

EXPLORING THE AUTOMOTIVE EMBEDDED SECURITY

by

Shivaprasad Parameshwarappa Angadi, BE, MBA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

MAY, 2025

EXPLORING THE AUTOMOTIVE EMBEDDED SECURITY

by

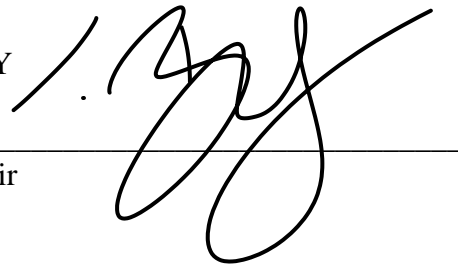
Shivaprasad Parameshwarappa Angadi

Supervised by

Velimir Sirca

APPROVED BY

Dissertation chair



RECEIVED/APPROVED BY:

Admissions Director

Dedication

My dedication is to my parents, wife, son, SSBM, and academic mentors. I also dedicate it to my beloved paramjyothi amma and bhagavan, whom I worship. In my embedded and automotive security career, my colleagues and seniors have guided me on those topics. I dedicate it to those professional mentors as well.

Acknowledgments

Thanks to the supreme light. I would like to express my deep gratitude to the mentors ivan pavic and velimir srica from SSBM for reviewing and sharing lots of comments and made this thesis better. Last but not the least, my gratitude to the parents, namely; parameshwarappa giriyappa angadi and dinamani parameshwarappa, wife, anushree and son, dhiraj shivarpasad.

ABSTRACT

EXPLORING THE AUTOMOTIVE EMBEDDED SECURITY

Shivaprasad Parameshwarappa Angadi
2025

Dissertation Chair: <Chair's Name>
Co-Chair: <If applicable. Co-Chair's Name>

Background

In the vehicle, there are many electronic components like ECUs (electronic control units) and also wireless components like infrared or UWB (ultra-wide band) - based remote car access, wireless charger, audio, lighting, and more. Additionally, many external communications are happening in connected car technologies like over-the-air updates (OTA) through cellular mechanisms and other smart devices like roadside traffic lights, pedestrians, other smart vehicles, and more. With this many attack entry points also called attack vectors/surfaces arise and hence need to be secured.

Methods

To explore automotive security, firstly, will investigate the business impacts that occurred in the automotive industry majorly, which covers the significant part of this research. Second, the automotive security process for security quality measures during the entire vehicle life cycle and third security concepts covering major security

protections will be researched. Finally, major use cases with its assets to be protected will be covered in the form of item definition, a block diagram covering the assets, followed by the assets threat analysis and risk assessment (TARA), and risk mitigation mechanisms.

Results, discussion and conclusion

For each asset under threats, results are derived quantitatively and quality for attack feasibility estimation, damage impact and risk. With this, we will see the major ECUs and use cases attack entry points, attack feasibility, threat scenarios, damage scenarios and countermeasures, which could be referred to by automotive security engineers for their concept (item definition, TARA, requirements elicitation and more), design, development, maintenance and decommissioning.

KEYWORDS

Security, automotive, threat, vulnerability, attack, risk, attack surface, attack vectors, confidentiality, integrity, availability, authenticity, authentication, authorization, spoof, eavesdropping, hack, privacy.

TABLE OF CONTENTS

CHAPTER I: INTRODUCTION	8
1.1 Introduction.....	8
1.2 Research Problem	9
1.3 Purpose of Research.....	9
1.4 Significance of the Study	11
1.5 Research Purpose and Questions	12
CHAPTER II: REVIEW OF LITERATURE.....	14
2.1 Literature Review Objectives	14
2.2 Attacks/threats.....	15
2.2.1 AI (Artificial Intelligence) model attack.....	15
2.2.2 Threats in EV (electric vehicles).....	16
2.2.3 Communication channel attacks	17
2.2.4 Attack using diagnostic port	22
2.2.5 Side-channel attacks (SCA).....	23
2.2.6 Attacks on sensors.....	24
2.2.7 Conclusion on attacks literature review	25
2.3 Vulnerabilities/weakness/attack surfaces.....	26
2.3.1 Automotive software, cryptography and interface flaws	26
2.3.2 Connected car vulnerabilities and weak points.....	28
2.3.3 Conclusion of literature review of vulnerabilities and weak points.....	29
2.4 Prevention and countermeasures – security in-depth.....	30
2.4.1 Automotive Security HW and SW security mechanisms	31
2.4.2 Automotive secure communication	32
2.4.3 Automotive security tests and finding solutions with simulations of real-world scenarios-based research - a left shift mechanism	35
2.4.4 Security and safety dependencies during security risks countermeasures.....	39
2.4.5 Security in Gateway and ADAS ECUs.....	40
2.4.6 Security measures in sensors – general sensors, ultrasonics and radar.....	42
2.4.7 Conclusion on prevention and countermeasures literature review.....	44
2.5 Summary of literature review and overview	45
CHAPTER III: METHODOLOGY.....	48
3.1 Overview of Methodology	48
3.2 Business/economic impact reports.....	48

3.3 Automotive security process	51
3.4 Security concept.....	54
3.5 Item Definition.....	55
3.6 Extended TARA.....	56
3.7 Extended TARA with a digital certificate as an asset example	63
CHAPTER IV: RESULTS	66
4.1 Research Question One: What is the automotive business/economic impacts? Who are the impacted stakeholders?	66
4.2 Research Question Two: What automotive processes to follow? What are the different aspects of automotive processes?	67
4.3 Research Question Three: What are the various security goals, concepts, requirements and claims?	70
4.3.1 Secure communication	71
4.3.2 Secure boot, secure download and secure update	76
4.3.3 Cryptography systems	77
4.3.4 Secure diagnostics	78
4.3.5 Secure debug	79
4.3.6 IDSM.....	79
4.3.7 Memory protection.....	80
4.3.8 Secure logging.....	81
4.3.9 Supply chain security	81
4.3.10 Secure software	82
4.3.11 Trusted environment	82
4.3.12 Security - safety collaboration and interference resolution.....	83
4.3.13 Security testing and vulnerability analysis.....	83
4.4 Research Question Four: Roughly how is the extended TARA to be executed in automotive security for various electronic components in the vehicle?	84
4.4.1 ADAS ECU	84
4.4.2 IVI/digital cockpit ECU	100
4.4.3 Telematics ECU	109
4.4.4 V2X (vehicle to everything).....	113
4.4.5 Keys and certificates in-vehicle ECUs.....	117
4.4.6 EV (electric vehicle) electric charging.....	122
4.4.7 OBD – Onboard diagnostics port	127
4.4.8 Keyless door entry	131
4.4.9 Two-wheeler electronic systems	136
4.5 Summary of Findings.....	141
4.6 Conclusion	143
CHAPTER V: DISCUSSION	145

5.1 Discussion of Results	145
5.2 Discussion of Research Question One: What is the automotive business/economic impacts? Who are all stakeholders impacted?	145
5.3 Discussion of Research Question Two: What automotive processes to follow? What are the different aspects of automotive processes?	146
CHAPTER VI: SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS	147
6.1 Summary	147
6.2 Implications.....	147
6.3 Recommendations for Future Research	148
6.4 Conclusion	148
REFERENCES	150
LIST OF ABBREVIATIONS	168
List of Tables	179
List of Figures	183

CHAPTER I:

INTRODUCTION

1.1 Introduction

Road transportation is increasing more than ever before and more of the latest technologies are getting embedded in vehicles for increasing comfort, convenience and safety of vehicle users. It is majorly achieved with the introduction of modern electronic components, termed ECU (electronic control units). ECUs have external and internal interfaces which are vulnerable to attacks. External interfaces for example are wireless communication outside the vehicle. An internal interface example is a vehicle bus. Even if one ECU is hacked then other ECUs connected with the same vehicle bus which the hacked ECU uses, are under threat. The following items should be investigated to ensure high security in the vehicle's electronic system which includes ECUs and popular and vulnerable communication use cases: ADAS (advanced driver assistance system) ECU, IVI (in-vehicle infotainment) ECU, TCU (telematics control unit) and V2G (vehicle to grid) use case. In ADAS, investigation will include the sensors (lidar, radar, ultrasonics (USS) and camera) and actuators (for example: steering, braking and acceleration kind of driving functions) along with the ADAS system. In IVI, the security vulnerabilities and countermeasures investigation will be done for IVI to mobile communication, navigation including SD card for HD map storage, radio (DAB-digital audio broadcast, AM-amplitude modulation, FM-frequency modulation), USB for multimedia use cases and more. In telematics, would do a security investigation on cellular (4G, 4G LTE) and DSRC (digital

short-range communication- example: WiFi6) kind of communication issues and their mitigations. In V2G, BMS (Battery management system) and electronic charging system will be the focus.

1.2 Research Problem

ECU interacts with other ECUs in vehicles and also with the outside world, the cloud, infrastructure, other vehicles, devices, pedestrians and other smart things. Such high intra-vehicular ECU interconnectivity and various wireless connectivity to the outside vehicle systems increase the attack surfaces, which are the entry points for attackers. Vulnerabilities/weaknesses in the system could add to such entry points/attack surfaces. As the modern era is evolving, hacking has become cheaper with the availability of cheaper attacking gadgets/equipment (like radio gadgets used for stealing the car) for remote attacks (away from the vehicle), local attacks (when attacking equipment is nearby) and physical (by physical access to the vehicle's electronic system) attacks. Physical attacks could be invasive, where the targeted system is made unusable after the attack and non-invasive, where the targeted vehicle system continues to function even after some physical damage/changes are done. In summary, attack and vulnerabilities in the vehicle systems is the problem. In the literature review attacks and vulnerabilities will be the first focus point.

1.3 Purpose of Research

The goal of the research is to firstly emphasize the importance of automotive security and develop an automotive security process. Further, research on strong security

concepts/goals/requirements and various types of equipment used by the hackers, will be done. Finally, investigation into the major security issues along with the countermeasures will be performed. For the importance of automotive security topic, exploration on the reports, news and magazines for major attacks that occurred, would be carried. For the automotive security process, will refer to the insight shared in several automotive security standards and regulations. The software concept will cover the countermeasures. The attack equipment's list will have the functionalities described with it. For exploring the automotive security problems and solutions, customized extended TARA (threat analysis and risk assessment) process tool (table, listing based) will be used, covering risk mitigation calculated against assets under threats or vulnerable assets. Extended TARA is TARA plus countermeasures. The literature review will majorly focus on extended TARA. The literature will be picked for attacks, vulnerabilities, prevention, and countermeasures in the embedded automotive electronics domain. For TARA process will refer to the ISO21434 kind of automotive cybersecurity management system (CSMS) standards. Assets will be picked majorly from ECUs like ADAS (advanced driver assistance system), IVI (in-vehicle infotainment), TCU (telematics control unit), electronic charging and v2X use cases. In ADAS ECU various sensors like cameras, lidar, radar, ultrasonics actuators and driving decisions like forward collision detection, object detection, adaptive cruise control, lane-keep-assist (LKA), parking assistance and more, depending on signals from ADAS, need to be researched as the industry is heading towards autonomous driving. Countermeasures will be suggested for each security issue to be investigated in the form of security goals, requirements and claims. These security goals, security requirements and security claims will highlight the solution part for each security problem under investigation. Thesis will be influenced heavily by most unique

automotive career of mine, covering OEM, Tier1/2 and service-based organizations in the automotive supply chain.

1.4 Significance of the Study

There are many ways in which vehicles can be connected to sensors and others like for example in V2* shown in the Table 1. Hence there is a need to protect the vehicle against all connections. A Futuristic modern Digital Cockpit has IVI system along with ADAS/AD sensors, instrument-clusters and various other remote Communication features embedded in one or more ECUs. Also has integrated audio, display, touch screen, IO controllers like buttons, knobs and more Modern ECU is heavily connected to external environment/interfaces and hence have many attack surfaces. Example: A modern car can have up to 200+ ECUs and various electronic components, sensors and actuators. To list a few: instrument cluster, ADAS, infotainment, sensors: camera, radar, Lidar (Laser + radar), USS, leddar, motor applications: wiper, power window, body comfort: HVAC, miscellaneous: BMS, TPMS. UNR155 mandates to follow the security process and protect the entire vehicle against the threats arising out of such a complex modern vehicle system.

*Table 1: V2**

<u>V2*</u>	<u>Remarks</u>
Vehicle to Everything (V2X)	as everything is going digital
Vehicle-to-Infrastructure (V2I)	like traffic light poles interacting with vehicles in accidents, road congestion, and other warnings and guidance

Vehicle to Vehicle (V2V)	to give some indications on-road situations that other vehicles may not be able to make out and more such information,
Vehicle to Pedestrian (V2P)	more helpful to blind persons, just an example
Vehicle-to-Personal Devices (V2T)	like mobile for remote access to the vehicle door (open and close) or for vehicle navigation, bluetooth music and bluetooth telephony, and more
Vehicle-to-Roadside Units (V2R)	
Vehicle-to-Sensors (V2S)	

1.5 Research Purpose and Questions

Vehicle has various attack surfaces/attack entry points. Some of them are listed as follows: side channels: cache Attack, power analysis, electromagnetic, vulnerable interfaces: USB/ SD Card, debug interfaces: DLT(ethernet), UART), wireless interfaces: WiFi, BT, cellular communications. Types of attacks are classified as listed: invasive, semi-invasive, non-invasive attacks, physical attacks and Remote attacks. Research purpose is to throw some light into the vehicle threats and propose a systematic approach for it's early detection and prevention . This systematic approach will be

covered in research methodology section. Various questions are addressed in the thesis.

Some of the questions are listed below:

Q1. What is the business impact of attacks on vehicle? Who are all the impacted stakeholders?

Q2. What automotive process need to be followed? How to securely execute the automotive project?

Q3. What are basic automotive security concepts?

Q4. What all assets are compromisable/can be attacked?

Q5. What are all the attack surfaces / entry points?

Q6. What are all the risk mitigations?

CHAPTER II:

REVIEW OF LITERATURE

2.1 Literature Review Objectives

In this literature review section, will investigate the various scientific literature and its shortcomings if any, which would emphasize the importance and need of the research on automotive security topics and countermeasures like automotive attacks, vulnerabilities/attack surfaces/weaknesses and prevention/countermeasures. Examples of prevention/countermeasures: securing various aspects in various hardware and various layers of various software components, various threat assessments and risk mitigations from the various scientific literature, secure testing, software countermeasures and hardware countermeasures. Will elaborate on the shortcomings of the various literature on automotive security, required to come up with robust and unique automotive security solution ideas.

Will focus one by one on various angles connected to automotive security during the literature review and discover the gaps in some areas and cover a few gaps among them. The literature review will be done based on the following topics: a. attacks/threats, b. vulnerabilities/weakness/attack surfaces and c. prevention and countermeasures. Attacks/threats are intentional actions that compromise one or more security properties like confidentiality, integrity, availability of the data and more. Example of attacks/threats is unethical access to information or indulging in wrong vehicle information generally for some illegal gains with wrong intentions. Vulnerabilities/weaknesses/attack surfaces are

entry points to attack the system. For example, loopholes in the electronic systems enhance the possibility of attack. Prevention and countermeasures are protection against attack. It is also actions taken to avoid being attacked and/or mitigate and/or resolve and/or recover and/or reduce the damage caused by the attack.

2.2 Attacks/threats

In this section, will be highlighting attacks/threats mentioned in the various literature reviews. It would also cover the problem statements and the importance of the research in the automotive security field. Attacks could be classified as remote (away from the vehicle), local (near the vehicle) and physical (touching the system) attacks, which would be covered in some of the picked use cases covering both HW (hardware) and SW (software) based attacks.

2.2.1 AI (Artificial Intelligence) model attack

The emergence of AI has not left the automotive world either. Paper (Sato, T. Et al., [Accessed 20 Sep. 2023]), reveals that recently released vehicles have a significant number of AI algorithms running, especially in ADAS (Advanced Driver Assistance Systems)/AD (Autonomous Driving). Even that is subjected to the threat of adversarial attacks creating optical illusions in the computing system. The attacker intends to fail the machine, with the creation and introduction of a faulty machine learning model. Such flawed models are difficult to recognize, causing enormous damage to the system. Missing threat analysis and risk assessment (TARA) for AI-based attacks, will be researched further, in the research.

2.2.2 Threats in EV (electric vehicles)

Emerging EV vehicles related infrastructure for easy charging of the battery and quick and simple payment methods for getting charged have emerged, introducing more attack possibilities. Paper (Zeinab Rezeifar et al., 2016) mentions that future technologies for wireless charging of EV vehicles on the move have a lot of security issues. Wireless communication with charging plates and wireless payments is vulnerable to many attacks like DoS (Denial of Service), eavesdropping, hardware attacks and more, which would cause a lot of threats. Confidentiality of PII (Personally identifiable information) could be compromised, like location privacy threat, causing easy kidnapping, vehicle theft and more.

The power grid used for charging electric vehicles is introducing new attack paths. Paper (Mohammad Ali Sayed *et al.*, 2021) mentions, power grids also are under threat. Such attacks on power grids have major business/economic and social impacts too. Grid attacks could be direct or remote. Paper (A. Mahmood *et al.*, 2021) states that modern vehicles are IoT-on-wheels or IoV (Internet of vehicles) and hence could cause a threat to power grids with their high connectivity and through electric charging grids. Hence power grids are vulnerable through vehicle networks too. The conclusion is that there is a security gap in the newly added infrastructure to facilitate secure EV charging and secure payments for getting charged. Threat scenarios, attack feasibility and attack paths in EV vehicles including BMS (Battery management system) risks will be researched further.

