributor and author of the original draft, a significant emphasis is placed on the notion of quantum as a service, while also extending the discussion to encompass quantum sensing, quantum communication, quantum annealing, and navigation technologies. To effectively convey the proposed quantum vehicular ecosystem, visualizations were employed by the author, presenting both a service-oriented framework and its practical applicability within the field.

6.3 Publication III:

The publication commences by elucidating the significance of researching the contemporary era characterized by ubiquitously interconnected, intelligent, and autonomous vehicles, wherein advancements in security are progressively implemented. These enhancements are facilitated by rigorous security analyses conducted across diverse modules, algorithms, operating systems, as well as software and hardware components. Subsequently, the study implemented and investigated the deployment of a dynamic Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) in real-time scenarios, utilizing a Renault heavy-duty truck as a case study. The effectiveness of the security analysis methodology and its implementation is critically assessed, with particular emphasis on the integrity and reliability of the analysis derived from experimental data sources. The validation of the security framework adheres to a comprehensive approach, encompassing both inbound and outbound traffic management.

Author Contributions: Akwasi Adu-Kyere conducted a formal analysis on the effectiveness of IDS/IPS in vehicles by using a Renault T520 freight truck with an extended trailer in real-time with a custom in-vehicle compute unit. The methodology used was an experiment based on the European H2020 ECSEL project—PRYSTINE. As the main contributor and the author, the research investigation and conducted implementations dwelt on enhancing vehicular security by transitioning from static in-vehicle security infrastructure to a real-time, dynamic, and self-aware infrastructure. Further emphasis was also placed on how each of the soft and hard security nodes interacted with other components, such as the multi-sensing arrays, implemented security rules and environments, all of which were developed and implemented by the author Akwasi Adu-Kyere.

6.4 Publication IV:

This publication investigates the application of multi-sensing technologies in vehicles aimed at enhancing road and pedestrian safety. Extended trailers on freight trucks pose significant challenges during urban maneuvering, primarily due to restricted visibility. Therefore, this research focuses on the assessment and validation of extended trailer dynamics for heavy-duty trucks within various road traffic scenarios. The study emphasizes multi-sensor object tracking, trailer dynamics, backend parameters, and the characteristics that inform decision-making strategies. The methodology incorporates a custom in-vehicle computing unit, which operates in conjunction with the truck's onboard computer system, thereby facilitating comprehensive data analysis and insights.

Author Contributions: Akwasi Adu-Kyere is the main contributor and the author, in the writing of the original draft based on two ideological perspectives: Multisensing from security interactions and in a right-turn traffic scenario using a Renault T520 freight truck with an extended trailer. In the formal analysis of these two perspectives, it was aided by the methodology centered on experiments in the European H2020 ECSEL project—PRYSTINE. In his investigation, Adu-Kyere examined a multi-sensing object tracking technique, focusing on the dynamics of freight truck trailers in relation to pedestrian and road commuter interactions, alongside strategies for implementation. This research resulted in the development and execution of a multi-sensing tracking system programmed in Python 3, undertaken by the author. Furthermore, he designed custom scripts to facilitate three distinct testing environments: on-road testing, sandbox simulations, and controlled simulations. Comprehensive visual representations were employed to accurately illustrate each phase of the research, inclusive of the data collection processes.

6.5 Publication V:

The inherent dynamism of recent technological advancements in intelligent vehicles has seen multitudes of noteworthy security concerns regarding interactions and data. As future mobility embraces the concept of vehicles-to-everything, it exacerbates security complexities and challenges concerning dynamism, adaptiveness, and self-awareness. It calls for a transition from security measures relying on static approaches and implementations. Therefore, to address this transition, this work proposes a hierarchical self-aware security architecture that effectively establishes accountability at the system-level and further illustrates why such a proposed security architecture is relevant to intelligent vehicles. The article provides an outlook by (1) offering a comprehensive understanding of the Self-Aware Security Concept, with emphasis on its hierarchical security that enables system-level accountability, and (2) a comprehensive deep dive into each layer supported by algorithms and a security-specific in-vehicle Black-box with external VSOC interactions. In contrast to the present in-vehicle security measures, this architecture introduces characteristics and properties that enact self-awareness through system-level accountability. It implements hierarchical layers that enable real-time monitoring, analysis, decision-making, and in-vehicle and remote site integration regarding security-related activities.

Author Contributions: Akwasi Adu-Kyere proposed the idea of a self-aware cybersecurity architecture for connected, intelligent, and autonomous vehicles. With formal analysis dwelt on security through system-level accountability with the aid of a security-specific black-box. He investigated the systematic exploration of security dynamism, self-awareness, and adaptiveness in the vehicular ecosystem. Additionally, an in-depth examination of the need for appropriate security measures that match the dynamic nature of the vehicular security landscape was also conducted. Methodology used in this work, as the main contributor and writer of the original draft, focuses on the sub-components, such as security analysis and decision-making of the self-aware architecture that included algorithms, and the integration of a security-specific black-box. He extended this formal analysis and the methodology to also include security fail-overs and fall-backs. Visualizations created by Akwasi Adu-Kyere were used to illustrate and demonstrate each of these algorithms based on the components highlighted in the actual implementation using the custom compute unit with the Renault T520 freight truck.

6.6 Publication VI:

Autonomous “Things” is becoming the future trend as the role and responsibility of IoT keep diversifying. Its applicability and deployment need to re-stand technological advancement. The versatile security interaction between IoTs in human-to-machine and machine-to-machine must also endure mathematical and computational cryptographic attack intricacies. Quantum cryptography uses the laws of quantum mechanics to generate a secure key by manipulating light properties for secure end-to-end communication. We present a proof-of-principle via a communication architecture model and implementation to simulate these laws of nature. The model relies on the BB84 quantum key distribution(QKD) protocol with two scenarios, without and with the presence of an eavesdropper via the interception-resend attack model from a theoretical, methodological, and practical perspective. The proposed simulation initiates communication over a quantum channel for polarized photon transmission after a pre-agreed configuration over a classical channel with parameters. Simulation implementation results confirm that the presence of an eavesdropper is detectable during key generation due to Heisenberg’s uncertainty and no-cloning principles. An eavesdropper has a 0.5 probability of guessing the transmission qubit and 0.25 for the polarization state. During simulation re-iterations, a base-mismatch process discarded about 50 percent of the total initial key bits with an Error threshold of 0.11 percent.

Author Contributions: Akwasi Adu-Kyere designed and implemented a proof-of-concept using the simulation of two communicating scenarios. He investigated the BB84 protocol in the literature review and devised a methodology to aid the verification of both Heisenberg’s uncertainty and no-cloning principles. Formal analysis was conducted as he presented his results through visualizations. **Akwasi Adu-Kyere** is the author of the original draft and the main contributor.

7 Conclusions

This dissertation proposed and developed novel concepts, architecture, protocols, and algorithms for strengthening the security of the connected, intelligent, and autonomous vehicular ecosystem. The developed security architecture has distributed monitoring and analysis of security with system-level accountability decision-making, enabling self-aware and adaptive security control. The proposed seaming security dependency-chains concept is based on an in-depth examination of the impact and influence of dependency, interdependency, and relationalities of dynamic security interactions within the vehicular ecosystem. Quantum vehicular ecosystem is also introduced to highlight the role of quantum applications within the vehicular context. In addition, the quantum key distribution protocol was developed and simulated. The role of existing quantum technologies and their applications was further explored through the proposed quantum vehicular ecosystem.

Experiments, simulations, and real-world testing scenarios, and a custom-built compute unit housed in a Renault T520 freight truck were used in this research. These experiments covered a multi-sensing study of freight truck trailer dynamics in an urban setting and the security interaction, implications, and complexities at the backend and decision-making process in a right-turn. An IDS/IPS security interaction in real-time, extending the multi-sensing implementation and in-vehicle application, was designed and implemented as a dynamic security infrastructure for securing the truck. The IDS/IPS implementation in this context highlighted the monitoring aspect of the proposed self-aware architecture, focusing on security accountability. The IDS/IPS and multi-sensing environment were also used to study the dynamic security interactions in the seaming security dependency-chains experiment and observations that were based on data collected in simulations, on-road, and sandbox testing scenarios. The quantum key distribution to secure in-vehicle and external communications utilized simulations of two implementation scenarios mimicking the presence and absence of an eavesdropper. These unique implementations were used because they justified the uncertainty principle and the no-cloning theorem.

The first finding of the dissertation is a security architecture featuring hierarchical self-aware security that effectively establishes accountability at the system-level with an integrated security-specific black-box, which was corroborated by the experimental results. The results showed the relevance of dynamic, adaptive, and self-aware security as the hierarchical layers of the architecture enabled the implementation of

real-time monitoring, analysis, and decision-making. It has also enabled a scalable and modular approach, allowing for the uncomplicated incorporation of new features throughout the vehicle's life cycle. The Black-Box maximizes security traceability and extends utilization in privacy and safety-related realms. The proposed synchronization and integration of in-vehicle and virtual security operations further strengthen security measures by enabling remote security controls.

The second finding was that capturing security interconnectedness by examining the individual and collective impact of dependency, interdependency, and relationality through the proposed seaming security dependency-chains. This offers much comprehension on security interactional factors for security mapping and modeling, resource management, system integrations, end-to-end security improvements, and efficient iterations.

The third finding centers on a quantum vehicular ecosystem (QVE) as an outcome of both the quantum-related literature review and experiment. It revealed the need for enhanced security measures and specialized quantum applications in automotive cybersecurity proved to be warranted. The QVE approach addressed a significant gap in the existing literature, shedding light on valuable insights, including the importance of quantum-like modeling approaches and solutions that can improve vehicular security and its relevant applications. Quantum key distribution serves as a vital and fundamental aspect of the emerging fully connected, intelligent, and autonomous vehicular quantum ecosystem.

The last finding generalizable beyond the vehicular realm in this dissertation is the evolution of security seams and chains. Observations of security interactions based on the data collected implied the existence of interactions within the security analysis, decision-making process, and other components within the proposed architecture, and beyond in real-time. Following the data flow path in the security communications and transactions also revealed the tied relationship with security dependencies, inter-dependencies, and relationality chains and seams within intersecting, overlapping, and converging security contexts. The experiments and simulations revealed that over time, more security seams and chains will be created and evolve from dynamic security interactions.

The findings in this dissertation imply that without dynamic, adaptive, and self-aware security solutions that extend beyond in-vehicle interactions and communications, the benefits of dynamic features and functionalities will not align with the vision of intelligent mobility. As such, instantiating the factoring of the intersection, overlapping, and convergence of dependency, inter-dependency, and relationality in the realm of security studies is here to stay. Due to increasingly intricate in-vehicle security systems with their complex hybrid architectures, automation-driven features, amid artificial intelligence and machine learning. The other perspective of these findings is the opportunities revealed from a research standpoint. With the security prominence of characteristics and properties such as dynamism, adaptiveness,

and self-awareness, future research avenues, such as the integration of AI-driven cybersecurity models, are significant. Extendable to the security relational interplays of security and dynamism, security and adaptiveness, security self-awareness, and security and context-awareness, offering a vast range of future directional research avenues with quantum hardware feasibility tied to these research realms.

List of References

[1] Yinghui Zhang, Jin Li, Dong Zheng, Ping Li, and Yangguang Tian. Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice. *Journal of Network and Computer Applications*, 122(August):50–60, nov 2018. ISSN 10848045. doi: 10.1016/j.jnca.2018.07.017. URL https://doi.org/10.1016/j.jnca.2018.07.017https://linkinghub.elsevier.com/retrieve/pii/S1084804518302480.

[2] Guillermo Cueva-Fernandez, Jordán Pascual Espada, Vicente García-Díaz, Cristian González García, and Nestor Garcia-Fernandez. Vitruvius: An expert system for vehicle sensor tracking and managing application generation. *Journal of Network and Computer Applications*, 42:178–188, 2014. ISSN 10958592. doi: 10.1016/j.jnca.2014.02.013. URL http://dx.doi.org/10.1016/j.jnca.2014.02.013.