2.2.3 Communication channel attacks

The emergence of the internet in the automotive world creates lots of attack possibilities like in computers and mobiles. In the paper (A. Mahmood et al., 2021) maliciously claiming higher execution privilege by a compromised vehicle network node/ECU in a vehicle network could cause an attack called a self-promoting attack. Randomly behaving good or bad by a hacked network node/ECU and getting higher execution privilege causes an attack called an on-off attack. Firstly, behaving well and then badly by an ECU/vehicle network node leads to so-called optimistic attack. Selective behavior attacks could be caused by selectively behaving well for some kind of services in the IoV network maintaining a reasonable reputation. A bad-mouthing attack is practiced by a hacker by colluding with good vehicles and thus damaging the reputation of trustworthy vehicles. In ballot stuffing, non-trustworthy vehicles collide with each other and thus enhance the trustworthiness of malicious vehicles.

There are a few ethical hacker attack cases too. Paper (C. Miller, IEEE, 2019) mentions that, remotely many motor control application ECUs and IVI/HMI (human-machine interface) systems are attacked at one instance, by hackers, firstly entering the most vulnerable ECU, via a vulnerable non-secure WiFi connection. There are many running vehicles and parked vehicle attack cases and will cover the most famous cherokee jeep hacking on highways in this literature review. It is a remote attack use case with high attack feasibility. The best threat scenario could be this cherokee Jeep attack on the running vehicles on the highway at great speeds to learn more. Various damage scenarios occurred

due to this hack. First example: hacked vehicle's display video, in the in-vehicle infotainment (IVI)/HMI (human-machine interface) ECU blocked the driver assist view. Second example: the brake/transmission/steering/pedaling was disabled by hacking the related ECU, by sending wrong signals through the vehicle bus. Third example: hackers kept the inside vehicle environment to max cold by hacking the HVAC (Heating, Ventilation and Air-Conditioning Systems) ECU. Fourth example: hacked IVI ECU's made radio volume to max, which could be in general an unbearable noise experience to any driver, and thus distracting, while playing a hip-hop song.

Both external and internal vehicular networks have lots of attack possibilities. Source (Bella, G., et al., I., 2020) reveals a few attacks out of which two attacks are summarized here from 2010 and 2015 incidents. In 2010, hackers controlled the car remotely through V2X cellular communication through the internet and made the engine exploitable. The brakes became redundant and the vehicle was unstoppable. The instruments were giving false readings. Thus integrity, availability and authenticity of the data are breached.

Source (Bella, G., et al., I., 2020) related another attack is of, the 2015, GM (General Motors) vehicle infotainment system hacking. Hackers stole the data from the infotainment system. Thus, the confidentiality of the data is breached here. They exploited the internet connection of the IVI system. A malicious version of IVI system software was installed. Communication if not secure enough through encryption and with proper authentication mechanisms, leads to a lot of attack possibilities. In the next paragraphs, the realization of these attacks would be discussed.

Attacks could be possible by sending various customized CAN frames (messages, with a unique meaning to each bit field, going through the CAN vehicle bus, which is the most used physical vehicle bus for intra-vehicle communication) to the receiving ECU like re-sending valid CAN frames which are also called a replay attack. CAN frames could be modified/alterd, called tampering. A hacker could also send a valid CAN frame, and hence a valid signal for ECU to perform a specific ECU action, called forging. Hacker injects already previously forged CAN frames, which were previously forged, to research the behavior of an ECU on target for strange inputs, called fuzzing. Hackers could do masquerading, wherein a valid CAN ID (Identifier) of another ECU is used. An adversary could gather information by identifying critical contents from CAN frames, such as the frame ID or payload (specific bit fields of the frame/CAN message) and its associated ECU functionality, to use it against a target ECU to perform a post-attack. Attack mechanisms acquire information in the network, injecting frames to manipulate the information to the ECU and avoiding privileged access to ECUs.

With modern vehicles having to wirelessly communicate with an external smart environment, the vehicle acts like a node in the outer network. Jadoon, A.K. et al., (2018) mentioned below possible attacks related to authentication in VANET (Vehicular Ad-hoc Network). Potential attacks related to authentication are the following: sybil attack, impersonation attack, bogus information attack, session hijacking attack, session hijacking attack, relay attack, and spoofing attack. A sybil attack is an attack, where one network node asserts itself as many nodes by replicating as many identities as possible, announcing at various positions and sending many messages and thus occupying network bandwidth.

An impersonation attack is an attack, which occurs when a hacker node is characterized as an authorized node by getting false attributes or stealing identity, to disturb the network and/or get network privileges. Bogus information is an attack, where a hacker sends unauthenticated fake data like a traffic jam on a specific road due to an accident to clear the hacker's route, to the beneficial system for their selfish aims. A session hijacking attack is an attack, where authentication is done only during the generation and allocation of session ID (SID). This loophole is used by attackers to pick up a specific SID and take control of the session. In replay attacks, a hacker mimics a good vehicle or roadside unit (RSU) to get data packets and then sends a copy of the packet to another node for its self-benefit thus causing a confidentiality threat along with authenticity. In a global positioning system (GPS) spoofing attack, a satellite keeps the locations of vehicles including their identities in a location table, which the attacker alters and generates a stronger signal using simulators, to cheat the vehicle.

There are many attacks impacting network efficiency. Examples are: FHSS attack, distributed DoS (DDoS), SYN flood/half-open attack, black hole attack, gray hole attack, wormhole attack, timing attack and intruder attack. In DoS attacks, dummy messages are sent to impact majorly on the performance and efficiency of the vehicular network and make victim node to the right users by jamming, distributed DoS attack (DDoS), or by SYN flooding TCP (Transmission Control Protocol) which is a type of distributed DoS attack. In routing attacks, weaknesses/loopholes in the network are attacked. In a black hole attack, a bad network node attracts the source node by sending a false route with a low hop count, to send packets to itself for dropping those packets. In gray hole attacks, which

is the same as black hole attack, but here it drops only selected packets. In a wormhole attack, two or more nodes make tunnels in the network and send the packets, thus reducing the route's hop count and attaining a great position for performing replay and DoS kind of attacks. In timing attacks, the malicious node alters the time of packets, creating a delay in communication and causing nearby nodes to miss important information within time which could cause traffic jams and accidents kind of issues. In an intruder attack, unauthenticated nodes or services may try to enter the network to obtain false attributes or reduce the efficiency of the network.

Some network attacks impact user privacy/confidentiality. Examples are: eavesdropping, location-trailing attacks and identity-revealing attacks. In eavesdropping, sniffing the network for sensitive information is done by the attacker. In a location-trailing attack, the attacker gets the position of the vehicle or the trace over a period to map out the victim's vehicle. In an identity-revealing attack, the attacker reveals the identity of the driver with cruel intentions. Now let's see some miscellaneous attacks. In differential related-key attacks, the attacker studies the differences in cipher operations when various keys are being used. It is a form of cryptanalysis (an analysis of ciphers, cipher text and cryptosystems with bad intentions). In a brute-force attack, the hacker tries to use a trial-and-error method to crack keys/passwords/credentials.

Though OTA (Over The Air software update – through wireless channel) gives great advantages for bug fixes and feature updates and more, but introduces possibilities of malicious images getting updated and executed. In paper (Christoph Schmittner, et al., 2015), 1. Confidentiality 2 availability and 3 integrity threats are mentioned, which are

summarized as follows. SW update availability could be under threat if hacker keeps sending fake updates to TCM (Telematics Control Module). Also, a hacker can send many firmware files to consume CPU (central processing unit) bandwidth and thus avoiding the verification of the binary image or disturbing the TCM communication stack. The integrity of the SW to be updated could be compromised by tampering in the communication channel by hackers when signing and verification methods are not incorporated at both the sender and receiver's end. The owner could mistakenly accept SW updates in greed of new features/functionality. The hacker could send the binary image (source code for the integration) as if it is from an authenticated source. The conclusion is that the literature covers threat scenarios for generic use cases. This thesis will deep dive into various specific threat scenarios, attack paths and attack feasibility as part of TARA across ECUs like ADAS, IVI, EV-related ECUs, TCU and other use cases.

2.2.4 Attack using diagnostic port

OBD (Onboard diagnostics) port if not secured could be an easy attacking point. Paper (McLachlan, S., et al., 2022), mentions that in 2013, an ethical hacker connecting to OBD – II located under the dashboard of a car, from a MacBook via a data cable, easily disabled the brake. Here OBD2 is a diagnostic protocol used for monitoring the vehicle for repair/prevention/safety purposes. On-board diagnostics are mainly targeting emission-related reporting while off-board focuses on all other ECUs. For diagnostics, there is also a dedicated port/interface, which is vulnerable to attack as mentioned at the beginning. In the literature, detailed countermeasures are missing. In the thesis, multiple

countermeasures will be seen, for securing the OBD port, as it is an easy path of attack and as it was a reason for the recall of 1.4 million cards in the year 2015, for a software update to fix the issue.

2.2.5 Side-channel attacks (SCA)

Attacks can be performed by just observations/eavesdropping or manipulating the execution through a different channel. Paper (Schlösser, A. et al., 2012), reveals that there are many hardware (HW) side-channel (indirectly getting info or altering the execution of the program, also called as implementation attack or sidebar attack) attacks. One of them is SPEA (Simple Photonic Emission Analysis), in which a hacker gathers information by observing the backside of ICs (Integrated Circuits). Here, extremely weak photoemissions from switching transistors are captured which are related to the electronic chip executing the program. SPEA could recover the full symmetric AES (Advanced Encryption Standard) crypto algorithm secret key by monitoring accesses to the key part of the algorithm (S-Box- a part of the AES algorithm).

This attack requires no processing of data/ no program execution. Source (Xun, Y., et al., 2019) mention that a lot of interfaces act as attack surfaces for side-channel attacks, like USB (universal serial bus), Wifi, BT (Bluetooth), ETH (Ethernet), CAN, Radio, GPS (Global Position System), and cellular networks like 5G. The conclusion is that there is a need to deep dive into various automotive ECUs, majorly heavily exposed to external interfaces once and sensitive ECUs and vehicle use cases for all possible attacks in them.

The thesis will follow TARA (Threat Assessment and Risk Analysis) for various side channel attacks and fault injection attacks at the HW level mentioning various hacker expertise levels and budgets required for various attacks and thus covering attack feasibility. Additionally, attack paths and attack trees will be included in TARA. In TARA, we investigate item definition assets, which are under threat, against cybersecurity properties like confidentiality, integrity, availability and more. In TARA we cover threats, damage scenarios and risk impact and in extended TARA also risk mitigations will be researched. Item definition is a system, sub-system or component for which assets under threat will be explored further in the TARA process. An example sub-system is an ECU. An example system is an ADAS system, which consists of related ECUs, sensors, actuators and its communication channels. Components could a single SOC (system on chip).

2.2.6 Attacks on sensors

With the emergence of autonomous driving, there is a significant increase in the usage of the sensors. Paper (Shoukry, Y., et al., 2015) mentions majorly on the possibility of passive eavesdropping attacks and spoofing active attacks through the physical/analog (visible waves, acoustic waves, magnetic waves) domain of RFID (radio frequency identification), optical sensors, radar, laser, ultrasonic sensors. Attacks could be performed by signal injection, signal masking or concealment (hidden attack).

Attacks on radars are planned on radar coverage properties. Paper (Cemil, A. et al., 2022) defines 4 practical ADAS jamming scenarios. Also, it mentions 2 methods of spoofing methods based on digital radio frequency. They are correlated range and velocity

gate pull off/in (RVGPO/I) and coherent false target (CFT). 4 scenarios are CFT way of false pedestrian generation of echo, manipulation of velocity and range in the front radar by RVGPO/I, parameter modification of pedestrian (real vehicle in scenario 4) by RVGPO/I. Attackers need to consider the maximum range, width of the beam and spatial resolution. This paper also studies the effectiveness of jamming. All radar ranges are considered, that is short-range radar (SRR), mid-range radar (MRR) and long-range radar (LRR). Power requirements also are researched.

In radio communications, interference is a problem. Paper (Yeh, E., et al., n.d.) additionally mentions interference attacks in radar, which could be intentional too. Types of radar jamming mentioned are forward and blind spot jamming. For DSRC and Radar, confidentiality, interference, spoofing and jamming are the risks mentioned. Both radar and DSRC are wireless communications. The conclusion is attacking threats on sensors like cameras, ground speed sensors and ground view sensors (GVS) are not covered and will be covered in the thesis. In the thesis, for quantitative risk analysis, the literature mentioned details like the level of easiness for jamming could be utilized which also reflects the expert level needed to jam and the resource and budget requirements for jamming. Going forward, TARA will be performed for DSRC and radar attacks in the thesis.

2.2.7 Conclusion on attacks literature review

The attacks section of the literature review concludes that there are missing systematic TARA approaches for explaining threat scenarios, attack feasibility, attack paths, and more for AI-based attacks and EV use cases. We also found that there is insecure

EV infrastructure, IoV, V2X, intra-vehicle CAN communication, SW update, diagnostics and more. In the thesis, attacks on sensors like the camera, ground speed sensor and GVS, specific attacks on major ECUs like on ADAS, and IVI also may be covered, with the TARA approach.

2.3 Vulnerabilities/weakness/attack surfaces

With the car's electronic hardware and software systems becoming more and more complex, loopholes also increase. This section emphasizes software flaws and connected-car vulnerabilities among many. Vulnerabilities give a way to attack by creating various threat scenarios covering various attack paths/attack tree which describes on the various attack possibilities/ways. Vulnerabilities are connected to a flaw in an asset design, operations, management and/or implementations, whereas threat is a possibility for a hacker to exploit the weaknesses/vulnerability in it.

2.3.1 Automotive software, cryptography and interface flaws

Software flaws could be introduced in the requirements, design and/or implementation stage. Software flaws arise from the software language or compiler or being taken from an open source where already there is a flaw. In this section, the focus will be on software flaws mentioned in the automotive software-based literature. Paper (Serban, A.C. et al., IEEE, 2018) mentions that the technology inside vehicles has moved from mechanical driven to drive-by-wire, through electronic components like ECUs. ECUs further are controlled by software. We are heading more towards software-driven vehicles

(SDV) in autonomous vehicles. The more autonomous and intelligent the vehicle's system becomes; the more electronics and related software will be needed. The more the lines of code, the more the chances would be there to find software flaws. Standard automotive software frameworks also have come up, like AUTOSAR (AUTomotive Open System ARchitecture) which also increases the wider acceptance of software-driven vehicles, increasing the software in the vehicle.

Cryptography is fundamental for security. Paper (L. Pike, J. et al., IEEE, 2017) mentions, cryptography is the key to providing security. Flaws in cryptographic implementation would lead to the leakage of keys and hence data leakage too. Some critical flaws could be known from databases like MITRE's CVE (common vulnerability enumeration) database. Glue logic codes need to be reviewed thoroughly due to the possibility of wrong implementation of interfaces between various software components. Source (pupuweb.com, 2023) mentions that, nowadays it is common to use more and more open-source code and standard APIs. Like for example TLS (Transport Layer Security) stack using OpenSSL open-source library (Levillain, O, 2021).

It would be a cakewalk for hackers to exploit the vulnerabilities in open-source codes used in the system. But currently, much software is not following it in the hunger for adding features, etc. Once hacked, lots of troublesome activities like an engine starting or stopping, door lock opening and closing, remote code executions in ECUs, location tracking and more. With this vehicle theft, and user privacy breach, car manufacturers and parts suppliers' brands and businesses would go down, incurring huge losses, vehicle recalls would happen, and vehicle and passenger safety is under threat. Web hackers are

finding rich infotainment systems in modern cars for hacking. The conclusion is that in literature, vulnerabilities in the AUTOSAR stack, latest SDV platform may not be explored, which could be a gap to be covered in the thesis. It is important to follow secure coding guidelines (like MISRA, AUTOSAR C++ and more) /practices which could be covered in this research.

2.3.2 Connected car vulnerabilities and weak points

With connected cars getting stronger with an increase in the number of smart things connected to cars, cars become more vulnerable. In this subsection, will review the literature regarding this issue. Paper (Dr. Thomas Strang, 2008/9), mentions cars are becoming smarter with more ECUs coming up to support modern features giving more comfort and moving towards more driver assistance and autonomous driving. With this connectivity inside the vehicle between ECUs and V2X like V2I (Vehicle to infrastructure), V2P (Vehicle to pedestrian), V2G (vehicle to Grid) and V2V (Vehicle to vehicle) comes into the picture increasing enormous vehicle communication with enormous data flowing in and outside the vehicle. Lots of network protocols would be used like HTTP (HyperText Transfer Protocol), and DSRC (WiFi6, 5G, 4G LTE). Each of the network layers follows a unique protocol like HTTP in the application layer, TCP/UDP in the transport layer, IPV6 (Internet Protocol address version) in the network layer, LLC/MAC (Medium Access Control) in the data link layer, PLCP and PMD in the physical layer.

In this subsection, will review the literature regarding this issue. Source (Kaya, K., 2023) mentions, V2X (Vehicle to Everything), V2V, V2I, V2P and V2C (Vehicle to cloud) have all wireless remote connections from various things to vehicle and vice versa, involving various ECUs in the connected car. With these remote attacks becomes easier with the vulnerabilities in V2* communication protocols, interfaces and more. It is important to see the measurability of vulnerability with methods like CVSS (Common Vulnerability Scoring System), impact levels and how hard it is to attack like laymen can do it or it needs a certain level of expertise which makes it costlier and rare possibility of attack. Also, it becomes more important to know which ECUs are more vulnerable and thus isolating the security issue in automotive. 47% and 39% of the vulnerabilities are found in infotainment and TCU respectively.

2.3.3 Conclusion of literature review of vulnerabilities and weak points

The conclusion of the vulnerability literature review is that vulnerabilities in major use cases like ADAS camera sensors and the latest SDV (software-defined vehicle) platform are not researched. Such missing vulnerabilities will be discussed along with the vulnerability detection and prevention mechanisms in the extended TARA process to be conducted in the thesis for each use case. In the thesis, research on the processes to find the vulnerabilities, shall be performed. Those security quality processes are listed as follows: secure implementation, SCA (SW complexity analysis), SAST (static application security testing), DAST (dynamic application security testing) and IAST (interactive application security testing). This security process will aim at continuous security

monitoring and improvements. A short description of each secure quality process is described in the next paragraph.