[3] Lu Tan and Neng Wang. Future internet: The Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, volume 5, pages V5–376–V5–380. IEEE, aug 2010. ISBN 978-1-4244-6539-2. doi: 10.1109/ICACTE.2010.5579543. URL http://ieeexplore.ieee.org/document/5579543/.

[4] Alexander M. Wyglinski, Xinming Huang, Taskin Padir, Lifeng Lai, Thomas R. Eisenbarth, and Krishna Venkatasubramanian. Security of Autonomous Systems Employing Embedded Computing and Sensors. *IEEE Micro*, 33(1):80–86, jan 2013. ISSN 0272-1732. doi: 10.1109/MM.2013.18. URL http://ieeexplore.ieee.org/document/6504448/.

[5] Michal Taraba, Juraj Adamec, Matus Danko, and Peter Drgona. Utilization of modern sensors in autonomous vehicles. In *2018 ELEKTRO*, pages 1–5. IEEE, may 2018. ISBN 978-1-5386-4759-2. doi: 10.1109/ELEKTRO.2018.8398279. URL https://ieeexplore.ieee.org/document/8398279/.

[6] De Jong Yeong, Gustavo Velasco-hernandez, John Barry, and Joseph Walsh. Sensor and sensor fusion technology in autonomous vehicles: A review. *Sensors*, 21:1–37, 3 2021. ISSN 14248220. doi: 10.3390/s21062140. URL https://www.mdpi.com/1424-8220/21/6/2140.

[7] Nicolas Scheiner, Florian Kraus, Nils Appenrodt, Jürgen Dickmann, and Bernhard Sick. Object detection for automotive radar point clouds – a comparison. *AI Perspectives*, 3:6, 11 2021. ISSN 2523-398X. doi: 10.1186/s42467-021-00012-z. URL https://aiperspectives.springeropen.com/articles/10.1186/s42467-021-00012-z.

[8] Akwasi Adu-Kyere, Ethiopia Nigussie, Jouni Isoaho, Jukka Ronkainen, and Arto Kyytinen. Validating multi-sensor object tracking in heavy-duty trucks with extended trailer dynamics for road traffic situations. *Procedia Computer Science*, 238:167–174, 2024. ISSN 18770509. doi: 10.1016/j.procs.2024.06.012. URL https://linkinghub.elsevier.com/retrieve/pii/S1877050924012481.

[9] Masoud Bagheri Ramiani and Gholamreza Shirazian. Ranking and Determining the Factors Affecting the Road Freight Accidents Model. *Civil Engineering Journal*, 6(5):928–944, may 2020. ISSN 2476-3055. doi: 10.28991/cej-2020-03091518. URL https://www.civilejournal.org/index.php/cej/article/view/2025.

[10] Et al., Xiao Li. Statistics of Dangerous Cargo Accidents during Highway Transportation. *CONVERTER*, 2021(5):53–63, jul 2021. ISSN 0010-8189. doi: 10.17762/converter.265. URL http://converter-magazine.info/index.php/converter/article/view/265.

[11] Manuel Alector Ribeiro, Dogan Gursoy, and Oscar Hengxuan Chi. Customer Acceptance of Autonomous Vehicles in Travel and Tourism. *Journal of Travel Research*, 61(3):620–636, mar 2022. ISSN 15526763. doi: 10.1177/0047287521993578. URL http://journals.sagepub.com/doi/10.1177/0047287521993578.

[12] Xiantao Jiang, F Richard Yu, Tian Song, and Victor C M Leung. Intelligent Resource Allocation for Video Analytics in Blockchain-Enabled Internet of Autonomous Vehicles With Edge Computing. *IEEE Internet of Things Journal*, 9(16):14260–14272, aug 2022. ISSN 2327-4662. doi: 10.1109/JIOT.2020.3026354. URL https://ieeexplore.ieee.org/document/9205310/.

[13] Abasi-amefon O. Affia, Raimundas Matulevičius, and Rando Tõnisson. Security risk estimation and management in autonomous driving vehicles. In Selmin Nurcan and Axel Korthaus, editors, *Intelligent Information Systems*, pages 11–19, Cham, 2021. Springer International Publishing. ISBN 978-3-030-79108-7.

[14] Tim Geppert, Stefan Deml, David Sturzenegger, and Nico Ebert. Trusted Execution Environments: Applications and Organizational Challenges. *Frontiers in Computer Science*, 4 (July):1–6, jul 2022. ISSN 2624-9898. doi: 10.3389/fcomp.2022.930741. URL https://www.frontiersin.org/articles/10.3389/fcomp.2022.930741/full.

[15] Qingyang Zhang, Hong Zhong, Jie Cui, Lingmei Ren, and Weisong Shi. AC4AV: A Flexible and Dynamic Access Control Framework for Connected and Autonomous Vehicles. *IEEE Internet of Things Journal*, 8(3):1946–1958, 2021. ISSN 23274662. doi: 10.1109/JIOT.2020.3016961.

[16] Felix Klement, Henrich C. Pohls, and Stefan Katzenbeisser. Change Your Car's Filters: Efficient Concurrent and Multi-Stage Firewall for OBD-II Network Traffic. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, 2022-Novem(Camad):19–25, 2022. ISSN 23784873. doi: 10.1109/CAMAD55695.2022.9966902.

[17] Zhiwei Chen, Chunhua Jin, Guanhua Chen, Ying Jin, and Hui Zong. A heterogeneous online/offline signcryption scheme for Internet of Vehicles. *Vehicular Communications*, 43:100635, 2023. ISSN 22142096. doi: 10.1016/j.vehcom.2023.100635. URL https://doi.org/10.1016/j.vehcom.2023.100635.

[18] Izhar Ahmed Khan, Nour Moustafa, Dechang Pi, Waqas Haider, Bentian Li, and Alireza Jolfaei. An Enhanced Multi-Stage Deep Learning Framework for Detecting Malicious Activities From Autonomous Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–10, 2021. ISSN 15580016. doi: 10.1109/TITS.2021.3105834.

[19] Yi Wang, Jing Xiao, Zhengzhe Wei, Yuanjin Zheng, Kea-Tiong Tang, and Chip Hong Chang. Security and Functional Safety for AI in Embedded Automotive System—A Tutorial. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 71(3):1701–1707, mar 2024. ISSN 1549-7747. doi: 10.1109/TCSII.2023.3334273. URL https://ieeexplore.ieee.org/document/10325613/.

[20] Mingming Yu, Zhen Guo, Shiwen Shen, Yuqiao Ning, Tianling Liu, and Dongqing Sun. An Intelligent Connected Vehicles Information Security Attack Matrix Model. *2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS)*, pages 82–86, 2023. doi: 10.1109/icpics58376.2023.10235357.

[21] Mohammed Lamine Bouchouia, Houda Labiod, Ons Jelassi, Jean Philippe Monteuuis, Wafa Ben Jaballah, Jonathan Petit, and Zonghua Zhang. A survey on misbehavior detection for connected and autonomous vehicles. *Vehicular Communications*, 41:100586, 2023. ISSN 22142096. doi: 10.1016/j.vehcom.2023.100586. URL https://doi.org/10.1016/j.vehcom.2023.100586.

[22] Bhaskar Pediredla, Kevin I.Kai Wang, Zoran Salcic, and Ameer Ivoghlian. A 6LoWPAN implementation for memory constrained and power efficient wireless sensor nodes. In *IECON Proceedings (Industrial Electronics Conference)*, pages 4432–4437. IEEE, nov 2013. ISBN 9781479902248. doi: 10.1109/IECON.2013.6699849. URL http://ieeexplore.ieee.org/document/6699849/.

[23] G. Snape. Automotive hacking – the cyber risk auto insurers must consider, insurance business america. insurance business, 2022. URL https://www.insurancebusinessmag.com/us/news/cyber/automotive-hacking--the-cyber-risk-auto-insurers-must-consider-416511.aspx. Available at:.

[24] Brian Blum. Cyberattacks on cars increased 225 *ISRAEL21c*, page 24– –2022, 2022. URL https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/#:~:text=The%20highlights%3A,attacks%20targeted%20back%2Dend%20servers. Online]. Available:.

[25] Upstream-Security. Global automotive cybersecurity report, upstream security, 2022. URL https://upstream.auto/2022report/. Available at:.

[26] Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Analyzing the effectiveness of ids/ips in real-time with a custom in-vehicle design. *Procedia Computer Science*, 238:175–183, 2024. ISSN 18770509. doi: 10.1016/j.procs.2024.06.013. URL https://linkinghub.elsevier.com/retrieve/pii/S1877050924012493. 0 citations (Crossref) [2024-07-22].

[27] Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3. *Sensors (Basel, Switzerland)*, 22(16): 6284, aug 2022. ISSN 14248220. doi: 10.3390/s22166284. URL https://www.mdpi.com/1424-8220/22/16/6284.

[28] Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Self-aware cybersecurity architecture for autonomous vehicles: Security through system-level accountability. *Sensors*, 23:8817, 10 2023. ISSN 1424-8220. doi: 10.3390/s23218817. URL https://www.mdpi.com/1424-8220/23/21/8817.

[29] P. Suresh, J. Vijay Daniel, V. Parthasarathy, and R. H. Aswathy. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In *2014 International Conference on Science Engineering and Management Research, ICSEMR 2014*, pages 1–8. IEEE, nov 2014. ISBN 9781479976133. doi: 10.1109/ICSEMR.2014.7043637. URL http://ieeexplore.ieee.org/document/7043637/.

[30] Rima Djellab and Mohammed Benmohammed. Securing encryption key distribution in wlan via qkd. In *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pages 160–165, 2012. doi: 10.1109/CyberC.2012.34.

[31] Akash Shrivastava and Manvendra Singh. A security enhancement approach in quantum cryptography. In *2012 5th International Conference on Computers and Devices for Communication (CODEC)*, pages 1–4, 2012. doi: 10.1109/CODEC.2012.6509349.

[32] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12:1012, 12 2020. ISSN 19438206. doi: 10.1364/AOP.361502. URL https://opg.optica.org/abstract.cfm?URI=aop-12-4-1012http://arxiv.org/abs/1906.01645http://dx.doi.org/10.1364/AOP.361502.

[33] Chia-Long Wu and Chen-Hao Hu. Computational complexity theoretical analyses on cryptographic algorithms for computer security application. In *2012 Third International Conference on Innovations in Bio-Inspired Computing and Applications*, pages 307–311, 2012. doi: 10.1109/IBICA.2012.9.

[34] E. Simion and N.-S. Constantinescu. Complexity computations in code cracking problems. In *24th International Spring Seminar on Electronics Technology. Concurrent Engineering in Electronic Packaging. ISSE 2001. Conference Proceedings (Cat. No.01EX492)*, pages 225–232, 2001. doi: 10.1109/ISSE.2001.931065.

[35] Ruhui Ma, Jin Cao, Dengguo Feng, Hui Li, Xiaowei Li, and Yang Xu. A robust authentication scheme for remote diagnosis and maintenance in 5G V2N. *Journal of Network and Computer Applications*, 198(December 2021):103281, feb 2022. ISSN 10848045. doi: 10.1016/j.jnca.2021.103281. URL https://doi.org/10.1016/j.jnca.2021.103281https://linkinghub.elsevier.com/retrieve/pii/S1084804521002770.

[36] Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya. A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, 40(July 2022):325–344, apr 2014. ISSN 10848045. doi: 10.1016/j.jnca.2013.08.004. URL http://dx.doi.org/10.1016/j.jnca.2013.08.004https://linkinghub.elsevier.com/retrieve/pii/S1084804513001793.

[37] Zhihua Wu, Engang Tian, and Hongtian Chen. Covert Attack Detection for LFC Systems of Electric Vehicles: A Dual Time-Varying Coding Method. *IEEE/ASME Transactions on Mechatronics*, 28(2):681–691, 2023. ISSN 1941014X. doi: 10.1109/TMECH.2022.3201875.