In a secure implementation, SW and HW security reviews need to be checked. Both SW and HW need to follow secure design/architecture principles against the expected security goals. In the SW review, the code will be reviewed for any vulnerabilities and weaknesses. Further, the code needs to follow the secure coding guidelines from MISRA kind of standards and the tailored secure coding guidelines customized to the organization and the project needs. Any deviations from the secure coding guidelines are to be caught during the SW review process. During the SW security review, the complexity of the code need to be captured, which would further add to the security loopholes as part of the SCA. SAST needs to be part of a DevSecOps (development, security and operations) based CI/CD (continuous integration/continuous deployment/delivery) secure integration strategy during the development and maintenance lifecycle. DAST is recommended to be part of the automated testing and thus considered in DevSecOps. IAST is futuristic low-performance impacting security testing for application software-defined vehicle (SDV). It covers interdependencies/interactions b/w the components and more. IAST overlaps with SAST and DAST. IAST is done during runtime. IAST helps in finding more specific vulnerabilities. IAST helps with more comprehensive security testing, as it covers more attack surfaces.

2.4 Prevention and countermeasures – security in-depth

The previous two sections cover more of the problem statement in the attack section and the cause in the vulnerabilities section. Prevention and countermeasures are on the

solution side. In the thesis, all three would be covered together, majorly as part of TARA and countermeasures. Prevention and countermeasures would cover automotive electronics hardware and software security mechanisms. In this section, will discuss automotive security solutions discovered in the literature.

2.4.1 Automotive Security HW and SW security mechanisms

Automotive security is achieved by both SW and HW. Source (Nagarjuna Rao Kandimala et al., 2012) mentions automotive security with the AUTOSAR framework. It covers security aspects like secure ECU access through the authorization, authorized SW update (example reason could be security fixes) and upgrades for new features, anti-theft system by using some verification/encryption mechanisms, secure diagnosis by DCM (Diagnostic Communication Manager) including managing security levels, isolation of application crypto requests for crypto services using CSM (Crypto Service Manager), non-re-programmability of secure data of NV (Non-volatile) memory, including not erasable and not overwritable memory and OS level memory protection once a fault occurs. The conclusion is that protection against glitches to fault interjection (FI) and SCA from an attack protection point of view is not covered. In SW various isolation mechanisms are not covered like application sandboxing, virtualization using hypervisor for different applications to avoid unnecessary interferences, compiler flags-based kernel hardening, code, data and application hardening. These gaps will be discussed in the thesis along with different ways of memory protection, TrustZone kind of trusted execution environment (TEE).

2.4.2 Automotive secure communication

Run time integrity of data is essential. Paper (Bella, G. et al., 2020), speaks on secure communication in automotive networks. It investigates CINNAMON (Confidential, Integral aNd Authentic on-board comMunicatiON). One of the problem statements addressed in the literature is discovering that CAN is a simple and widely used protocol though FlexRAY and ethernet kinds of vehicle bus communications have emerged and is mostly not secure by design concerning confidentiality, integrity, authenticity and quick availability of the data. When compared to AUTOSAR SecOC (Secure Onboard Communication), this research additionally emphasizes items like confidentiality through encryption of running information and information gathering as part of the process of mitigation of threats. Highlights are configuration of different security properties/requirements, point-to-point protection along with end-to-end protection, verification, authentication and performance time measurement through freshness value. This secure communication mechanism also has a freshness manager software module. Secure diagnostics is essential. Paper (McLachlan, S., et al., 2022), mentions securing OBD-based diagnostic communication by having an authentication using a dongle.

One would need HW accelerators to avoid performance issues with using of core heavy-weighted crypto engine. Jadoon, A.K. et al. (2018) mention VANET vulnerabilities, attacks and mitigation protocols including some crypto details. VANET demands quick data transfers for the availability of information in running vehicles for V2X secure communications. Here in VANET, X majorly could be vehicles, CA (Certificate

Authority), base stations and RSUs. To select the most suitable protocols and associated cryptography in VANET, we need to consider VANET characteristics like high mobility, time-critical data exchange, dynamic network topology, unbounded network density, frequent disconnections, wireless medium, power constraints, limited power transmission, wireless transmission limitations, computing capacity and energy storage. Security requirements for VANET to be considered are message authentication, CIA (confidentiality Integrity Availability), access control, non-repudiation and privacy.

This demands more efficient protocols that use more efficient security cryptography which has less complexity, less computation and is also less vulnerable to attacks. Symmetric LWC to mitigate various possible attacks like blowfish, PBAS, camellia and CAST. Lightweight protocols suggested by Jadoon et al. are ARAN (Authenticated Routing for Ad hoc Networks), SEAD (Secure and Efficient Ad hoc Distance), ariadne - a secure on-demand routing protocol for ad hoc networks, SAODV (secure ad hoc on-demand distance vector), A-SAODV (an extension of secure ad hoc on-demand distance vector), OTC (One-time cookie), ECDSA (Elliptical Curve Digital Signature (ECDS) algorithm, RobSAD – a protocol for sybil attack detection and holistic protocol. Jadoon et al. also mentions random HW key generation for more secure communication.

Major intra-vehicular communication between electronic components is on CAN and hence securing CAN communication is one of the major automotive security tasks. In the future, ethernet communication will also increase due to its lightweight and speed and widely used in LAN (Local Area Network and WAN (Wide Area Network) and other

physical networks. As per the paper (Farag Mohamed e. Lagnf et al, 2022), legacy CAN FD (FD-Flexible Data Rate) and CAN bus are very much vulnerable to attacks like replay attacks and DoS attacks. CAN XL brings compatibility with ethernet communication protocols due to its increased bandwidth and 20 times higher data rate adding to security without adding latency compared to legacy CAN FD and CAN bus. Using robust SHA512 hashing is possible now with increased CAN frame length in CAN XL. With the introduction of the CAN XL, the “availability” security pillar is achieved with a reduction in latency, as it supports up to 20Mbps (megabits per second) data rate and increased CAN frame length and data width up to 2048 bytes unlike only max 64 bytes in CAN FD and 32 bytes in CAN.

Detection of attacks would help the system to take appropriate action when the system is compromised. ECU is an embedded system, and the connectivity of ECUs is also based on internet technology. Based on that, the literature on “Risks and Security of Internet of Systems” by (Levillain, O., 2021), mentions a lot of detections like anomaly intrusions detection using model-based checking and ML (Machine Learning), AI (Artificial Intelligence), malicious HTTP (HyperText Transfer Protocol) request detection using code level CNN (Convolution Neural Network), malware detection and more. CWE (Common Weakness Enumeration) also gives various suggestions for various attacks like CWE-1319- improper protection against electromagnetic fault injection (EM-FI), weakness ID-319. (cwe.mitre.org, 25 Mar. 2023). Protection suggestions given are adding redundancy – comparing the results with redundant logic added, EDCC, failing the default option in switch/if case, making implementation random to avoid timing attacks, using

sensors for glitch detection of current/voltage/clock, physical barriers shield to the chip and finally program flow integrity check.

Secure communication and access control are key security prevention/countermeasure mechanisms. Want to cover sandboxing in the research, which is more related to secure communication in (Rumez, M., Grimm, D., Kriesten, R. and Sax, E., IEEE, 2020) literature, as part of IAM (identity and access management). In the literature, the following security controls are mentioned: DAC, ACL, MAC (Mandatory Access Control), capBAC, RBAC, ABAC, T-RBAC and P-RBAC. Source (Autosar.org, R18-03, 2018) mentions secure communication protocols like DTLS (Datagram Transport Layer Security), and SecOC (secure onboard communication) (autosar.org, R19-11, 2019).

In the literature review, protection mechanisms for vulnerabilities in wireless communications like BT, WiFi and DSRC are missing, which will be covered in the thesis. Other than the literature mentioning OBD security mechanisms, in the thesis, further research will be done on secure debug security countermeasures. Literature review would cover missing SW and HW countermeasures and missed crypto algorithms used for achieving security mechanisms in missed use cases including for quick availability/freshness improvement in missed features and missed point-to-point communication. Will add cryptographic details on secure communication in the research going forward. Will majorly cover security controls from a linux OS point of view.

2.4.3 Automotive security tests and finding solutions with simulations of real-world scenarios-based research - a left shift mechanism

One needs to perform various tests and vulnerability analysis from the initial lifecycle of the project for early detection and fix. Source (L. Pike, J. et al., IEEE, 2017) mentions that verification, validation, and reviews of HW and SW requirements, architecture, design, and implementation are vital to achieving the desired security level. Through testing one could foresee and prevent many attacks, find vulnerabilities, estimate the impact/risks and more. Such testing could positively influence the security requirements, design and development phase, process/methodology and more. So, security testing plays a vital role in robust automotive security building. Compared to the consumer electronics domain, the drive-by-wire automotive industry needs more security as here impact is directly on the safety of the driver/passengers, pedestrians and more. Hence offensive automotive security research needs to be performed by Tier2/1 and OEMs or by contacting external service providers. Vulnerability analysts could play a vital role here. One may need a sophisticated lab for performing a few of the side channel attacks and fault injections, including cryptanalysis. Advanced testing like penetration testing and fuzz testing could discover some difficult vulnerabilities. The use of static analysis before code execution would find most of the vulnerabilities at the initial stages only. Unit testing and system integration testing also play a vital role in the code coverage of the code to be tested.

The fuzz test is useful to discover some unknown failures and random new code paths. Paper (Fowler, D.S. et al., 2018) mentions the SAE J3061 mentioning about fuzz test as part of the process for reduction in vulnerabilities for CAN buses in inter-ECU communication. It also mentions fuzz test is a black box test. To execute more test cases, it could be automated. System interfaces are sent with random inputs and responses from

the system for those inputs are monitored/recorded. If the system fails, then the system again resets to do more coverage in testing. In the paper, there is a big elaboration of moving from physical locks to cyber-locks for protecting security fundamentals like the CIA triad, by finding bugs in code in advance and thus making hackers difficult to further find the vulnerabilities. With random inputs, unknown and untested code paths could be tested.

The fuzz test is an easy testing mechanism for complex OS and drivers. Paper (Sim, K.-Y. et al., 2011) proposes an adaptive random fuzzing method over a simple random method with fewer inputs to achieve linux OS (operating system) kernel OOM (out of memory) killing. Paper (Zhao, W. et al., n.d.) mentions device-free driver fuzzing as many of the drivers run with the same privileges as kernel in linux. Thus, the few most critical drivers are researched. However, this paper does not speak on how relevant it is in an automotive environment. Paper (Muench, M. et al., 2018) emphasizes memory corruption through fuzzing with suggestions on different fuzzing mechanisms for different OS (Operating System) types for the monolithic kernel, a random approach is suggested. It also mentions various memory-related bugs like stack/heap buffer overflow, format string, double free and null pointer dereferencing and corresponding detection mechanisms for its mitigations. Paper (Wilson, T., 19 Apr. 2018) mentions about four fuzzing methods, pure random, mutation, generation and evolutionary and 2 types of fuzzing remote and local. It also gives a list of various fuzzers like AFL (American Fuzzy Lop), hongfuzz, libfuzzer, peach fuzzer and defensics fuzzer. In paper (Macarie, M., n.d.), fuzzing in android automotive OS (AAOS) using AFL fuzzer is mentioned, emphasizing on growing usage of

android OS in IVIs (In-Vehicle-Infotainment) along with the sample fuzzing code. Paper (Fioraldi, A. et al., 2022) mentions about 3 fuzzers, white-box, grey-box and black-box fuzzers and introduces a widely used libAFL framework majorly considering scalability, portability and extensibility principles. LibAFL core, targets and CC are 3 core libraries in it.

Some tests do help in designing. Paper (Fowler, D., n.d.) mentions that fuzz test help with better design of the vehicle. Bestorm tool uses protocol-based and booFuzz tool uses design-based. A security testing method for automotive is to set up a test system, find the test to be performed, and then target, then tool development, tool validation experimental methods for tooling and finally improve the tooling and methods. Paper (Fowler, D. et al, n.d.) mentions referring to in-vehicle network specifications for fuzz testing. The fuzz test is an extension to the test process for the legacy functional test.

Left Shifting the development process is necessary for quick time to market in the automotive security world as well. The source ("Simulation of Malware Propagation and Effects in Connected and Autonomous Vehicles," 2020, *International conference*) mentions that proactive introduction of threats through simulation could be done for researching susceptibility, exposure, infection and recovery patterns during different traffic conditions for CAVs (connected autonomous vehicles). The threat could be malware. The paper predicts that autonomous L3 (level3), L4 and L5 vehicles may reach between 40% to 80% respectively by 2030 to 2035. Autonomous levels are the level of autonomous driving / driverless vehicles with L5 being considered as the highest autonomous level

wherein none of the passengers need to pay any attention to the automatic driving of the vehicle.

The summary is that the fuzz test could be used to reverse messages, as an attack mechanism, easily disrupting the vehicle network and component damage. The conclusion is that simulation is also the right approach in the path to come up with countermeasures, but in this research, we would not cover detailed application-intensive simulations and could be considered out of scope and/or limitation of the research. The focus would be more on real embedded systems and their communications. The literature does not mention fuzz tests for replay attacks, DoS attacks, software updates and more, which will be researched more in the thesis.

2.4.4 Security and safety dependencies during security risks countermeasures

There is an overlap in security and safety. Paper (Christoph Schmittner, et al., 2015) mentions that in many cases we need to do a co-analysis of safety and security as they overlap and contradict at times. Attacks in cyberspace could affect safety in physical space. Combining security and safety processes in the engineering process has become vital to achieving better security and sync with safety. We need to look into the safety effects of security threats and vice versa. So, we need a co-analysis method leading to a holistic approach. There is a tight coupling of electronics and its software and physical systems and hence there is a great correlation between safety and security. There is no safety without security. Threat modeling and an attack tree are recommended for security analysis. Here attack tree is again an extension of fault tree analysis. In network-based attacks, the attack

graph method is used to identify security risks. Here it is stated hazard and risk analysis cannot go independently and combined techniques and methods are recommended. Here major combined methods are spoken of, FMVEA (Failure Mode, Vulnerabilities and Effects Analysis) and CHASSIS (Combined Harm Assessment of Safety and Security for Information Systems). CHASSIS is recommended to be used at an early stage when details are not there and for critical cases. Whereas FMVEA is to be used at later phases of the engineering phase where system details are available. The paper mentions about STRIDE-based threat modes (user identity Spoofing, Tampering, Repudiation, disclosure of Information, DoS, and privilege Elevation). Misuse case diagrams (D-MUC) for security are spoken in the paper against the failure sequence diagrams (FSD).

This paper also speaks on TCC (Telematics call centre) which could be OBD or GSM which interacts with TCM (Telematics control module). In correlation to the literature, in the thesis, may use STRIDE threat modes and misuse case diagrams for security. In the thesis, will not do co-analysis, as safety itself is another big topic and because of the expertise on security, want to focus purely on security. Would do more research to cover more specific and significant cases on ADAS (Camera., lidar (Light Detection and Ranging), radar-based sensors) kind of safety-based ECUs protection mechanisms. In the research, will not emphasize more on specific safety cases, though there is a correlation between safety and security.

2.4.5 Security in Gateway and ADAS ECUs

Security-sensitive/critical areas like the ADAS area need to have secure communication and a secure environment. Paper (Zuo, Z., et al., 2021) explains the business scenario using the secure gateway to communicate to ADAS (Advanced driver assistance system) ECU by the vehicle controller unit, battery management system for information on vehicle speed, faults and battery status and more to tune the ADAS functions like ISA (intelligent speed assistance), HUD (Head-up-display), ACC (Adaptive cruise control). The paper also mentions that in general only MAC (Message Authentication Code) for message integrity forgetting confidentiality in SOME/IP (Scalable service-oriented MiddlewarE over IP) standard application layer. Also, one more problem statement spoken is about latency due to protocol conversion, for example, CAN* to ethernet-based SOME/IP. The solution mentioned is to use the best-in-class gateways like NXP's S32G* which helps in bringing in confidentiality too along with low latency while protecting against tampering, sniffing and frame forgery.

While MAC (Message Authentication Code) protects against only frame tampering and forgery attacks in the protocol conversion process and transmission process, while AEAD (Authenticated Encryption with Associated Data) algorithm also protects against sniffing. Additionally, a high-routing performance mechanism is also mentioned. Majorly SHA256 HMAC (HMAC - Hash-based MAC), AES128 CMAC (AES - Advanced Encryption Standard CMAC- cipher-based MAC) is used for integrity based on MAC and for confidentiality suggested are AEAD mechanisms are AES256 GMAC (GMAC- Galois/Counter Mode), and chacha20-poly1305. DoS could be defended by intrusion detection mechanisms and firewall while other attacks like frame sniffing, forgery and

tampering are defended with crypto mechanisms. MAC and AEAD both are implemented based on OpenSSL. Communication between gateway and domain controllers is through automotive SOA (Service Oriented Architecture) middleware.

The security process is given utmost importance in advanced driver assistance supporting cars. In Paper (McLachlan, S., et al., 2022), cyber security management system and testing and certification process/roadmap based on WP.29 regulation and legislative importance. It mentions the implementation cost, approval authority, and post-market vehicle surveillance. Literature gives various generic secure communication mechanisms in a generic gateway ECU, while in the thesis, more specific examples of secure communication between the gateway and ADAS will be researched. In addition to the above-mentioned regulation in the literature, will consider the ISO21434 process, and UNR155/6 regulations based on WP.29 in the thesis.

2.4.6 Security measures in sensors – general sensors, ultrasonics and radar

In ADAS many different types of sensors are used but are subject to attacks and hence need security protection too. Paper (Shoukry, Y., Martin, P., Yona, Y., Diggavi, S. and Srivastava, M., 2015) mentions about 2 types of sensors, active and passive. Passive sensors are ambient light, humidity and temperature. Active ones are radar, ultrasound and laser scanners. In passive sensors, digital filtering is used to remove noise. Finding a mismatch in GPS and odometer may be because one of them is getting hacked and thus by heterogeneous sensors reading, at least in this case hack was detected. If there is a violation in the physics handling of the dynamics of the sensor, then hacking could be detected.