[38] Ilja Nastjuk, Bernd Herrenkind, Mauricio Marrone, Alfred Benedikt Brendel, and Lutz M. Kolbe. What drives the acceptance of autonomous driving? An investigation of acceptance factors from an end-user's perspective. *Technological Forecasting and Social Change*, 161(July):120319, dec 2020. ISSN 00401625. doi: 10.1016/j.techfore.2020.120319. URL https://linkinghub.elsevier.com/retrieve/pii/S0040162520311458.

[39] Kum Fai Yuen, Yiik Diew Wong, Fei Ma, and Xueqin Wang. The determinants of public acceptance of autonomous vehicles: An innovation diffusion perspective. *Journal of Cleaner Production*, 270:121904, oct 2020. ISSN 09596526. doi: 10.1016/j.jclepro.2020.121904. URL https://doi.org/10.1016/j.jclepro.2020.121904https://linkinghub.elsevier.com/retrieve/pii/S095965262031951X.

[40] Fahimeh Golbabaei, Tan Yigitcanlar, Alexander Paz, and Jonathan Bunker. Individual predictors of autonomous vehicle public acceptance and intention to use: A systematic review of the literature. *Journal of Open Innovation: Technology, Market, and Complexity*, 6(4):1–27, oct 2020. ISSN 21998531. doi: 10.3390/joitmc6040106. URL https://www.mdpi.com/2199-8531/6/4/106.

[41] Peng Jing, Gang Xu, Yuexia Chen, Yuji Shi, and Fengping Zhan. The determinants behind the acceptance of autonomous vehicles: A systematic review. *Sustainability (Switzerland)*, 12(5):1719, feb 2020. ISSN 20711050. doi: 10.3390/su12051719. URL https://www.mdpi.com/2071-1050/12/5/1719.

[42] Joseph B. Lyons, Thy Vo, Kevin T. Wynne, Sean Mahoney, Chang S. Nam, and Darci Gallimore. Trusting Autonomous Security Robots: The Role of Reliability and Stated Social Intent. *Human Factors*, 63(4):603–618, jun 2021. ISSN 15478181. doi: 10.1177/0018720820901629. URL http://journals.sagepub.com/doi/10.1177/0018720820901629.

[43] James M Anderson, Kalra Nidhi, Karlyn D Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A Oluwatola. *Autonomous vehicle technology: A guide for policymakers*. Rand Corporation, 2014.

[44] Richard A. Caralli, James F. Stevens, Lisa R. Young, and William R. Wilson. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical report, US Dept of the Air Force, may 2007. URL http://www.dtic.mil/docs/citations/ADA470450.

[45] Georg Franz Heinrich Macher, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Josef Kreiner. Sahara: A security-aware hazard and risk analysis method. In *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, pages 621–624. ., 2015. Design, Automation and Test in Europe Conference and Exhibition ; Conference date: 10-03-2015 Through 10-03-2015.

[46] Federico Mancini, Solveig Bruvoll, John Melrose, Frederick Leve, Logan Mailloux, Raphael Ernst, Kellyn Rein, Stefano Fioravanti, Diego Merani, and Robert Been. A Security Reference Model for Autonomous Vehicles in Military Operations. *2020 IEEE Conference on Communications and Network Security, CNS 2020*, 2020. doi: 10.1109/CNS48642.2020.9162227.

[47] Feng Luo, Yifan Jiang, Zhaojing Zhang, Yi Ren, and Shuo Hou. Threat Analysis and Risk Assessment for Connected Vehicles: A Survey. *Security and Communication Networks*, 2021:1–19, sep 2021. ISSN 1939-0122. doi: 10.1155/2021/1263820. URL https://www.hindawi.com/journals/scn/2021/1263820/.

[48] Mohamed Abdel-Basset, Abduallah Gamal, Nour Moustafa, Ahmed Abdel-Monem, and Nissreen El-Saber. A Security-by-Design Decision-Making Model for Risk Management in Autonomous Vehicles. *IEEE Access*, 9:107657–107679, 2021. ISSN 21693536. doi: 10.1109/ACCESS.2021.3098675. URL https://ieeexplore.ieee.org/document/9491157/.

[49] Yousik Lee, Samuel Woo, Yunkeun Song, Jungho Lee, and Dong Hoon Lee. Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis. *IEEE Access*, 8:120009–120018, 2020. ISSN 21693536. doi: 10.1109/ACCESS.2020.3004661. URL https://ieeexplore.ieee.org/document/9123897/.

[50] Roberto Passerone, Daniela Cancila, Michele Albano, Sebti Mouelhi, Sandor Plosz, Erkki Jantunen, Anna Ryabokon, Emine Laarouchi, Csaba Hegedus, and Pal Varga. A Methodology for the Design of Safety-Compliant and Secure Communication of Autonomous Vehicles. *IEEE Access*, 7:125022–125037, 2019. ISSN 21693536. doi: 10.1109/ACCESS.2019.2937453. URL https://ieeexplore.ieee.org/document/8812663/.

[51] Jin Cui and Biao Zhang. VeRA: A Simplified Security Risk Analysis Method for Autonomous Vehicles. *IEEE Transactions on Vehicular Technology*, 69(10):10494–10505, oct 2020. ISSN 0018-9545. doi: 10.1109/TVT.2020.3009165. URL https://ieeexplore.ieee.org/document/9140383/.

[52] Rhea C. Rinaldo and Timo F. Horeis. A Hybrid Model for Safety and Security Assessment of Autonomous Vehicles. *Proceedings - CSCS 2020: ACM Computer Science in Cars Symposium*, pages 1–10, dec 2020. doi: 10.1145/3385958.3430478. URL https://dl.acm.org/doi/10.1145/3385958.3430478.

[53] Mani Amoozadeh, Arun Raghuramu, Chen Nee Chuah, Dipak Ghosal, H. Michael Zhang, Jeff Rowe, and Karl Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, jun 2015. ISSN 01636804. doi: 10.1109/MCOM.2015.7120028. URL http://ieeexplore.ieee.org/document/7120028/.