Sensors need to be placed in secure remote areas to avoid easy physical contact. Passive sensors cannot be protected at the physical layer. Active sensors have the advantage that it sends the signals too and not just receive which gives the option of protection using PyCRA (PhYsicalChallenge-ResponseAuthentication) against spoofing attacks. Passive eaves-dropping attacks were detected in RFID readers, as part of experiments. Detecting active attacks on magnetic encoders and resilience against it was performed. So majorly PyCRA shows resilience to bad spectra by its accurate estimations, detection within time and with precision of hacker's signal interference sources and passive eavesdropping attacks detection with accuracy. Performance degradation due to PyCRA is handled by oversampling but of course, power consumption also goes high as a price for extra security.

Paper (Lou, J., Yan, Q., Hui, Q. and Zeng, H., n.d.) proposed a physical layer system defense called soundfence to prevent spoofing and signal injection attacks. Also, parameters used for rejecting the signals above the threshold are distance and multi-path, signal strength versus pulse length. It has limitations with the hacker's short pulse width. Here additional defense mechanisms are mentioned. The on-off challenge method which is also a generic defense method for various sensors has limitations with ultrasonic sensors as it keeps oscillating still due to ringing time (additional oscillations after transmitting signal). Randomizing pulse width also called side echo analysis with analog signal and by varying waveform (duration) receiving signal modeling are other defense methods. Hacker's capabilities are categorized as level 0, for no target knowhow. Level 1, for some offline information acquired either by reverse engineering of firmware or measurements or reading sensor's pulsing period from documents. Level 2 hacker gets additional run time

information from early observations like speed and time of signal emission. Level 3 obtains information in real-time with enough resources for eavesdropping, replaying and precise position prediction as per trajectory and real-time speed and last but not least, kalman filtering for better accurate predictions and estimations.

Radars are getting more common nowadays as they compensate for the daylight majorly used camera sensors, as radars are very efficient irrespective of environment light (day or night does not matter) but are subjected to attacks and hence need to be protected. Paper (Neng-Jing, L. and Zhang Yi-ting , 1995) refers to two radar attack countermeasures research against jamming, that is, electronic counter-countermeasures (ECCM) and electronic countermeasures (ECM). Ultrasonics are used for parking assistance and more in automotive. Paper (Xu, W., Yan, C., Jia, W., Ji, X. and Liu, J., 2018) suggests using multiple ultrasonic sensors (triangulation) at the system level and 1 sensor checking physical shift authentication at the physical level by shifting physical parameters. The conclusion is lidar, camera-based sensors are not covered specifically. Will cover missed lidar, camera sensors and other sensors extensively along with the TARA process.

2.4.7 Conclusion on prevention and countermeasures literature review

The conclusion for the prevention and countermeasures literature review is it missed protection against glitches to fault interjection (FI) and side channel attacks (SCA). From an implementation perspective, missing are different ways of memory protection, TrustZone kind of TEE and more. In SW various isolation mechanisms are not covered like application sandboxing, virtualization using hypervisor for different applications and

more to avoid unnecessary interferences, compiler flags-based kernel hardening, code, data and application hardening. These gaps could be covered in the thesis. In thesis will cover more specific examples of secure communication between the gateway and ADAS. Will refer to ISO21434 process and UNR155/6 regulations based on WP.29 in the thesis. In the thesis, may use STRIDE threat modes and misuse case diagrams for security. In the thesis, will not do a co-analysis of safety and security. Still will try to cover exhaustively ADAS (Camera., lidar, ultrasonics and radar-based sensors) kind of safety-based ECUs protection mechanisms. Literature covers few countermeasures for radar vulnerabilities/threats, while in the research, will cover more. In the research, would cover various protection mechanisms in detail against various threats. Would include various specific SW and HW countermeasures for SW and HW attacks and vulnerabilities. Fuzz test for replay attacks and DoS attacks and software updates and would be included, in the thesis.

2.5 Summary of literature review and overview

In the literature review, the problem was discussed in the attack section, weaknesses leading to attack in the vulnerability section and finally solution in the prevention and countermeasures section. In this section, will highlight the most important parts and scientific gaps from those three sections. Research questions shall be structured based on above three mentioned questions in the beginning of this paragraph.

In the attack section, different attacks were covered. AI-based attacks have emerged with AI in almost every area. Attacks on new systems supporting EV charging and its payments were seen. The literature on attacks through side channels, and communication

channels (wired and wireless) was reviewed. The literature considered in the attacks section misses the systematic TARA approach for explaining threat scenarios, attack feasibility, attack paths and more for AI-based attacks and EV use cases. The literature review also does not cover the attacks possibility due to insecure EV infrastructure, IoV, V2X, intra-vehicle CAN communication, SW update, diagnostics and more. Attacks examples mentioned in the standards like ISO21434 and from recent hacks also could be explored further in the research to enhance the problems list and work on reduction in impact of those attacks. Will use the TARA method to explain attack paths, attack feasibility including the hacker expert level required and may be attack tree to explain on threat scenarios in the research for ADAS, IVI ECUs, electronic charging, V2X and other major use cases.

In the vulnerability section, SW, crypto, interface flaws and car connectivity issues were covered. In HW vulnerabilities, only crypto is covered. This thesis may investigate missed HW vulnerabilities related to side-channel attacks and fault injections as well. In this thesis, may elaborate on artifacts/documents needed as part of the vulnerability analysis/management process. May do the vulnerability analysis in the AUTOSAR and SDV stack, as well. May create a vulnerability analysis in the form of attack paths/trees in ADAS, IVI ECUs, electronic charging, V2X and other major use cases.

In the prevention and countermeasures section, various security mechanisms were covered like SW, HW, communication, tests, simulations, message freshness, GW (gateway) ECU, access controls and sensor protection. The prevention and countermeasures literature review missed protection against glitches to FI (fault injection),

SCA (side-channel attack), memory protection, TrustZone kind of TEE (trusted execution environment, a trusted platform) and more from HW perspective. In SW, various isolation mechanisms are not covered like application sandboxing, virtualization using hypervisor for different applications and more to avoid unnecessary interferences, compiler flags-based kernel hardening, code, data and application hardening. In this research, may cover security for ADAS including ADAS GW, front camera authentication, camera input till display protection and more. Security countermeasures for all the interactions in IVI, smart antenna and electric charging systems may be further explored in this thesis.

CHAPTER III:

METHODOLOGY

3.1 Overview of Methodology

In the research, data is collected along with TARA execution based on my experience in the automotive industry from 2016 till date. In that I worked majorly on ADAS and infotainment ECUs. For TARA execution of ECUs, electronics components, use cases I have depended on the knowledge gained from the case studies/paper in the literature review. For, TARA execution of other ECUs, electronic components and use-cases, many of the attack surfaces are similar to attack surfaces/scenarios/attack methods of infotainment and ADAS.

In the research, first will cover the automotive security business/economic reports, emphasizing the importance of the need for automotive cybersecurity. Secondly, will suggest a customized automotive security process that helps to manage the security to its entirety right from concept to the decommissioning stage of the vehicle lifecycle. Third, the security concept shall be defined. Fourth, will list down the various types of equipment used by the hacker. Finally, the item definition for items (systems/sub-systems/components) would be written and will perform the customized extended TARA process for the items. The summarized methodology sequence is listed as follows: business reports > automotive security process > security concept > item definition and TARA.

3.2 Business/economic impact reports

Business and economic impact reports that will be reviewed can come from a company in the automotive supply chain, a research firm, journals, magazines, news channels, newspapers, and more. The automotive process helps in finding the potential attacks, vulnerabilities and security solutions for security threats in advance and allows not to miss out on security actions to be taken. In the automotive process, we will refer to various standards, regulations, frameworks, and community/forum suggestions as well. The automotive process will cover the needed artifacts as well. Items can be a system, subsystem (ECU) or an HW or SW component and more. The literature review covered the extended TARA part from the academia. But now for all three, the literature review will refer to non-academia references as well. In this methodology will also give one example for each.

A business/economy impact example is mentioned below which emphasizes the mandatory need for automotive embedded security. An increase in climate awareness worldwide has led to more usage of Electric vehicles. With this Electric vehicle (EV) manufacturing and sales and charging stations have increased drastically in smart/green cities. With this, power grids also are under threat. Such attacks on power grids have major business/economic and social impacts too. (Mohammad Ali Sayed *et al.* , 2021). An example of general attacks is mentioned in Table 2, which is also of importance as evolving automotive security needs to learn from the comparatively more evolved and old cyber security domains. In the thesis, more automotive attacks would be considered. The name of the attack tells where the attack happened and/or who got impacted majorly, though it is the familiar name given to the attack after its occurrence for future reference to further

discuss on it. The source and/or timeline column in Table 2 explains the type of attacks or from which entry point, attack surface attack was made and/or the time when it occurred. The impact column tells about the business suffered due to the attack and/or the user's loss. Personal data mentioned in Table 2: Generic cybersecurity attacks having major impacts. Source (Mohammad Ali Sayed a et al. , 2021)in the last row are sensitive items like personally identifiable information (PII), for example, the social security number connected to the name.

Table 2: Generic cybersecurity attacks having major impacts. Source (Mohammad Ali Sayed a et al. , 2021)

Name of the attack	Source and/or timeline and/or timeline column	Impact
Colonial Gas Pipeline in the US (United States) – (produces refined oil, 3 million barrels produced per day)	Ransomware (asks for a ransom amount to mitigate the impact)	Global increase in gas price
Solarwinds hack (Solarwinds is a network monitoring tool)	Compromised Orion software update.	Affected ~18,000 Solarwinds clients including many fortune 500 companies,

	Infected SW used by NATO, european parliament and other country's governments	high-security firms like US Department of Homeland Security, the US Department of Energy and the Center for Disease Control
Saudi Aramco hack (Saudi Aramco Information Technology)	2012	Affected 10% of the world's oil supply. 35000 computers were compromised(attacked).
US OPM hack (OPM- office of personnel management)	2014	21.5 million users' personal data were stolen. Penalty/fine/settlement of \$63M was made.

3.3 Automotive security process

For the automotive security process, will take references majorly from ISO21434 (www.iso.org., 2021) and UNR155 (Unece.org., 2022). Process and required artifacts and actions across the lifecycle will be described. The concept, design, production, maintenance and decommissioning stage/phase of the lifecycle is proposed to be covered. The concept will cover the TARA process, requirements, goals, claims and more. Supply chain management of security processes, actions, reviews and more also will be mentioned. Any certifications required and third-party actions like audit, certification, vulnerability analysis and more will be researched.

An artifact example is the TARA document from the supplier to be received in the concept phase and updated in the design and production phase. In each phase, there could be many artifacts that need to be worked upon/reviewed. An example of phase versus Artifacts is shown in Table 3. In rare cases, even post-production if any changes are made in the field, due to some new bug found and patched, TARA may have to be updated during the maintenance phase. In a chain of suppliers, each supplier would have many artifacts. Tier 1 can have one or more suppliers. Similarly, tier 2 can have a few software and HW vendors.

Table 3: Artifacts concerning each phase of the vehicle lifecycle

System development life cycle phase	Artifacts – security documents (reports/plan/design/architecture/guidelines/...)
Concept (includes proposal, requirements creation)	Ex: security concept, TARA

Design/architect and development/implementation	Ex: secure code review report
Production	Ex: SAST (static application security testing) report
Post-production/maintenance	Ex: Vulnerability analysis document
De-commissioning (stop usage)	Ex: Disabling security, deleting PII proofs

RASIC (Responsible, Accountable, Supportive, Informed and Consulted) needs to be prepared as shown in Table 4:.. Each of the teams/organizations has different roles. These roles are performed by a team in an organization in the supply chain. The R (responsible) team will perform the actual tasks primarily. The A (accountable) team will track the task to completion. The S (supportive) will assist R in the completion of the task. The ‘I’ (informed) team needs to be informed on the progress of the task mostly by the ‘A’ team. The C (consulted) team majorly will share the knowledge/guide with the R and S teams. For any task to be completed, one or multiple roles may need to be executed by one or the other organization in the supply chain. Each organization in the supply chain can have multiple roles and vice versa. However, the RASIC matrix in the thesis will not be created. May not take the specific case and just as an example can mention it in this methodology section. RASIC will be different for each vehicle manufacturer, as each vehicle manufacturer will have a different set of suppliers, and hence the supply chain will vary. In Automotive security, each customer needs to check the security compliance of their supplier. It is also mentioned in ISO21434 (www.iso.org., 2021) and UNR155 (Unece.org.,

2022). The sample RASIC matrix is shown in Table 4:. Here in the sample RASIC matrix, tier 2 and OEM are doing multiple roles for TARA of ADAS ECU. Supplier and consultation jobs are done by both tier 2 and OEM.

Table 4:Sample RASIC matrix for the ADAS ECU (sub-system) TARA artifact

Sample artifact	R	A	S	I	C
TARA for ADAS ECU	Tier1 ECU manufacturer	Tier1	OEM, Tier2	OEM	OEM, Tier2 SOC manufacturer

3.4 Security concept

In the security concept section will design a secure goals/requirements/claim. Security concepts will define the various major countermeasures like secure update, secure debug, secure download, secure communication and more. In extended TARA, these security concepts will be referred to for countermeasures/risk mitigations. Further equipment list will support the TARA attack path/tree descriptions. This attack equipment section very well maps to the attack section of the literature review, describing how attacks are made using those tools.

Generic security concepts/security claims/goals would be defined for secure communication, secure debug, secure diagnostics, secure download, secure update, firewall, IDPS, secure GW and more, after the automotive process is covered and before

taking various use cases for the item definitions plus extended TARA for each target assets. These concepts shall be referred to in the countermeasures section of extended TARA.

3.5 Item Definition

In item definition, first will pick a few sub-systems like ADAS, IVI, V2G, and Telematics ECUs. Second will draw the item definition diagram for those sub-systems. Item definition can cover a few things like the attack surfaces, assets under threat and the data source till the data finally reaches the destination, including the intermediate processing, data transfer protocols and interfaces and more.

For the Item definition example, a part of the vehicle system as an example as shown in

, is taken. ADAS and IVI ECU subsystems along with sensors and actuators are shown. The ADAS system receives information from sensors, processes it and sends the information to other connected systems and actuators. Sensors are camera, lidar, radar and ultrasonics. A connected sub-system example is IVI. Actuators examples are driving functions actuators like EPS (electric power steering), acceleration, and braking. Will further divide this item definition and expand to focus on one sub-system. An item definition could apply to more assets under the item and generally, that could be the case. Item definition in the thesis may have interfaces and more to cover up all the assets to be investigated for the sub-systems item definition. Will draw more item definitions for each sensor and/or asset under security research. During depiction, vulnerable paths and items will be shown bolder by increasing the width of the item edge or the line widths. In

all item's borders are bold, as all are candidates for separate sub-items for TARA execution with each having multiple assets to be investigated.

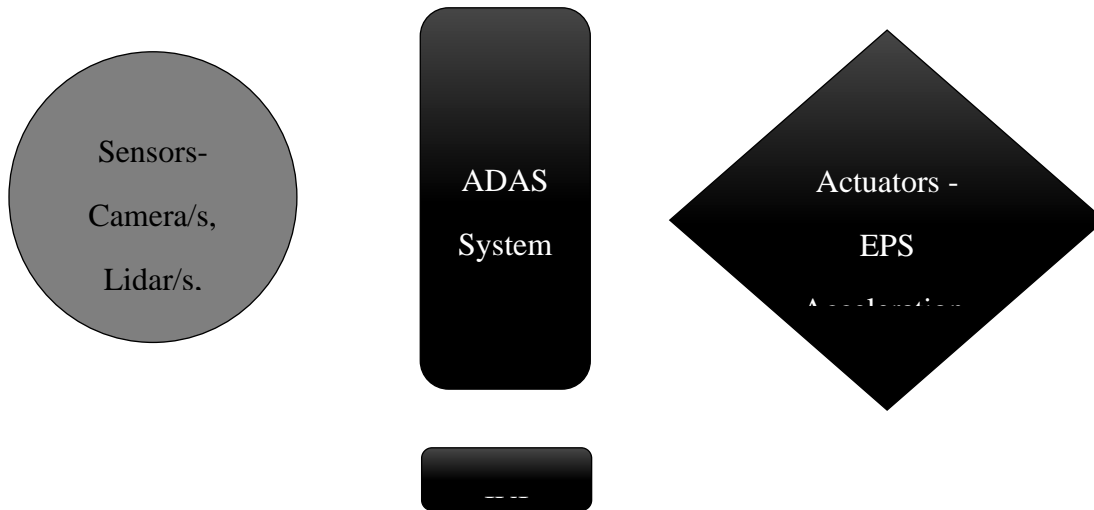


Figure 1: Item definition sample

3.6 Extended TARA

TARA would start with finding out the assets in those sub-systems that are under threat and/or vulnerable. Assets can be data being attacked, entry points for the attacks, vulnerable HW or SW modules and more. Secondly, would further investigate the threat scenarios, attack feasibility, damage scenarios, risk determination and risk mitigation for the selected asset for security investigation and protection. Identification of assets, executing the threat scenarios, attack feasibility, damage scenarios and risk determination are part of the TARA process. And TARA + risk mitigation could be said to extend TARA. This TARA could be performed right from the concept phase till the production phase too. For each asset also TARA could be updated, based on updates going further in the concept,

development and production phase of the lifecycle. In the threat section of the TARA execution, we would also see attack path/ attack trees.

The extended TARA proposed process will have asset identification, threat scenario using STRIDE, attack feasibility, damage scenarios for risk impact determination using STRIDE, risk valuation and risk mitigation. An asset can be many in an item. Like in the ADAS system, asset candidates are sensor data, trusted platform's FW (firmware), cryptographic keys and more. For each asset, an extended TARA will be conducted. An asset can be runtime data being communicated or stored static data. Data can be even a program, a configuration, a calibration file or other information. The attack part of the literature review is mapped inside the threat scenario. The vulnerability/weakness part of the literature review will be mapped inside the threat scenario, attack path or another part of the TARA or separately in TARA for the asset, vulnerability/weaknesses if any will be mentioned.

Threat scenarios will be explained using a text description and by attack path/attack tree analysis (ATA). Attack path/ATA will be depicted or explained using text. ATA will have different attack paths, explaining the means used/method/how and/or from where the attack is made, the attack objectives and/or the final attack intention/goal. Attack path if represented perfectly in item definition itself, then in extended TARA attack path depiction may be skipped and only scenario will be described.

Attack tree as shown in Figure 2 consists of nodes. 1 or multiple nodes will be there at each level. In the attack tree, the 'OR' gate is used in case there are multiple possibilities and the "AND" gate is used in case all the branch actions are required to achieve the target

step in the attack tree path. $A.B.(C+D) = G$, $E.F = G$, where A to G are various steps in the attack tree. In the thesis, an attack tree will be used partially, not depicting each attack scenario.

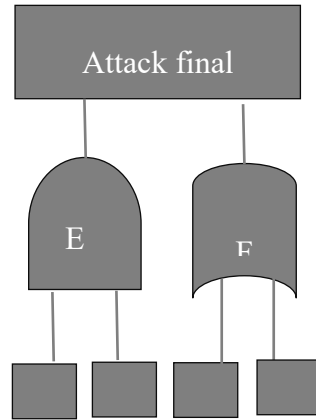


Figure 2: Attack tree

Attack feasibility rating will depend on the budget available for securing the vehicle at the OEM level and on items, which again depend on the supplier and OEM agreements. Here, the rating is given roughly, as it depends more on the business-specific factors. If some protection is mentioned in regulations, then it will be mandatory to protect. Attack feasibility for mandated protection mechanisms will be more. The total feasibility rating will be derived by adding the attack feasibility rating given against each factor as shown in Table 5. If the total is greater than 100, then stack feasibility shall be considered high. In brackets, values/ratings are given. These values would tell how feasible the attack is. Each attack parameter is given a different weightage and hence the values differ. More the ‘value’, the more feasible it would be to have a successful attack and vice versa. Weightage

rationale is based on the rough intuition of the importance of each attack parameter compared to the other attack parameter.

Opportunity window means the duration of an attack once the direct attack process is started till the success of the attack without getting detected and mitigated. Attack start could be finding the attack surface or accessing the asset under threat if the attack surface is priorly known. Elapsed time includes finding the weaknesses, developing the attack and further successfully exploiting the target asset.

Table 5: Attack feasibility estimation

Attack parameters	valuation rationale
Hacker expertise/knowledge	Layman/trivial (100) Medium (50) Expert (10)
Information availability to the Hacker	Public information (100) (example: data sheets) Restricted (10) (Example: i. network protocols used for specific communications, ii. supplier details (to avoid supply chain attack)

	Strictly confidential (0) (example- security manuals)
Hacking equipment/tool cost	Cheap (10) Medium (5) Costly (0)
Hacking equipment availability Note: Availability in the market and considering the legality of selling the equipment	Easily available (10) Can be assembled (5) Rare (0) (reason could be legal issues or costly or scarcity)
Hacker proximity/distance Note: distance to the vehicle or the equipment used for hacking	Remote/far (100) Local/nearby (10) Physical access (0)
Number of hackers Note: The expertise of each hacker is not considered to make valuation easier	1 hacker (10) 2 to 4 hackers (5) >4 hackers (0)
Number of equipment Note: Equipment can be the same or different	1 equipment (10) 2 to 5 kinds of equipment (5) >5 equipment (0)
Opportunity window (optional)	Always (15) Always during power on and/or running (10) Medium (5)

	Less or never (0)
Elapsed time	< 1 day (20) <= 1 day and <= 1 week (15) >= 1 week and <= 1 month (10) >= 1 month and <= 6 months (5) > 6 months (0)

In TARA, as part of risk assessment, one need to calculate the risk impact, quantitatively based on various parameters. SFOP (Safety, Financial, Operational, legal/Privacy) based risk impact measurement is done by adding ratings of each risk area. Table 6: Damage impact⁶ shows the damage impact. Here safety is given the highest risk rating as it is related to life and accident kind of safety concerns. Once the brand image has gone due to a potential attack, OEM, related suppliers and users' business is impacted, causing financial loss. Also due to the attack, when the vehicle undergoes damage, financial loss occurs to the user and/or vehicle insurer. Privacy breaches would impact the brand image and financial penalties once legal actions are taken. SFOP is rated as high/medium/low/nothing. The total SFOP impact rating is calculated by adding all the SFOP ratings. Impact rating is considered high if SFOP total is greater than 100. Similarly, medium if greater than 50. Low if greater than 10 and nothing/negligible for 10 or less.

Table 6: Damage impact

	S	F	O	P
Risk	High/medium/low	High/medium/low	High/medium/low	High/medium/low

	High=100	High=50	High=10	High=25
	Medium=50	Medium=15	Medium=5	Medium=12
	Low=0	Low=0	Low=0	Low=0

Table 77 shows the risk matrix. Each of the damage impact SFOP parameters is rated either high, medium or low. Risk in the risk matrix increases as the cell moves away from the left top and has the highest risk at the right bottom cell. Higher ratings among the impact and attack feasibility ratings will be considered risk ratings. The high, medium combination is considered high risk and similarly among low, medium combination, risk is rated as medium risk.

Table 7: Risk matrix

Damage impact (rows) vs attack feasibility (columns)	Low	Medium	High
Low	Low risk	Medium risk	High risk
Medium	Medium risk	Medium risk	High risk
High	Medium risk	High risk	High risk

Finally, countermeasures against STRIDE (Spoofing, Tampering, Repudiation, Information disclosure /leakage of info, Denial of service (DoS), Escalation of privilege) will be mentioned, which fulfill the risk treatment after finding the risks. Countermeasures

will be mentioned from terms defined in the security concept section. These countermeasures would protect various security properties of the data target from the chosen asset.

3.7 Extended TARA with a digital certificate as an asset example

Asset description: The certificate will have a public key of asymmetric cryptography, embedded in it. Certificates follow a specific format. Certificates are digitally signed for authorization of the right user. Certificates are securely stored. Data encrypted using the public key in the certificate can be decrypted by the recipient who has the private key. Table 88 represents a quantitative analysis of attack feasibility for each attack parameter along with the total attack feasibility rating calculation. For more details, Table 55 can be referred.

Table 99 shows the damage impact on quantitative analysis. For more details, Table 6: Damage impact6 can be referred.

Table 8: CA - total attack feasibility rating is $100 + 10 + 10 + 10 + 10 + 20 = 160 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Hackers need to be knowledgeable about cryptography, digital communication,

	certificates, diagnostics, UART, ethernet, CAN communication and more (expert-10)
Information availability to the hacker	Key and certificate details are not easily available as they are highly confidential (0)
Hacking Equipment cost	cheap, as it can be done remotely (10)
Hacking equipment availability	easily available as just a smart internet-connected device like PC (personal computer) is enough. Easily available (10)
Hacker proximity to the device	remote/far (100)
Number of hackers	1 hacker, so (10)
Number of equipment	1 pc (equipment) needed as just a smart internet-connected device like PC (personal computer) is enough (10)
Opportunity window	Always when it is power on (10)
Elapsed time	< 1 day (20)

Table 9: Sample damage impact is High (SFOP total=100+50+10 =160 (>100))

	S	F	O	P
Impact	High=100	High=50	High=10	Low=0

In

attack entry points from CAN, ethernet, OBD and UART are shown. It is a bottom-up approach, with attack entry points at the bottom and the final target achieved mentioned at the top. OR branch emphasizes that any of the entry points can be chosen by the attacker. AND will be used in case a sequence of actions is required to have a successful attack.

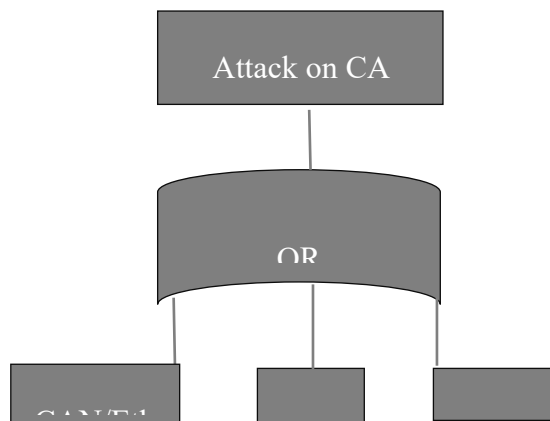


Figure 3: Sample attack tree for a digital certificate

Extended TARA has risk mitigation. There may be one or many risk mitigations. Have selected 'certificate' as an asset and hence sample certificate protection mechanisms

are explored here. Certificates need to be stored securely using secure storage principles. Certificates are accessible only to the related crypto functions. Secure communication to be followed like AUTOSAR's SecOC, message authentication and integrity using MacSec-based encryption of the message. Debug ports like UART to have the password protection mechanism if any. In general, UART needs to be disabled during the production stage. Secure diagnostics to be followed. Secure locking/unlocking of OBD ports needs to be followed. In the thesis, details of countermeasures derived from the security concept will not be repeated, as they will be covered in the security concept itself.

CHAPTER IV:

RESULTS

4.1 Research Question One: What is the automotive business/economic impacts? Who are the impacted stakeholders?

In the literature review lots of attacks, weaknesses, vulnerabilities and risk mitigations were covered, which also impacts SFOP and this impacts the business as well. Few more sources have been searched, mentioning the business/stakeholder impacts. Much news also speaks of future threats not ever imagined like charging stations for electric cars. Example source (Dudley-Nicholson, J, 2024). The conclusion is EV market is increasing but also needs secure charging and secure payment mechanisms in place before EVs are rolled out. V2G needs to follow a secure protocol. Figure 4 shows the size of the cybersecurity process market compared to cybersecurity solutions. The figure also depicts

how much cyber security processes take compared to others and a decade's progression. In the future, it is predicted that incident response, security regulatory implementations and certificate/auditing will take the least time compared to risk and software tracking. It also implies the automotive industry is heading towards SDV, open sources and standard software frameworks/architectures.

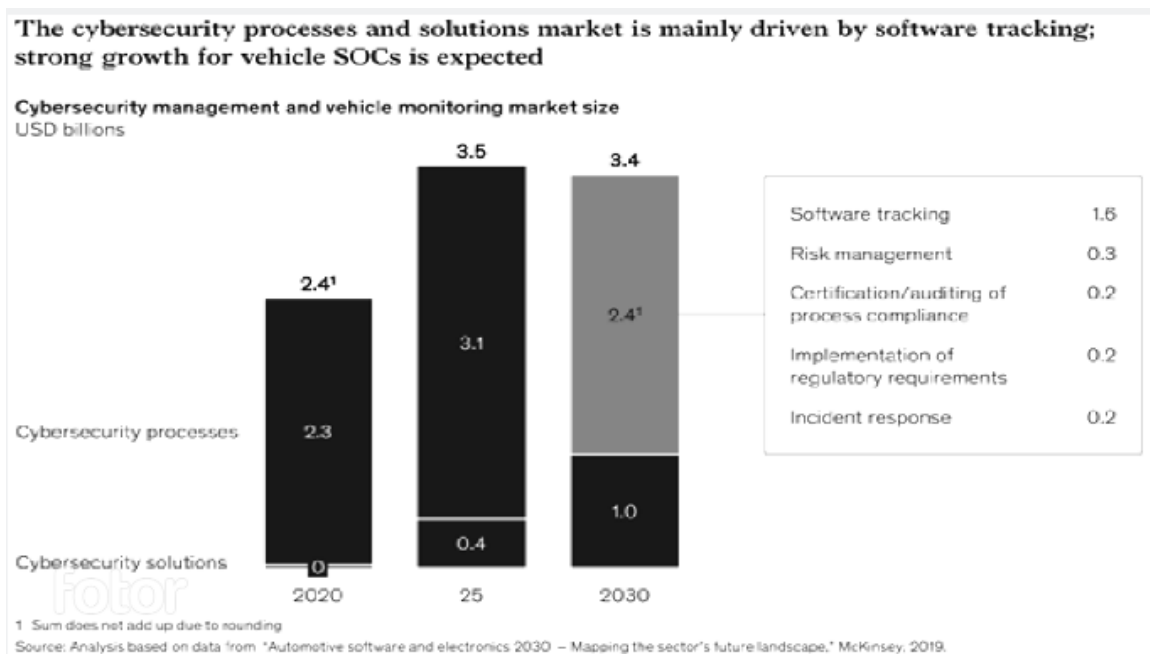


Figure 4: (<https://www.mckinsey.com/>, 2020)

4.2 Research Question Two: What automotive processes to follow? What are the different aspects of automotive processes?

There is mandatory UNR155 security process regulation and CSMS ISO21434 giving more details of the recommended security process across different phases of the vehicle lifecycle. UNR155 and CSMS ISO21434 does not emphasize much on how to do it and what all to do? Majorly it says security process to be followed to secure the vehicle to the best. In this section, will research on major steps required or to be followed in the process of securing the vehicle. Will mention the documents/artefacts for

automotive security process in sequence from beginning of lifecycle till end. Though artifact may be mentioned against some lifecycle phases, should be modifiable in the future based on need basis. So the Table 10: Automotive security process artifacts lifecycle phase for a artifact would imply that this artifact is initiated in that phase and majorly updated in that phase and is subject to the further changes if required in future phases which could be due to the new findings which could happen during TARA, supplier discussions, system integrations and many other reasons, business changes, change in regulations, standards and more.

Table 10: Automotive security process artifacts

Lifecycle phase	Automotive security process document/artefacts	Description
Concept phase	RFQ for security	During initial business initiation between the supplier and the immediate customer
Concept phase	CIA/DIA/RASIC	Interface agreement with suppliers on RASIC, who will do what and when
Concept phase	Security specification	Technical requirements are listed here
Concept phase	Cybersecurity plan – software, hardware, system level	Plan shall have the project and vehicle schedule, security RASIC of entire

		supply chain (at various levels, as per convenience like for example product, project, program, item based)
Concept till post-production phases	TARA	It contains attack, risk, mitigation details and again TARA is generally done at the system level
Design phase	Security architecture document	Security plan before implementation/development
Development phase	Security unit/fuzz/pen testing reports, code review proofs, SAST report, SCA reports	
Integration phase	Security integration/system/fuzz/pen test reports with maturity as per integration phase	
Production	Certification and Audit reports if applicable. Final verification and validation reports	

Maintainance	RCA reports	
Decomissioning	How securely it is decomissioned, need to be mentioned in writing and stored.	

4.3 Research Question Three: What are the various security goals, concepts, requirements and claims?

Security goals are the security measure/protection/intentions/claims. They are nothing but the headings of this section. Security concept will give lot of insights on security measures for various security goals in the form of use cases and/or security features, which will be referred to later during TARA and other sections. Security claims are security measure that are implemented in the real project. Security concept shall mention various security claims for each goal. Only some major security goals will be covered. Some specific use case security goals/claims/concepts shall be covered at a high level in the extended TARA.

Many times, the “shall” word is used for the security recommendations in the security concept. “must” is rarely used and is considered it to be mandatory but it depends project to project. Many are must but still “shall” will be used in many places considering possibility of various approaches and to make the securing mechanisms more flexible rather than rigid. Also “must” or not can be decided in real project scenarios depending on various factors. In security concepts for different security goals, can have same security

mechanisms, considering the similarity. Explanation is given in brief at higher level. But in reality, when we go deeper, the specific implementations may need to be done at a different place and/or differently implemented.

The security concept may look like a superset of the protection mechanisms for that particular use case. Each protection mechanism shall be explained in brief. It means, that each protection mechanism may have some implementation details or may not have, considering the vastness of each topic. Considering the business requirements, attack feasibility, risk level and various other factors, could implement a sub-set of it. This security concept does not claim that this is the only way to have the protection mechanism for a particular use case. There could be various other ways to implement security protection and other ways of security protection mechanisms. Below are the various security concepts.

In this security concept, have combined multiple requirements in a single statement to make it more compact considering the scope of security concept compared to other topics in the thesis. In real project security concept documents, it is recommended to have unique statements for each requirements.

4.3.1 Secure communication

In this section, will cover various communication channels along with generic runtime communication. Here secure communication framework standards for example, secOC of AUTOSAR, TLS, and more are not covered, and just at max is mentioned, as they are standard by themselves and can be referred to from publicly available sources.

4.3.1.1 Secure communication/run time data/data in transit protection (generic)

All critical data vehicle bus communications shall follow secure communication by authorization/authenticity of the sender and receiver. Secure communication shall follow various cryptography mechanisms like symmetric, asymmetric and hashing. Run time data confidentiality shall be protected by encrypting the data and sending and at the receiving end, shall be decrypted. Autosar SecOC communication shall be used for inter-ECU communication for critical data transmission. Critical data intra-ECU inter-process/processor communication shall be secured.

IDPS/firewall/secure gateway for critical data ECUs is a must. Gateway shall be achieved by having a dedicated SOC, scrutinizing the critical data and vulnerable communication channels like from ECU with external interface/s. Communication channel/network/data paths carrying critical data shall be isolated from ROW data paths. Access control to the critical data carrying communication channel shall be followed using least privilege with least needed permissions, IDPS/firewall/secure gateway and/or other kind of security mechanisms. A multi-layered defense approach to be followed, not just depending on security from one perspective. Each layer in the communication layer is to be protected for critical data flow. Shall have physical tamper-proof vehicle bus, interfaces and it's components.

4.3.1.2 Secure ethernet communication system

Secure Ethernet communication system shall have multi layer defense approach. All layers of ethernet communication shall have the security. Shall have robust IDPS/monitoring system and firewall policies. Shall have IDPS. Tight access controls shall be implemented for further securing ethernet communication. ECU and the ethernet bus, components, and interfaces shall be physically tamper-proof. Shall implement/support MACsec – AES GCM crypto to avoid unauthorized access to ethernet against spoofing/interception.