[54] Ahmed Abdullahi, Tooska Dargahi, and Meisam Babaie. Vulnerability Assessment Of Vehicle To Infrastructure Communication: A Case Study Of Unmanned Ground Vehicle. In *2020 IEEE Globecom Workshops (GC Wkshps*, pages 1–6. IEEE, dec 2020. ISBN 978-1-7281-7307-8. doi: 10.1109/GCWkshps50303.2020.9367408. URL https://ieeexplore.ieee.org/document/9367408/.

[55] Mashrur Chowdhury, Mhafuzul Islam, and Zadid Khan. Security of Connected and Automated Vehicles. *Bridge*, 49(3):46–56, dec 2020. ISSN 07376278. doi: https://doi.org/10.48550/arXiv.2012.13464. URL http://arxiv.org/abs/2012.13464.

[56] Simona Gifei Cas. Aionoaie and Alexandru Salceanu. Autonomous and Electrical Vehicles Development using Optimized Processes Defined by Cyber Security and Safety Management System. In *2021 International Conference on Electromechanical and Energy Systems (SIELMEN)*, pages 257–261. IEEE, oct 2021. ISBN 978-1-6654-0078-7. doi: 10.1109/SIELMEN53755.2021.9600343. URL https://ieeexplore.ieee.org/document/9600343/.

[57] Tejasvi Alladi, Sombuddha Chakravarty, Vinay Chamola, and Mohsen Guizani. A Lightweight Authentication and Attestation Scheme for In-Transit Vehicles in IoV Scenario. *IEEE Transactions on Vehicular Technology*, 69(12):14188–14197, dec 2020. ISSN 0018-9545. doi: 10.1109/TVT.2020.3038834. URL https://ieeexplore.ieee.org/document/9261991/.

[58] Mostafa Anwar Taie, Mohammed Diab, and Mohamed ElHelw. Remote prognosis, diagnosis and maintenance for automotive architecture based on least squares support vector machine and multiple classifiers. In *2012 IV International Congress on Ultra Modern Telecommunications and Control Systems*, pages 128–134. IEEE, oct 2012. ISBN 978-1-4673-2017-7. doi:

10.1109/ICUMT.2012.6459652. URL http://ieeexplore.ieee.org/document/6459652/.

[59] Mahdi Dibaei, Xi Zheng, Kun Jiang, Sasa Maric, Robert Abbas, Shigang Liu, Yuexin Zhang, Yao Deng, Sheng Wen, Jun Zhang, Yang Xiang, and Shui Yu. An Overview of Attacks and Defences on Intelligent Connected Vehicles. *arXiv e-prints*, pages 1–36, jul 2019. URL http://arxiv.org/abs/1907.07455.

[60] Gourav Bathla, Kishor Bhadane, Rahul Kumar Singh, Rajneesh Kumar, Rajanikanth Aluvalu, Rajalakshmi Krishnamurthi, Adarsh Kumar, R N Thakur, and Shakila Basheer. Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities. *Mobile Information Systems*, 2022:1–36, jun 2022. ISSN 1875-905X. doi: 10.1155/2022/7632892. URL https://www.hindawi.com/journals/misy/2022/7632892/.

[61] J. Bekemeyer. Report: Identity Attacks a Top Cybersecurity Threat in 2022 - DBusiness Magazine. https://www.dbusiness.com/daily-news/report-identity-attacks-a-top-cybersecurity-threat-in-2022/, may 26 2022. [Online; accessed 2023-06-15].

[62] M. Plato. Rise in Identity-Based Attacks Drives Demand for a New Security Approach. https://www.sentinelone.com/blog/rise-in-identity-based-attacks-drives-demand-for-a-new-security-approach/, jun 29 2022.

[63] CrowdStrike. 7 Types of Identity-Based Attacks – CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/identity-security/identity-based-attacks/, 1 2023. [Online; accessed 2023-06-15].

[64] A. Khadka, P. Karypidis, A. Lytos, and G. Efstathopoulos. A benchmarking framework for cyber-attacks on autonomous vehicles. *Transportation Research Procedia*, 52(2020):323–330, 2021. ISSN 23521465. doi: 10.1016/j.trpro.2021.01.038. URL https://doi.org/10.1016/j.trpro.2021.01.038https://linkinghub.elsevier.com/retrieve/pii/S2352146521000703.

[65] Attlee M. Gamundani. An impact review on internet of things attacks. In *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015*, pages 114–118. Institute of Electrical and Electronics Engineers Inc., aug 2015. ISBN 9781479977062. doi: 10.1109/ETNCC.2015.7184819.

[66] Vrizlynn L.L. Thing and Jiaxi Wu. Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. In *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pages 164–170. IEEE, dec 2017. ISBN 9781509058808. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52. URL http://ieeexplore.ieee.org/document/7917080/.

[67] 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, dec 2021. ISSN 19410050. doi: 10.1109/TII.2021.3071405. URL https://ieeexplore.ieee.org/document/9397393/.

[68] Wenbo Jiang, Hongwei Li, Sen Liu, Xizhao Luo, and Rongxing Lu. Poisoning and Evasion Attacks Against Deep Learning Algorithms in Autonomous Vehicles. *IEEE Transactions on Vehicular Technology*, 69(4):4439–4449, 2020. ISSN 19399359. doi: 10.1109/TVT.2020.2977378.

[69] Stefan Covaci, Matteo Repetto, and Fulvio Risso. Towards Autonomous Security Assurance in 5G Infrastructures. *IEICE Transactions on Communications*, E102.B(3):401–409, mar 2019. ISSN 0916-8516. doi: 10.1587/transcom.2018NVI0001. URL https://www.jstage.jst.go.jp/article/transcom/E102.B/3/E102.B_2018NVI0001/_article.

[70] Eduardo J. S. Villasenor, Rui Loja Fernandes, and Roger Picken. Introduction to Quantum Mechanics. In *AIP Conference Proceedings*, volume 1023, pages 107–117. AIP, 2008. ISBN 9780735405462. doi: 10.1063/1.2958160. URL http://aip.scitation.org/doi/abs/10.1063/1.2958160https://pubs.aip.org/aip/acp/article/1023/1/107-117/821485.

[71] R. Friedberg and P. C. Hohenberg. What is Quantum Mechanics? A Minimal Formulation. *Foundations of Physics*, 48(3):295–332, mar 2018. ISSN 0015-9018. doi: 10.1007/s10701-018-0145-4. URL http://link.springer.com/10.1007/s10701-018-0145-4.

[72] G. Brassard. Brief history of quantum cryptography: a personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 19–23, 2005. doi: 10.1109/ITWTPI.2005.1543949.

[73] Michael Brooks. the Race To Find Quantum Computing'S Sweet Spot. *Nature*, 617:S1–S3, 2023. URL https://arxiv.org/abs/1902.02332.

[74] Tanya Rastogi, Vikas Hassija, and Vikas Saxena. Quantum communication: Concept, applications, and future outlook. In *ACM International Conference Proceeding Series*, pages 51–56, New York, NY, USA, aug 2021. ACM. ISBN 9781450389204. doi: 10.1145/3474124.3474131. URL https://dl.acm.org/doi/10.1145/3474124.3474131.

[75] Robert Coolman. What is quantum mechanics?, July 2021. URL https://scinerds.tumblr.com/post/658075954562908161/what-is-quantum-mechanics-by-robert-coolman.

[76] Deziel Chris. The famous physicist who discovered photons, 2022. URL https://sciencing.com/famous-physicist-discovered-photons-16203.html.

[77] Britannica Editors. "arthur holly compton". encyclopedia britannica, 6 Sep. 2025,. URL https://www.britannica.com/biography/Arthur-Holly-Compton. Accessed 9 December 2025.

[78] Alvaro Cintas-canto. Reliable Code-Based Post-Quantum Cryptographic Algorithms through Fault Detection on FPGA. *2023 IEEE Nordic Circuits and Systems Conference (NorCAS)*, pages 1–5, 2023. doi: 10.1109/NorCAS58970.2023.10305475.

[79] Ritik Bavdekar, Eashan Jayant Chopde, Ankit Agrawal, Ashutosh Bhatia, and Kamlesh Tiwari. Post quantum cryptography: A review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)*, pages 146–151, 2023. doi: 10.1109/ICOIN56518.2023.10048976.

[80] A. Aguado, D. R. López, A. Pastor, V. López, J. P. Brito, M. Peev, A. Poppe, and V. Martín. Quantum cryptography networks in support of path verification in service function chains. *Journal of Optical Communications and Networking*, 12(4):B9, April 2020. ISSN 1943-0620, 1943-0639. doi: 10.1364/JOCN.379799. URL https://opg.optica.org/abstract.cfm?URI=jocn-12-4-B9. 11 citations (Crossref) [2024-07-03].

[81] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, and Hong Guo. Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1):011318, March 2024. ISSN 1931-9401. doi: 10.1063/5.0179566. URL https://pubs.aip.org/apr/article/11/1/011318/3279669/Continuous-variable-quantum-key-distribution.

[82] Id quantique, the home of quantum-safe crypto, 2025. URL https://www.idquantique.com/. Accessed: 09-12-2025.

[83] John Prisco. Council post: Moving forward with the security of quantum key distribution, 05 2023. URL https://www.forbes.com/sites/forbestechcouncil/2023/05/22/moving-forward-with-the-security-of-quantum-key-distribution/?sh=44adaa383dde.

[84] James Dargan. 25 companies building the quantum cryptography & communications markets, 01 2021. URL https://thequantuminsider.com/2021/01/11/25-companies-building-the-quantum-cryptography-communications-markets/.

[85] Shouvanik Chakrabarti, Xuchen You, and Xiaodi Wu. ICCAD Special Session Paper: Quantum Variational Methods for Quantum Applications. *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, 2021-Novem:1–7, 2021. ISSN 10923152. doi: 10.1109/ICCAD51958.2021.9643519.

[86] Emmanuel Haven and Andrei Khrennikov. Editorial: Applications of Quantum Mechanical Techniques to Areas Outside of Quantum Mechanics. *Frontiers in Physics*, 5(NOV):1–2, nov 2017. ISSN 2296-424X. doi: 10.3389/fphy.2017.00060. URL http://journal.frontiersin.org/article/10.3389/fphy.2017.00060/full.

[87] Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Self-aware cybersecurity architecture for autonomous vehicles: Security through system-level accountability. *Sensors*, 23(21):8817, October 2023. ISSN 1424-8220. doi: 10.3390/s23218817. URL https://www.mdpi.com/1424-8220/23/21/8817. 0 citations (Crossref) [2024-07-08].

[88] 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)*, page 1–9, Kuala Lumpur, Malaysia, December 2023. IEEE. ISBN 9798350325041. doi: 10.1109/ICECIE58751.2024.10457489. URL https://ieeexplore.ieee.org/document/10457489/. 0 citations (Crossref) [2024-07-25].

[89] Sara Imene Boucetta and Zsolt Csaba Johanyak. Survey on security attacks in software defined vanets. In *2022 IEEE 16th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, page 000185–000190, Timisoara, Romania, May 2022. IEEE. ISBN 978-1-66548-125-0. doi: 10.1109/SACI55618.2022.9919595. URL https://ieeexplore.ieee.org/document/9919595/. 2 citations (Crossref) [2024-07-25].

[90] Ju-Ho Choi, Sung-Gi Min, and Youn-Hee Han. Macsec extension over software-defined networks for in-vehicle secure communication. In *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, page 180–185, Prague, Czech Republic, July 2018. IEEE. ISBN 978-1-5386-4646-5. doi: 10.1109/ICUFN.2018.8436963. URL https://ieeexplore.ieee.org/document/8436963/.

[91] Alejandro Aguado, V Martin, D Lopez, M Peev, J Martinez-Mateo, JL Rosales, F de la Iglesia, M Gomez, Emilio Hugues Salas, A Lord, et al. Quantum-aware software defined networks. In *42nd European Conference on Optical Communication, ECOC 2016: 42nd European Conference and Exhibition on Optical Communication*, page 188. QCrypt, 2016.

[92] Claudio A. Ardagna, Valerio Bellandi, Ernesto Damiani, Michele Bezzi, and Cedric Hebert. Big data analytics-as-a-service: Bridging the gap between security experts and data scientists. *Computers & Electrical Engineering*, 93:107215, July 2021. ISSN 00457906. doi: 10.1016/j.compeleceng.2021.107215. URL https://linkinghub.elsevier.com/retrieve/pii/S0045790621002081. 6 citations (Crossref) [2024-07-25].