Shall encrypt the data to be transmitted, to avoid interception of data, for confidentiality and against replay attacks. Secure n/w (network) design to be followed by separating out the critical ethernet paths, from non-critical ones. Firewalling shall first blacklist all and then whitelist the needed ones. The firewall shall set the communication filtering rules for interfaces, IP (internet protocol) addresses of source and destination ports and more. Firewall rules shall restrict access to diagnostic ports. Ethernet port security policies shall be followed, like disabling unused ports, MAC address-based filtering and allowing limited MAC addresses per port.

4.3.1.3 Secure CAN communication system

Access restrictions shall be implemented by a. MAC based strong authentication mechanisms to control access to network resources, ensuring only legitimate traffic to flow in the CAN network and b. firewall (based on K-matrix, packet filtering, application level, HW circuit/session level checks) to be in place for authorized access. IDPS shall also detect, a. CAN calibration data mismatch detection and b. CAN message mismatch

detection. Upgrading to the latest CAN-XL is recommended as CAN-XL has more speed and more robust security protocols are supported compared to CAN security protocols.

One shall use the latest CAN stack. During maintenance, the patch shall be applied immediately for new CVEs found in CAN software. Supply chain security audits/assessments to be performed and submitted with proofs. Secure n/w design/architecting shall follow the appropriate n/w segregation/segmentation, isolation of critical data carrying traffic from normal data traffic and firewalls to prevent unauthorized access. Shall have physical security measures to protect CAN HW controller, transceivers and CAN bus from/against unauthorized CAN bus access. The HIL CAN fuzz test shall be done in advance to find any security vulnerabilities during implementation stage onwards at component level, ECU and vehicle integration level.

4.3.1.4 Secure inter SW, API communication security

Zero trust security models shall be followed even between software components. So, authenticate and authorize the IPC communications for data integrity, by using hash, MAC, digital signatures and encryption-based secure communications with supported TP (trusted platform)/HSM having cryptos and secure storage. But it may not be applicable for low attack feasibility. Unique session keys (for secure encrypted communication) and frequent timeouts are to be practiced. Each SW component/execution environment/process shall be sandboxed/isolated. Logging for suspicious/anomaly events/API interactions/client-server requests shall be done.

SW components traffic/requests/behavior shall be checked. Secure network design with n/w segregation/separation of critical paths from the rest. Secure - update/download/boot, bootstrapping, SW signing and verification, rollback-protection, Key management, RoT, CoT, secure storage, secure diagnostics and secure debug shall be followed. Shall introduce a dynamic attestation system among interacting SW components. Each such SW component shall provide a trusted state proof to a 'monitoring SW component'.

In inter-software components interactions, client-server mechanisms, API security shall allow only needed API/SW components to interact with other SW components, which could be said as a logical SW component firewalling. Client-server session timeouts shall be implemented. No continuous (persistent) sessions shall be allowed. Session management shall handle damage reduction and recovery. Input sanitization (against wrong parameters) checks shall prevent injection attacks. SW vulnerabilities shall be used for spoofing and tampering through physical attack.

API/user/SW component authenticity and authorization shall be done before starting the communication. If shared memory with IPC communication is used, then shall configure RO/WO and least privileges for the shared memory as per the need and file/resource access to be limited. Majorly WO shall be configured very judiciously to avoid any data unavailability by overwriting the data. Resources shall be isolated from other processes if not required. Strict inter-process isolation and segregation of resources

shall be followed. Resource/process shall be sandboxed. Shall use sniffers and track data leakages for protection against spoofing, replay attacks and confidentiality.

4.3.1.5 Secure LVDS communication systems

Shall transit encrypted data to protect against eavesdropping and tampering. Shall authenticate the data sources. Shall shield the cables against EMI interference. Shall avoid bundling the LVDS cable along with other power cables. EMI filters shall be installed to reduce interference. Voltage glitches shall be mitigated using electrostatic protected zener diodes. Shall have high frequency noise reduction ferrite beads. For protection against physical attack to LVDS components, shall securely enclose with tamper-evident seals. LVDS components shall be securely mounted. Supplier security checks shall be performed.

4.3.1.6 Secure GMSL communication systems

Shall have tamper-evident/anti-sniffing/anti-spoofing protection. Shall have secure communication in serdes-GMSL/LIN communications with authenticity, integrity and confidentiality checks. Not mandatory but voltage glitches shall be mitigated using electrostatic protected zener diodes. Shall have high frequency noise reduction ferrite beads on the cable for GMSL and for low frequency LIN, it is not mandatory.

4.3.2 Secure boot, secure download and secure update

Shall have RoT and CoT during secure download, secure update and secure boot. RoT shall have a hardware touch for RoT robustness. For example, the master key shall

be secured through hardware. Keys/certificates used shall be revoked on compromise or expiry. Recommended to have a dedicated firewalling SOC to reduce the attack surface for the target SOC for secure download and update, which further operates as a client-server or front-end back end with the back end communicating to the target SOC and front-end to the vulnerable system, connected to more vulnerable external interfaces.

Secure download code and data shall be signed cryptographically for integrity and authenticity. The image to be downloaded shall transit securely protecting the integrity and confidentiality by a robust hashing mechanism and secure communication protocols. Downloading code at the receiver end shall be verified for hash and signatures. Even for more robust secure downloads, images can be encrypted. In this case, secure download performance could be a concern and needs fast decrypting computing unit and a parallel and/or asynchronous mechanism.

Secure updates shall be atomic. Shall be performed with higher priority. Partial updates shall be avoided. Update failure recovery mechanisms like dual image booting and/or other mechanisms shall be supported. Always the next/future version update shall be supported by using counters and/or version numbers and thus ensuring rollback protection.

Secure boot shall load and boot first the most secure software like for example, bootloader, then secure OS, rich OS and finally application image. Keys and certificates shall be stored inside a trusted platform like HSM having dedicated secure storage, accessible only to the HSM critical components. Before every execution, shall check for

integrity of the code, calibration and configs to be executed, after power up, reset, suspend or other power states.

4.3.3 Cryptography systems

Should not use proprietary crypto algorithms. Should not use deprecated algorithms. Should use competitive robust future PQC proof algorithms. Crypto algorithms implementation shall be SCA attacks, brute force attacks and cryptanalysis proof by introducing needed redundancy and more to achieve a secure crypto implementation. For asymmetric cryptography, one shall use beyond RSA 2k, if supported. For symmetric cryptography, shall use AES 256 and beyond. In asymmetric, ECC is preferred compared to RSA. PQC-resistant algorithms shall be supported.

4.3.4 Secure diagnostics

Shall allow diagnostics functionality only on diagnostics tool connection and recommended for remote diagnostics as well. Diagnostics data shall be protected by encrypting critical once, securely storing critical data and by pseudonymization. Shall have strong access control with user authentication and/or strong password and password management like recovery and revoking on compromise or expiry. Shall have diagnostics tool setting authentication. Secure protocols should be used like TLS, SSH for critical diagnostics data transmission over network.

4.3.4.1 Secure key and certificate management and provisioning (secure VKMS)

Shall have various centralized systems for key and certificate/CAs management at ECU level, intra-vehicle level and at the cloud servers for key/certificate generation, revoking and for RoT and CoT for Keys and certificates.

Shall ensure secure key/certificates provisioning at the factories and during installation. Shall ensure secure key/certificate distribution using authentication and encryption related crypto mechanisms. Keys/certificates used during development shall not be used postproduction in vehicles. To the maximum possible extent shall have unique keys at the highest possible granular level for each purpose.

Shall have secure certificate/key lifecycle management covering new certificate/key generation the first time, after expiry, duplication, compromise and as a recovery mechanism. Secure certificate and key transfer/distribution and revocation shall be supported. Shall have continuous monitoring of certificate/key usage/access for detection of unauthorized access, duplication and compromise kind of suspicious activities. Response/incident reporting action shall be made for risk mitigation.

4.3.5 Secure debug

Shall not have debug symbols for executable codes to avoid debug and reverse engineering. Debug authorization shall be followed with robust mechanisms like having strong passwords, secure protocols and authentication checks of access control to only dedicated systems.

4.3.6 IDSM

IDSMS shall monitor the spikes/overloads and traffic rate limiters for protecting against DOS/flood/replay attacks compromising availability. Employ IDSMS to monitor network traffic for suspicious/anomaly activities to prevent or mitigate potential attacks. Develop and regularly update incident response plans to guide the organization's actions in the event of a security breach or attack. Shall support intrusion detection/management/reporting/event logging and storing mechanisms using Ethernet/CAN/LIN controllers in IDSMS.

Shall develop and regularly update incident response plans to guide the organization's actions in the event of a security breach or attack. Firewall rules in the network shall be set to support IDSMS. AI integration is recommended for IDSMS. IDSMS during the incident, shall support risk mitigation, recovery, avoidance, resolve the security issue and incident triaging.

Intrusion Detection/management/reporting/event logging and storing mechanisms using ethernet/CAN/LIN controllers in IDSMS shall do the following: a. CAN/eth blacklisted traffic (violated ID), b. traffic overload, c. flood attack detection on TCP protocol, d. bandwidth management, e. debug: manage unlock/lock the debug mechanism and reporting denied attempt to unlock, f. diagnostic: i. wrong usage reporting in the communication flowing through IDSMS's managed network, j. limiting the privileged diagnostic services, k. CAN calibration data and CAN message mismatch detection and l. filtered security events are reported and stored in persistent memory.

4.3.7 Memory protection

Flash integrity shall be maintained by using dm-verity in EMMC NAND flash memory in linux environment, at least for critical filesystems like for RootFS. Shall have CRC and parity checks like ECC and EDCC, if memory hardware supports. Shall use memory protection attributes like RO, WO, RW and execute judiciously by following least privilege principles. Shall have memory segmentations with secure memory regions too dedicated for TEE. Secure storage for keys/certificates shall be accessible only in TEE by only authorized firmware components.

Memory related compiler hardening flags shall be enable to harden the images to be loaded like ASLR, DEP, stack protection and buffer overflow. Sensitive data shall be encrypted and stored. Malicious access to memory shall be monitored, reported and risk shall be mitigated. Capability, task/role, privacy based access control shall be ensured. Sensitive data memory area, after no further use shall securely be disposed like using secure delete (overwriting with junk values). Process and VM memory isolation shall be maintained.

4.3.8 Secure logging

Logs logging and observation shall be allowed for legitimate purposes. Shall log security event. PII and other sensitive information logging shall be avoided. Forensic data shall also be attested with timestamp. Old data shall be regularly and judiciously deleted securely. Shall have redundant backups for critical data. Pseudonymization, encryption and secure transport kind of security mechanisms shall be used for sensitive data for privacy and confidentiality. Access to logs shall be limited and authenticity shall be

checked. Sensitive data shall be integrity protected/tamper proofed through signatures/checksums. Secure log storage shall also have WORM memory area for integrity of the critical data.

4.3.9 Supply chain security

Buyers shall have a security process to ensure they are getting secure component from the supplier. Buyers shall ensure that supplier support for maintenance and decommissioning of the component. Thus, the plier component shall be bonded to the buyer with secure life cycle process of the component. Buyer shall ensure HW or SW component is properly accessed at every stage of the life cycle, by buyer demanding different documents/reports like for SW components need to check SCA, SAST, DAST and IAST reports at the appropriate stage. Buyer shall demand security certifications and get PEN test done, depending on the component.

4.3.10 Secure software

To avoid SW vulnerabilities the following shall be performed: SCA, SAST, AST, IAST, DAST on the interacting SW components at both ends. Shall use secure compiler flags to harden the SW application against buffer overflows, program randomization and more such vulnerabilities. Should use secure kernel flags to harden the OS and SW component updates if any in the field as well. The latest patch shall be applied. The fuzz test and PEN test shall be performed for client-server interactions, inter-SW component interactions as a left shift mechanism for early detection and fixing of vulnerabilities/weaknesses.

4.3.11 Trusted environment

The trusted environment is getting used with various terminologies like TP, HSM, TEE, secure world, HSE and a few more. Various vendors use different names. Basic requirement of a trusted environment is HW crypto engine should have dedicated secure storage and its firmware shall boot earlier compared to rich OS and applications during secure boot process, immediately after the bootloader. Recommended to have dedicated host processor to take the related client's trusted environment service requests and interact with the crypto engine firmware. Suggest that crypto engine firmware only interacts with secure storage, majorly for better security.

4.3.12 Security - safety collaboration and interference resolution

During TARA, in SFOP impact analysis, safety impact is captured. All major and moderate safety impacts need to be intimated to the safety stakeholders. Residual risks after security measures are further handled with safety countermeasures in case the residual risk is still not acceptable.

4.3.13 Security testing and vulnerability analysis

Fuzz test and PEN (penetration) test are common security tests to be performed. Fuzz test depends on random inputs to find failures/vulnerabilities and pave the way for the specific input tests to check the robustness against the specific known and/or suspected vulnerabilities.

Vulnerabilities analysis for SW is done statically using code reviews, SAST, SCA (static code analysis) and by code complexity checks. While DAST provides run time

vulnerability finding. IAST provides both static and dynamic vulnerability finding. DAST is more favorable for black box testing of proprietary third-party codes. Static analysis is more of white box testing.

HW security testing needs tools for fault injections like EM-FI and FIB.

Cryptanalysis is done to check the crypto implementation robustness. A side channel attack is performed to know the cipher details like the algorithm used and crypto algorithm operation modes if applicable and the exact key length and key bits/value. Side channel attacks can be performed based on power, CPU noise and more. Side channel attacks based on power analysis are DPA and SPA and sound based in acoustic analysis. At different times, power consumption and sound of the CPU would vary and hence these attacks are also categorized under timing attack. The summary is, that one needs to perform attacks like this, to discover vulnerabilities and test the fixes/robustness of the implementation.

4.4 Research Question Four: Roughly how is the extended TARA to be executed in automotive security for various electronic components in the vehicle?

Extended TARA shall be executed for major ECUs and some specific use cases.

4.4.1 ADAS ECU

Majorly in ADAS ECU, will focus on sensors only. There are multiple types of sensors in the ADAS/AD system used in different environmental conditions and use cases. For each sensor will have a single TARA to make it more compact and less complex, though different types of sensors have different threats and damage scenarios.

ADAS SOC attack surfaces can be reduced by adding a dedicated gateway that does the IDSM and by prechecking software updates and downloads, by having client server architecture by using multiple SOC's. This countermeasure is common for all sensor protection. Further SDV-based architecture for ADAS SOC's and perception and signal processing SOC's having hypervisor-based isolation and virtualization through virtual machines shall enhance the ADAS ECU HW and SW security.

4.4.1.1 Camera

Asset description: Asset is data flowing from camera further through serdes, ISP, GMSL, LVDS and ethernet cables carrying video stream from camera source till the destination. Camera source data will go to the ADAS system for processing. Processed video stream meant for rendering to IVI HMI shall further be transmitted. Multiple cameras are used for different use cases like for external objects and internal monitoring. Here TARA will be performed combinedly for multiple use cases to keep it simple. In real project, performing TARA separately for occupants, external objects and driver monitoring is recommended.

Direct or indirect attack surfaces/entry points could be many like CAN, OBD, JTAG, UART, I2C and various communication channels used in the camera data path. Tools that can be used are for example: logic analyzer, exploitnano, JTAGulator, Arduino UARTFuzz tool, bus auditor and putty terminal/minicorn.

Threat scenarios could be many like changing the parameters/configurations of serdes, ISP and/or ADAS algorithms processing the camera data. Replay or DOS attacks,

with sending same data or stoppage could lead to freezing the camera output at the rendering HMI and/or decision-making entity. EMI and voltage glitches at LVDS can also tamper the video data. Data altering could be possible for compromised communication channel or image memory.

Table 11: Camera - total attack feasibility rating is
 $10+100+10+10+100+10+5+5+0 = 250 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Hackers need specific expertise on video data, GMSL and ethernet communication and serdes. Also, hackers need to know about embedded systems and automotive communications. So multilevel skills are required. Expert (10)
Information availability to the hacker	Video formats, GMSL, serdes, ethernet communication is publicly known. Public information (100)
Hacking Equipment cost	cheap, as it can be done remotely (10)
Hacking equipment availability	Standards tools like bus protocol analyzers, video tools and more are required (10)
Hacker proximity to the device	remote/far also possible (100)

Number of hackers	1 expert hacker also can manage, so (10)
Number of equipment	Video tools, bus analyzers, smart PC (equipment) needed. 2 to 5 equipment's (5)
Opportunity window	Could be easy only if before production itself, malicious code is integrated. Medium (5)
Elapsed time	In general, a few months (but an insider physical attack can just take some days and local diagnostics just some hours). >6 months (0)

Damage scenarios could be freezing the video data being fed, leading to safety issues while parking with parking camera data paths under attack. Safety issues could occur with stoppage of information leading to forward collision, lane deviation and more. Wrong image injection at compromised communication channel or image memory could be shown for example, potholes and patches in wrong lane could cause driver to change the lane, leading to accident.

DMC and interior cameras recording and storing the driver behavior and occupant's details could lead to privacy issues. Once dragged to court can lead to financial losses due to legal fighting expenses and can cause damage to the supplier's brand image. Camera can capture infrastructure details like traffic junctions along with map databases, GPS, AI-ML can find geographical details.

Table 12: Camera - damage impact is High (SFOP total=100+15+5+12=132 (>100))

	S	F	O	P
Impact	High=100	Medium=15	Medium=5	Medium=12

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures against related STRIDE are to follow secure communication of LVDS, GMSL, ethernet, memory protection, IDSM, supply chain security, secure debug and secure diagnostics mentioned in security concept. Also indirectly needs to protect the ECU itself by practicing secure CAN communication as mentioned in security concept. ADAS ECU shall have gateway SOC's in between ADAS core SOC's and IVI, telematics, VKMS and OBD kind of vulnerable and more external exposed ECUs. Shall have tamper proof ADAS SOC pins. Configurations related to LVDS, GMSL, ethernet and camera algorithms configurations shall be secured and securely updated. Physically tamper proof sealed LVDS, GMSL and ethernet cables shall be used. Installation of LVDS, GMSL and ethernet components should be done securely to avoid tampering.

4.4.1.2 Radar

Asset description: In a modern premium car there could be around 20 radars, with a few being internal radars monitoring the occupants and external radars to complement cameras at nighttime also. Radar signals pass through the ethernet communication channel. Radar signals are processed in radar processing units and sent to fusion ADAS ECU for

further decision making. Here assets to be protected are radar data, Radar processing unit ethernet channel and ADAS ECU.

Major attack surfaces/entry points could be radar sensor and ethernet communication channel. Threat scenarios could be jammers, jamming the radar signals, leading to unavailability or integrity of data. Radar processing unit configurations are vulnerable in case of hackers gaining the ethernet communication access and hacker's actions look legitimate.

Table 13: Radar - total attack feasibility rating is $10+100+0+0+10+5+0+10+0 = 135 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Hackers need jammers and remote access. Jammer's handling shall be considered at expert level. Hackers need to know the RF, automotive electronics communications and signal processing knowledge. Expert (10)
Information availability to the hacker	Automotive ethernet communication, RF communication and signal processing details are openly available. Public information (100)

Hacking Equipment cost	Jamming requires multiple equipment like RF generators, amplifiers, antennas and SDRs. Hence, the total cost will be more. Costly (0)
Hacking equipment availability	Legally radar jamming equipment is not available. Rare (0)
Hacker proximity to the device	Jammers need to be within RF range. Local/nearby (10)
Number of hackers	Multiple expert hackers are required, maybe 3 to 4 hackers. (5)
Number of equipment	A minimum of SDR, RF generators, spectrum analyzer, modulators, filters, receivers, transmitters, antennas and PC are needed. Greater than 5 kinds of equipment (0)
Opportunity window	Vehicle running is must (10)
Elapsed time	Ethernet-based remote attacks on ethernet communication hardly take a few hours, insider attack may take days, while the most difficult would-be physical jamming

	<p>which takes few months and interference attacks directly on the sensor will take many months.</p> <p>>6 months (0)</p>
--	--

Damage scenarios are many. Jamming the signal by sending same frequency signals. Spoofing is possible by generating fake object signals. Radar efficiency can be diminished by noise generation and electromagnetic radiation. Once the communication channel is hacked, radar data could be manipulated including the radar processing unit configurations. All this leads to safety concerns and vehicle operations concerns like steering, braking and acceleration malfunctioning due to passing of wrong decisions.

Internal and external radars on capturing the driver, occupants and external object movements with wrong intentions shall lead to privacy issues leading to legal and brand image issues and hence financial issues. Radar systems also interact with navigation systems like road/map database and GPS with its integrated geography matching algos to determine vehicle place and surroundings, which could be used for wrong intentions, leading to privacy breach.

Table 14: Radar - damage impact is High (SFOP total=100+15+5+12 = 132 (>100))

	S	F	O	P
Impact	High=100	Medium=15	Medium =5	Medium =12

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: STRIDE countermeasures are many. Spoofing could be avoided by authentication protocols, introducing cross checks by introducing redundant radars, isolating radar path from rest of the networks, encryption and signing using crypto digital signatures. Jamming could be avoided by using frequency hopping algorithms FHSS and by IDSM. IDSM could avoid eavesdropping. Interferences from EMI can be avoided by implementing adaptive filtering. Software vulnerabilities causing tampering of radar signal processing algorithms parameters, calibration and configurations could be avoided by having proper access controls, IDSM and following secure software as mentioned in security concept. Radar shall be physically securely installed.

4.4.1.3 Lidar

Asset description: Compared to radar, camera and ultrasonics, lidar is less used currently. Around 4 lidar sensors we can consider are installed in a modern autonomous level 2+ vehicle. Lidar uses laser pulses to measure the size of the object and radar signals for distance determination of the object and is effective during night times, especially in forest areas. Lidar sensor and serdes calibration/settings are the key for the right perception of the data. Lidar data reveals the location details.

Attack surfaces: Lidar light and radar signals at transit are susceptible to attacks during transit. Serdes I2C control communication channel, LVDS and ethernet communication for lidar data transit are also vulnerable to attacks. Malicious additions in

the supply chain could pose a threat. The vicinity of the lidar sensor itself could be physically threatful.

Threat scenarios: Spoofing and tampering of the data is done by sending fake or old object signals, sending the wrong distance of the object and thus creating phantom objects, jamming by EMI, sending same frequency lidar signals and sensor settings/calibration data tampering through unauthorized remote or physical access. Signals could be made unavailable with DOS attacks through malicious SW injection and execution and flooding. Reflecting lidar signals physically is also a threat.

Table 15: Lidar - total attack feasibility rating is $10+100+0+5+10+5+0+10+0 = 140 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	<p>Hackers need to know about lidar data formats and signal processing. Serdes, laser beam forming and radar, I2C, LVDS and ethernet communication knowledge are needed. Cybersecurity, automotive embedded electronics debug and diagnostics knowledge is essential. AI-ML knowledge is required for sophisticated attacks.</p> <p>Expert (10)</p>

Information availability to the hacker	<p>Forums, communities, technical papers, reports, industry publications, open-source codes and open-source projects, vendor's data sheets and manuals, automotive vehicles, ethernet, LVDS and RF communication details are publicly available. Laser and radar signal processing and perception and fusion algorithms knowledge need to be acquired. Plenty of courses are available for AI-ML for advanced automated attacks.</p> <p>Majorly public information (100)</p>
Hacking Equipment cost	<p>Lidar spoofing and jamming require many kinds of equipment like lidar signal-detecting oscilloscopes, RF generators and SDRs costing in total thousands of dollars.</p> <p>Costly (0)</p>
Hacking equipment availability	<p>Customized lidar equipment is not available and could be made by integrating many electronic parts by buying from the electronic dealers.</p> <p>Can be assembled (5)</p>

Hacker proximity to the device	<p>Physical and local attacks need to be performed from a nearby distance.</p> <p>Note: Remote attacks also are possible considering what attack and attack surface is considered.</p> <p>Local/nearby (10)</p>
Number of hackers	<p>Diversified 3 to 4 hacker experts are required.</p> <p>(5)</p>
Number of equipment	<p>A minimum of lidar-specific oscilloscopes, photodetectors, laser diodes, SDR, RF generators, lidar emulators, PC and more are needed.</p> <p>Greater than 5 equipment (0)</p>
Opportunity window	<p>During vehicle motion only (10)</p>
Elapsed time	<p>Direct sensor attacks would be difficult and time consumed remote attacks on communication channel may just take a few hours.</p> <p>> 6 months (0)</p>

Damage scenarios: Getting wrong information like the wrong location of the object or the wrong object itself or the unavailability of the signal itself. High-power laser signals can blind the laser part of the lidar sensor. Wrong control information coming from the compromised radar-related data path.

Table 16: Lidar - damage impact is High (SFOP total=100+15+5+12 = 132 (>100))

	S	F	O	P
Impact	High=100	Medium=15	Medium =5	Medium =12

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: IDSM secure diagnostics, secure debug and secure communication as explained in the security concept for ethernet, CAN and inter SW secure communication shall be incorporated. IDSM shall be capable of detecting DoS attacks. IDSM shall do integrity check of lidar data by crypto secure communication checks and localization mechanisms like secure logging of anomalies along with timestamps, spatial analysis and audits. Abundant backup mechanisms with the addition of redundant sensors and other recovery mechanisms shall be implemented. Lidar light beams blinding impact shall be reduced by having appropriate AGC algorithms.

Serdes I2C communication to be authorized and access controlled. Additional redundant sensors and runtime lidar sensors settings changing mechanisms shall be used to adapt to changing reflective and jamming attack situations. Additionally, to mitigate the reflective attack, lidar shall use many lidar scanners/lidar signal beams and thus diversify

the beams, making attack difficult. FHSS shall be used against the same frequency jamming attack. Physically secure enclosed/placed, grounded (to chassis) and metal-shielded sensors shall avoid the reflective and interference attacks. EMI filters shall be installed in the lidar signal/power supply lines to suppress HF noise. Algorithms to change the FOV at run-time, to reduce the impact of physical obstruction attacks shall be supported.

4.4.1.4 Ultrasonics

Asset description: There could be few to too many ultrasonics surrounding the vehicle. It is used to detect objects' distance during parking and other operations and is the cheapest of other sensors like camera, lidar and radar.

Attack surfaces and threat scenarios: The ultrasonic sensor receiver itself is the major attack surface along with the ultrasonic data communication path. The ultrasonic sensor has exploitable blind spots. Ultrasound emitting devices can be used by attackers for interference, spoofing and blind spot exploitation attacks. Fake objects could be mimicked at the wrong location by tricky timing of the ultrasonic wave pulse echo.

Table 17: Ultrasonics - total attack feasibility rating is $10+100+10+10+10+5+0+10+0 = 155 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating

Hacker expertise	Hackers need to know about Ultrasonic sensor components, embedded systems, cryptography, signal processing and more. Expert (10)
Information availability to the hacker	All expertise items are available publicly. Majorly public information (100)
Hacking Equipment cost	Ultrasound emitting devices, signal analyzers, ultrasonic transducers, microcontrollers and amplifiers are worth 100 to 1000 dollars. Costly (0)
Hacking equipment availability	All the equipment is easily available. Easily available (10)
Hacker proximity to the device	Blind spot exploitation, reflective, jamming and interference kind of attacks need to be done from nearby. Note: SW vulnerabilities can be exploited with remote attacks through wireless and then intra-vehicle networks. Local/nearby (10)
Number of hackers	2 to 4 hackers with expertise in various domains are required.

	(5)
Number of equipment	Multiple equipment's shall be required like signal analyzers, PC, ultrasonic wave emitters, transducers, amplifiers, embedded microcontrollers and more. Greater than 5 equipment (0)
Opportunity window	Vehicle in motion is a must (10)
Elapsed time	Attack on ethernet channel will take few hours while the attack on sensors directly will take many months. > 6 months (0)

Damage scenario: A spoofing attack creates a fake object at the wrong location creating safety concerns for the vehicle and nearby environment stakeholders. Jamming and flooding attacks can reduce the functionality of the ultrasonic sensor to the extent of making the ultrasonic sensor functionality unavailable.

Table 18: Ultrasonic - damage impact is High (SFOP total=100+15+15+0 = 130 (>100))

	S	F	O	P
Impact	High=100	Medium=15	Medium =15	Low =0

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Follow secure communication for FlexRAY, ethernet and CAN communication. Multiple ultrasonic sensors will help with recovery mechanisms and cover all spots for object detection, thus avoiding any blind spots and its exploitation. Ultrasonic frequency hopping will help with acoustic interferences causing flood attacks, DoS attacks and cloaking attacks. Tamper evident seals are recommended for ultrasonic sensors to cause any damage physically.

4.4.2 IVI/digital cockpit ECU

IVI is very rich in HMI with lots of user-usable interfaces like display menus, USB for audio video, SD-card for navigation (optional and will be there in integrated navigation GPS receiver), wireless interfaces like satellite and AM/FM radio, Wi-Fi and bluetooth for mobile interactions and sensor-based interfaces like voice and gesture recognitions where in even audio mic and camera is integrated. Other common interfaces are CAN, LVDS, GMSL and ethernet. Lastly also has debug (JTAG, UART) and diagnostics interfaces.

4.4.2.1 IVI to mobile communication

Asset description: Wi-Fi, bluetooth and wired USB are used for mobile to IVI and IVI-to-mobile communication for features like bluetooth music, navigation, bluetooth telephony and miracast/screen mirroring. Dedicated apps like android auto with android OS-based mobiles, car play for apple smartphones and car life for Symbian OS-based phones are used for mobile messaging, calling and navigation projection to IVI from

mobile. TCP-IP protocol runs over Wi-Fi and USB for android auto, car life and car play kind of features.

Attack surfaces and threat scenarios: Hacked mobile or hacker's mobile, wireless and wired communication channels with and without TCP-IP protocols and vulnerabilities in Wi-Fi, bluetooth kind of SW stack could be the attack entry points. Insecure OBD or offboard diagnostics and unprotected debug ports like JTAG and UART can also be the attack surfaces.

Table 19: IVI – mobile communication - total attack feasibility rating is $10+100+10+10+10+5+0+10+0 = 155 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	<p>Hackers need to know about wireless communications like Wi-Fi, bluetooth and its SW stack. Hackers also need to be knowledgeable of TCP-IP and USB kind of protocols. Hackers should be aware of embedded systems interfaces like UART and JTAG-based debug mechanisms. Hackers should be aware of android auto, car play, car life, bluetooth music application services.</p> <p>Expert (10)</p>

Information availability to the hacker	<p>All required knowledge is available publicly.</p> <p>Majorly public information (100)</p>
Hacking Equipment cost	<p>Hacking mobile is required majorly.</p> <p>Cheap (10)</p>
Hacking equipment availability	<p>Mobile availability should not be an issue.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>Attacks need to be done locally.</p> <p>Note: A remotely compromised externally connected ECU and a remotely compromised intra vehicle network is also a possibility.</p> <p>Local/nearby (10)</p>
Number of hackers	<p>Diversified multiple security experts for test, vulnerability analysis, BT, Wi-Fi, TCP-IP, network scanning experts and reverse engineering may be required.</p> <p>Minimum two specialists (5)</p>
Number of equipment	<p>At least two kinds of equipment shall be required for GPS/navigation system attack among SDR, RF analyzers, directional antennas, PC and navigation signal</p>

	<p>mimicking devices/simulators. Along with mobile, one or more equipment may be required like network scanners, HWs like GSM modulators/SIM emulators along with PC may be required.</p> <p>2 to 4 equipment (5)</p>
Opportunity window	IVI power on is must (10)
Elapsed time	<p>Expertise on Wi-Fi/BT, android auto, carplay and more is required. To achieve that expertise, it will take at least a few weeks. Finding vulnerability may take many months.</p> <p>>6 months (0)</p>

Damage scenario and impact analysis: Location, PII, voice/conversations inside the vehicle, phone details like call details, contacts, etc... can be stolen through eavesdropping/privacy/confidentiality breach without any tools. Stealing of financial credentials may affect toll payment and illegal transactions could happen. Such privacy/confidential breaches cause damage financially, legally, trust and brand image. Fixing vulnerabilities would affect maintenance/production/service costs due to recalls and SW updates, in case the SOTA feature is absent. ADAS uses IVI to display the camera and other inputs for safety. If IVI is compromised, then safety is impacted heavily.

Table 20: IVI – mobile communication - damage impact is High (SFOP total=100+50+10+25 = 185 (>100))

	S	F	O	P
Impact	High=100	High=50	High =10	High = 25

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Wi-Fi/BT/USB, android auto, carplay, carlife and all related software stacks are to be kept updated with the latest security patches applied. Need to use secure protocols like TLS/HTTPS for all network layers. Authentication and authorization are to be checked for the mobile device. Encrypted communication is recommended for sensitive data like display frames and needs to be stored securely so that malicious mobile devices cannot access it and/or cannot decrypt it.

4.4.2.2 IVI miscellaneous interfaces

Asset description: Multimedia USB, navigation SD-card and GPS antenna receiver, DAB/FM/AM, apps, UART and JTAG port are the interfaces in IVI other than IVI-mobile interfaces.

Threat scenarios and attack surfaces: USB-based storable devices like USB-stick/pen drive and SD-card could have malicious executables that could auto-execute during access to USB device and SD-card, if not secured appropriately. Also, auto executables once copied could start self-execution. Malicious multimedia files can have headers with metadata having malicious executables. The file once copied and/or during

header parsing, can start auto-execution in case of any vulnerabilities in the multimedia software used for parsing and/or playing. AM/FM/DAB and GPS wireless signals are remotely and locally (like other RF based sensors like radar, ultrasonics and lidar) hackable. Malicious app installation by mistake or by insider attack could be an easy entry point for attackers.

Table 21: IVI – miscellaneous interfaces - total attack feasibility rating is $50+100+10+10+10+5+5+10+20 = 220$ -> high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	<p>Attackers should know about GPS, AM/FM/DAB-based wireless communication, multimedia file formats, decoding mechanisms, parsing and playback, USB/SD-card file systems, malicious app creation and more.</p> <p>Note: Not all needs to be known but knowledge of one attack surface also is enough.</p> <p>Medium (50)</p>
Information availability to the hacker	<p>All required knowledge is available publicly.</p> <p>Majorly public information (100)</p>

Hacking Equipment cost	<p>USB stick/SD-card is cheap. Wireless communication hacking is possible locally and/or remotely and hence is cheaper. Malicious multimedia file and app creation is easy for the expert.</p> <p>Cheap (10)</p>
Hacking equipment availability	<p>USB stick/SD-card is available in abundance and nearby, in almost any laptop or mobile shop. Wireless communication hacking equipment may be moderately difficult concerning availability. Malicious multimedia file-generating tools may not be that easily available. Malicious app generation tools nowadays may be available but illegal and hence may not be that easily available.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>Attacks need to be done nearby/locally.</p> <p>Note: A remotely compromised externally connected ECU and a remotely compromised intra-vehicle network is also a possibility.</p>

	Local/nearby (10)
Number of hackers	<p>Diversified multiple security experts for GPS-navigation, audio broadcast, USB, SD-card experts are required.</p> <p>Minimum two specialists considering one or two attack surfaces (5)</p>
Number of equipment/tools	<p>At least two kinds of equipment are required. HWs like GSM modulators/SIM emulators along with PC may be required to compromise the navigation system.</p> <p>Tools like USB rubber ducky for keystroke injection of malicious scripts or commands and reverse engineering tools for debugging, disassembling and decompiling are used for physical attacks.</p> <p>Firmware emulators can be used to understand firmware and modify it. USB drive and/or SD-card read-write to add dangerous files and execute specific or arbitrary executables/code. USB armory, a USB port-connected board, can be used by hackers.</p>

	<p>Most of the above equipment/tools are used physically or locally and remote is less.</p> <p>2 to 4 equipment (5)</p>
Opportunity window	IVI power-on is a must (10)
Elapsed time	<p>Vulnerable software stacks of USB/SD-card, navigation, multimedia and radio with poor detection and protection mechanisms can allow an attack to happen in some seconds.</p> <p>< 1 day (20)</p>

Damage scenario and impact analysis: Through USB/SD-card and multimedia files one can inject malicious code/executables which could run automatically as well, leading to the possibility of denial of infotainment services, PII data theft, wrong information like wrong navigation details and more. Radio interference can lead to loss or manipulated information like wrong traffic/location information, leading to dangerous locations, travel time delays and more. Safety will go for toss with wrong navigation information. Privacy breaches would happen with stolen PII. Financial losses would follow due to the fall of brand image and legal issues and operational failures due to false decisions by the system and more.