[93] Haozhe Lin, Yushun Fan, Jia Zhang, Bing Bai, Zhenghua Xu, and Thomas Lukasiewicz. Toward knowledge as a service (kaas): Predicting popularity of knowledge services leveraging graph neural networks. *IEEE Transactions on Services Computing*, page 1–1, 2022. ISSN 1939-1374, 2372-0204. doi: 10.1109/TSC.2022.3145019. URL https://ieeexplore.ieee.org/document/9693263/. 2 citations (Crossref) [2024-07-25].

[94] Theotonio Dos Santos. The structure of dependence. *The American Economic Review*, 60(2):231–236, 1970. ISSN 00028282. URL http://www.jstor.org/stable/1815811.

[95] Chee Wei Lee and Stuart Madnick. Cybersafety approach to cybersecurity analysis and mitigation for mobility-as-a-service and internet of vehicles. *Electronics (Switzerland)*, 10(10):1220, may 2021. ISSN 20799292. doi: 10.3390/electronics10101220. URL https://www.mdpi.com/2079-9292/10/10/1220.

[96] Jin Cui, Lin Shen Liew, Giedre Sabaliauskaite, and Fengjun Zhou. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, 90, 2019. ISSN 15708705. doi: 10.1016/j.adhoc.2018.12.006.

[97] José Javier Anaya, Pierre Merdrignac, Oyunchimeg Shagdar, Fawzi Nashashibi, and José E. Naranjo. Vehicle to pedestrian communications for protection of vulnerable road users. In *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pages 1037–1042, 2014. doi: 10.1109/IVS.2014.6856553.

[98] Lynn M. Hulse, Hui Xie, and Edwin R. Galea. Perceptions of autonomous vehicles: Relationships with road users, risk, gender and age. *Safety Science*, 102:1–13, feb 2018. ISSN 18791042. doi: 10.1016/j.ssci.2017.10.001. URL https://linkinghub.elsevier.com/retrieve/pii/S0925753517306999.

[99] Ramy Q. Malik, Khairun N. Ramli, Zahraa H. Kareem, Mohammed I. Habelalmatee, Ali H. Abbas, and Abdulla Alamoody. An Overview on V2P Communication System: Architecture and Application. In *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, pages 174–178. IEEE, sep 2020. ISBN 978-1-7281-8231-5. doi: 10.1109/IICETA50496.2020.9318863. URL https://ieeexplore.ieee.org/document/9318863/.

[100] Máté Zöldy, Zsolt Szalay, and Viktor Tihanyi. Challenges in homologation process of vehicles with artificial intelligence. *Transport*, 35(4):447–453, nov 2020. ISSN 16483480. doi: 10.3846/transport.2020.12904. URL https://journals.vilniustech.lt/index.php/Transport/article/view/12904.

[101] Rafael Angarita. Responsible objects: Towards self-healing internet of things applications. In *Proceedings - IEEE International Conference on Autonomic Computing, ICAC 2015*, pages 307–312. Institute of Electrical and Electronics Engineers Inc., sep 2015. ISBN 9781467369701. doi: 10.1109/ICAC.2015.60.

[102] Hauke Petersen, Emmanuel Baccelli, Matthias Wählisch, Thomas C. Schmidt, and Jochen Schiller. The role of the internet of things in network resilience. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, volume 151, pages 283–296. Springer Verlag, 2015. ISBN 9783319197425. doi: 10.1007/978-3-319-19743-2_39.

[103] Arjun Athreya, Bruce DeBruhl, and Patrick Tague. Designing for Self-Configuration and Self-Adaptation in the Internet of Things. In *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 585–592. ICST, 2013. ISBN 978-1-936968-92-3. doi: 10.4108/icst.collaboratecom.2013.254091. URL http://eudl.eu/doi/10.4108/icst.collaboratecom.2013.254091.

[104] Sylvain Cherrier, Yacine M. Ghamri-Doudane, Stephane Lohier, and Gilles Roussel. Fault-recovery and coherence in Internet of Things choreographies. In *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, pages 532–537. IEEE Computer Society, 2014. doi: 10.1109/WF-IoT.2014.6803224.

[105] Joey Sun, Shahrear Iqbal, Najmeh Seifollahpour Arabi, and Mohammad Zulkernine. A classification of attacks to in-vehicle components (ivcs). *Vehicular Communications*, 25:100253, October 2020. ISSN 22142096. doi: 10.1016/j.vehcom.2020.100253. URL https://linkinghub.elsevier.com/retrieve/pii/S2214209620300243.

[106] Luisa Andreone, Andrea Guarise, Francesco Lilli, Dariu M. Gavrila, and Marco Pieve. Cooperative systems for vulnerable road users: The concept of the watch-over project. In *13th World Congress on Intelligent Transport Systems and Services*. Intelligent Transport Systems (ITS), 2006.

[107] Phi Le Nguyen, Ren-Hung Hwang, Pham Minh Khiem, Kien Nguyen, and Ying-Dar Lin. Modeling and Minimizing Latency in Three-tier V2X Networks. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, volume 2020-Janua, pages 1–6. IEEE, dec 2020. ISBN 978-1-7281-8298-8. doi: 10.1109/GLOBECOM42002.2020.9348182. URL https://ieeexplore.ieee.org/document/9348182/.

[108] Carsten Maple, Matthew Bradbury, Anh Tuan Le, and Kevin Ghirardello. A connected and autonomous vehicle reference architecture for attack surface analysis. *Applied Sciences*, 9(23):5101, November 2019. ISSN 2076-3417. doi: 10.3390/app9235101. URL https://www.mdpi.com/2076-3417/9/23/5101.

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

ISBN 978-952-02-0547-8 (PRINT)
ISBN 978-952-02-0548-5 (PDF)
ISSN 2736-9390 (PRINT)
ISSN 2736-9684 (ONLINE)

Painosalama, Turku, Finland 2026