Table 22: IVI – Miscellaneous interfaces - damage impact is High (SFOP total=100+10+10+25 = 145 (>100))

	S	F	O	P
Impact	High=100	medium=10	High =10	High = 25

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Each of the attacks surfaces-related SW stack, i.e. for USB, sd-card, GPS/navigation system and multimedia radio are recommended to be isolated from other applications and/or processes by following sandboxing and virtualization. Access controls to be in place for protecting critical data and the discussed interfaces acting is attack surfaces. Secure communication to be followed in GPS/navigation system. Firewall to be followed in the interface ports to accept interaction with chosen sd-card and USB devices only. Secure debug and secure update to be followed.

4.4.3 Telematics ECU

Asset description: Telematics ECU is also called TCU (telematics control unit). Telematics ECU is a middleman for all other ECUs to the cloud server. TCU-to-cloud communication is also called V2C. It uses cellular or satellite-based or Wi-Fi-based long-distance communication. Telematics sends a lot of vehicle data to external servers. Vehicle data could be of the vehicle location like GPS data, fuel level, engine temperature and more. It also does OTA software updates.

Threat scenarios and attack surfaces: V2* communication channel is the specific attack surface in TCU. A major specific threat in TCU is from remote wireless communication. Also, the vulnerable ethernet and CAN-based vehicle communication is a threat. The vulnerable TCU software itself could be an entry point of attack. Telematics is a major entry point for attackers due to its external connectivity.

Table 23: Telematics - total attack feasibility rating is
 $50+100+10+10+100+5+5+10+20 = 310 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	<p>Attackers should know about GSM cellular/satellite/Wi-fi wireless communication. Attackers need to know about vehicle networks and more.</p> <p>Note: Not all needs to be known but knowledge of one attack surface also is enough.</p> <p>Medium (50)</p>
Information availability to the hacker	<p>All required knowledge is available publicly.</p> <p>Majorly public information (100)</p>
Hacking Equipment cost	<p>Basic attacks are free or cheaper, costing a few dollars. Many remote hacking tools are</p>

	<p>available for free like wireshark, nmap, metasploit, burp suite and more. SDR (software-driven radio) costs also start from a few dollars and are hence cheaper. Whereas RF jammers and interceptors used for advanced attacks seem comparatively costly. HW equipment needed for physical attacks through USB and JTAG interfaces is cheap. Oscilloscope and logic analyzers may be costly, but considering it may be already owned, it may not be costly for attackers.</p> <p>Cheap (10)</p>
Hacking equipment availability	<p>All required types of equipment are legally available except for RF jammers and interceptors used for advanced attacks.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>Most specifically, here wireless communication is considered majorly and it could be attacked remotely.</p> <p>Remote/far (100)</p>

Number of hackers	Even one expert hacker could be enough for a remote attack. (10)
Number of equipment/tools	For a remote attack, just a PC with a freely available wireless communication tool would be enough. 1 equipment (10)
Opportunity window	Telematics ECU power-on is a must (10)
Elapsed time	Vulnerable software stacks of wireless communication, vehicle networks and wireless communication with poor detection and protection mechanisms can allow an attack to happen remotely in a few minutes. < 1 day (20)

Damage scenario and impact analysis: Through remote attacks in case of poor security in wireless communication, one can jam the network and introduce noise in the communication by manipulation of wireless waves. Vehicle theft in the fleet shall be easy. Services like SW updates may get delayed due to the larger downtime of the telematics ECU. Leakage of vehicle information like location, decisions of the driver and more are sensitive and those PII information could cause legal issues and hence financial loss can

incur. Manipulation of vehicle operating decisions could cause safety and operational issues.

Table 24: Telematics - damage impact is High (SFOP total=100+50+10+25 = 185 (>100))

	S	F	O	P
Impact	High=100	High=50	High =10	High = 25

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Since Telematics ECU has maximum risk, SFOP, safety, financial, operations and privacy, each being maximum, needs best security protections. Since it is most vulnerable to remote attacks, wireless communication data for sensitive data shall be encrypted and sent for confidentiality. A hashing/signature mechanism shall be used for the integrity of the data. Since TCU is very critical for software updates of all the ECUs and for vehicle data, it should also have strong physical protection along with SW and HW IDPS mechanisms.

4.4.4 V2X (vehicle to everything)

Asset description: V2X ECU can have Wi-Fi and existing cellular-based communication (C-V2X). It can interact with pedestrians wearing/embedded with smart devices and infrastructure like traffic lights, cellular RSUs/base stations and satellites. RSU/base station can use either Wi-Fi or cellular communication. Satellite communication is cellular based. V2V uses DSRC (Wi-Fi-based) or C-V2X communication. Even NFC is

used for secure short messaging in V2V like exchanging vehicle authorization for V2X communication and more and in V2I like finding the nearest empty parking areas, toll and parking fee payments, fleet management like goods tracking, automated vehicle entry tracking and more. NFC could also be used for traffic congestion and hazard alerts, accident location reporting, vehicle details, medical information during emergencies and many more.

Threat scenarios and attack surfaces: The V2X communication channel is a major remote attack surface. Tampering traffic signal data and GPS data could lead to severe safety issues. Sensitive vehicle data read from the cloud or V2X channel would lead to privacy breaches.

Table 25: V2X - total attack feasibility rating is
 $50+100+10+10+100+10+5+10+20 = 315 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Attackers should know about GSM based cellular and/or Wi-Fi6-based DSRC wireless communication. Attackers need to know about cloud and vehicle networks. Vehicle identity cloning along with corresponding short-duration pseudonymous PKI is challenging.

	<p>Note: Not all needs to be known but knowledge of one attack surface also is enough.</p> <p>Medium (50)</p>
Information availability to the hacker	<p>Knowledge is available publicly for basic attacks.</p> <p>Majorly public information (100)</p>
Hacking Equipment cost	<p>V2X radio communications can be analyzed through SDR (software-driven radio) which are available cheaply for a few dollars. Packet analyzers and simulators for the network protocol stack of V2X can be used and checked for vulnerabilities by generating real-world scenarios before hacking using USB, JTAG, oscilloscope, logic analyzers and costly RF interceptors and jammers.</p> <p>Medium (10)</p>
Hacking equipment availability	<p>SDR simulators, USB and JTAG-based HW are legal except for RF interceptors/jammers used for</p>

	<p>eavesdropping and DOS-like sophisticated attacks.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>Remote for cellular, local for NFC and DSRC, and physical for HW interface-based attacks are possible. Here for rating most easy cases will be considered.</p> <p>Remote/far (100)</p>
Number of hackers	<p>Remote attacks can be done single-handedly. One hacker also could be enough (10)</p>
Number of equipment/tools	<p>For a remote attack, at least a PC with a simulator tool is needed. So at least one piece of equipment and one tool is needed.</p> <p>2 to 4 equipment (5)</p>
Opportunity window	<p>V2X-related ECU power-on is a must with a vulnerable V2X communication scenario.</p> <p>Power-on/ ECU running is must (10)</p>
Elapsed time	<p>A replay attack can be the shortest one with elapsed time of just a fraction of second to some minutes.</p>

	< 1 day (20)
--	--------------

Damage scenario and impact analysis: Eavesdropping of V2X data causes confidentiality/privacy breaches of PII data like localization information. Spoofing/data manipulation of V2X data causes authenticity breach with lots of safety, financial and operation issues. Replay and DOS attack cause data/service availability issues and lead to safety and operation issues, further leading to financial issues as well.

Table 26: V2X - damage impact is High (SFOP total=100+50+10+12 = 172 (>100))

	S	F	O	P
Impact	High=100	High=50	High =10	Medium = 12

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: V2X channel needs to be hardened. Cryptography to be used for authenticity/authorization and data encryption of V2X data. Short-term pseudonymous PKI shall be used. IDPS shall be in place to detect and prevent any malicious activities over V2X channel. FHSS/DSSS physical method shall be used to keep hackers in bay by using a wider spectrum. Geolocation and V2V collaboration shall be used to detect and communicate any jamming efforts. Dynamic power variations and directional antennas shall be in place to mitigate jamming efforts. Diversified channels shall be used to mitigate jamming efforts by using both DSRC and C-V2X.

4.4.5 Keys and certificates in-vehicle ECUs

Asset description: Cryptographic keys and asymmetric cryptography certificates are the main security pillar assets in-vehicle electronic system's cryptography-based security. These are used to maintain privacy/confidentiality, authentication, non-repudiation and integrity of the data. Certificate and key generation/management/revocation/life cycle management, certification issuing and installation and Key provisioning uses a process, protocol and communication shall be considered as assets to be protected.

Keys are used for encryption and decryption. Keys and certificates are stored securely in trusted platforms also called secure storage and are access controlled. Keys can be symmetric or asymmetric. The same symmetric key is used for encryption and decryption and hence needs to be kept confidential and known only to the encryptor and decryptor. In an asymmetric key, the private key is with the owner and is confidential and used for encryption/signing.

Certificates can be TLS/SSL types, with x.509 and other standard formats and released by multiple CAs. There is a possibility of a secure chain of certificates. Root, intermediate and leaf/end-entity certificates. The public key is generally embedded in certificates. PKI is a superset of CA, which also has RA, OCSP and CRL. RA helps CA in certificate-related processes/tasks and certificate requestor verification, CRL in revocation and OCSP for runtime checking of certificate status.

Threat scenarios and attack surfaces: Various side-channel attacks are possible to decode the private keys and symmetric keys. Analysis can be done for power, acoustic and timing during key operations to decode the key. Poor crypto algorithms and deprecated

ones could be more vulnerable to cryptanalysis attacks. MITM attack is possible during unsecure communication during key and certificate usage in secure communication, distribution, installation/provisioning leading to false identity, eavesdropping/confidentiality, data integrity breach, malicious code signing and more depending on the various use cases. Unsecure key/certificates storage leads to key stealing and hence misuse.

Table 27: Keys and certificates in-vehicle ECUs - total attack feasibility rating is $50+100+10+10+0+5+5+10+10 = 200 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Attackers should know about cryptography, all vehicle communications, ECUs and more. Shall be able to exploit once vulnerabilities are known. Reverse engineering, side-channel attack, certificate and key generation, distribution, secure storage, trusted platforms, PKI, VKMS, certificate formats and more expertise also may be required. Tracking CVEs and CWEs also may give some hints to hackers.

	<p>Note: Knowledge of one or few attack surfaces is enough.</p> <p>Medium (50)</p>
Information availability to the hacker	<p>Knowledge is available publicly for basic attacks.</p> <p>Publicly available information (100)</p>
Hacking Equipment cost	<p>Advanced HW based tools will cost beyond 500\$ and SW based basic tools will cost less than that. Side channel attacks may need some costly oscilloscopes/analyzers too.</p> <p>Medium (10)</p>
Hacking equipment availability	<p>Diagnostics tools are readily available and most of the equipment is easily available.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>Many side-channel attacks need physical proximity. Wired diagnostic port access being the easiest entry also needs physical proximity. Key and certificate hacking is a sophisticated job and could be comparatively easier with local presence rather than remote hacking. During key and</p>

	<p>certificate distribution, installing/provisioning, hacking may be an easier task for insiders which again needs a local presence. Remote hacking during distribution and communication is possible and again difficult as generally key and certificate-related operations are protected using cryptography.</p> <p>Physical/local (0)</p>
Number of hackers	<p>Remote attacks can be done single-handedly but here physical proximity is required and hence it may take at least 2 hackers for a comfortable hacking.</p> <p>2+ hackers (5)</p>
Number of equipment/tools	<p>Generally, for physical/local attack, may need at least two types of equipment's.</p> <p>2 to 4 equipment (5)</p>
Opportunity window	<p>ECU power-on is a must with a key and certificate-based use case running is being preferable except in attacking the secure storage itself.</p> <p>Medium (10)</p>

Elapsed time	<p>Key and certificates are already protected and even for preparation of side-channel attacks, it takes some days. So roughly on average prediction, it may take some weeks.</p> <p>≥ 1 week and ≤ 1 month (10)</p>
--------------	--

Damage scenario and impact analysis: Compromised key/certificates could cause eavesdropping/interception/MITM losing control of the main driving features like acceleration, braking and steering, stealing the PII and other sensitive data and more. Such damage scenarios may lead to injuries, legal issues, brand image impact and thus financial issues and more. Malicious code also could be injected if key/certificates are compromised.

Table 28: Keys and certificates management in-vehicle ECUs - damage impact is High (SFOP total= $100+50+10+25 = 185 (>100)$)

	S	F	O	P
Impact	High=100	High=50	High =10	High = 25

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Latest robust proven recommended and non-deprecated crypto algorithm shall be used. Standards like the vehicle key management system and virtual key management systems of AUTOSAR shall be used. Keys and certificates storage and key and certificates distribution channel need to be hardened. Robust intrusion detection and prevention system to be in place to monitor, detect and log suspicious communication and

suspicious access to the key and certificates. Periodic rotation of keys/certificates can mitigate the issue in case keys and certificates are compromised. Certified robust random number generators shall be used during key generation. Keys/certificates shall be stored in secure storage and access controlled like majorly crypto engines shall be able to access it.

4.4.6 EV (electric vehicle) electric charging

Asset description: Here, the major asset to be secured is the vehicle to a charging station communication channel. One needs to check on, how legitimate is the charging station. Charging stations to power grid communication channel also is an asset to be secured.

The payment channel between the payment processor and the charging station is an asset to be secured. Gateway network firewall configurations concerning electric charging and payments also is an asset to be protected. The user himself is an asset to be educated against phishing emails and apps related to electric charging payments. Mobile or infotainment system apps related to electric charging payment systems are the assets here.

Threat scenarios and attack surfaces: Compromised charging stations and unsecure vehicles and charging station intercommunication channels are the major electric charging-specific attack surfaces. Also, the payment channel is a potential attack surface. Hacked electric charging stations could disrupt the BMS leading to over or undercharging and advanced attacks could take control of the vehicle's driving control decisions. Electric charging and payment-related network gateways firewall could be misconfigured. Phishing attacks related to electric charging payments are also a concern. Malicious mobile and

infotainment system apps related to electronic charging and its payment process and vulnerabilities in those apps could be an easy entry point for hacking the vehicle and charging system.

Table 29: EV electric charging - total attack feasibility rating is $50+100+10+10+100+10+5+15+20 = 320 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	<p>Attackers shall be knowledgeable on electric charging stations and vehicle intercommunication standard protocols. Shall have known how the cryptography works for securing the electric charging and vehicle intercommunication channel and for checking on authorized electric charging stations.</p> <p>Medium (50)</p>
Information availability to the hacker	<p>Knowledge of electric charging and vehicle intercommunication standard protocols and cryptography is openly available.</p> <p>Openly available information (100)</p>

Hacking Equipment cost	<p>Penetration tools may cost 0 to many thousand dollars. While network analyzers and scanners would cost hundreds to thousands of dollars.</p> <p>Medium (10)</p>
Hacking equipment availability	<p>It is not illegal to have network analyzers and scanners and penetration tools as they are used for countermeasures and testing purposes as well. Hence equipment/tools are available freely or at some cost.</p> <p>Not: Wrong purpose to having it is illegal.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>The trend is towards remote attacks compared to physical/local attacks though currently physical/local attacks are also prominent.</p> <p>Remote (100)</p>
Number of hackers	<p>A single basic knowledgeable hacker can cause impactful damage to an electric charging system with data theft, vehicle control and payment fraud.</p> <p>1 hacker (10)</p>

Number of equipment/tools	For remote or physical/local attack a minimum of 2 kinds of equipment/tool would be needed with most common being a laptop and on top of it one or more equipment/tools would suffice. 2 to 4 equipment (5)
Opportunity window	The vehicle need not be at electric charging station and so anytime it can be attacked. Always (15)
Elapsed time	Remote attacks like DOS/replay attacks could be done in just few seconds as well though a complex attack may need some days. < 1 day (20)

Damage scenario and impact analysis: A compromised charging station and vehicle could cause payment irregularities causing loss financially. An unauthorized or hacked electric charging system could overcharge the battery leading to a fire mishap in the vehicle and thus causing safety issues. User location data, credentials used for payment and other PII data, if used with bad intentions cause privacy breaches leading to brand and thus further causing financial losses. Attacks could disrupt operations and data stealing leading to economic losses as well.

Table 30: EV electric charging - damage impact is High (SFOP total=50+50+10+25 = 135 (>100))

	S	F	O	P
Impact	Medium=50	High=50	High =10	High = 25

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Intrusion detection system with AI capabilities to secure payment and charging communication channels of vehicle to electric charging station and electric charging station to power grid channels. Encrypted communications on these channels are recommended. Very minimal required user and vehicle data shall be shared and the rest of the sensitive data shall be protected against the hacks to the electric charging and its payment process. A robust firewall shall be used at the network gateways of the electric charging and payment system. Users shall be educated against phishing attacks related to electric charging payments. The app used during the electric charging process shall be regularly updated and during the installation shall be checked if it is an authorized and secure app. PCI DSS, GDPR and OCPP standards shall be followed.

4.4.7 OBD – Onboard diagnostics port

Asset description: Major assets are OBD port and the cable connecting to the OBD port. Sensitive assets accessed through OBD port are the assets in OBD use case. Vehicle networks like CAN, wireless networks and other inter-ECU communication networks, control mechanisms and data are the assets. OBD software, OBD communication protocol

and the encoding formats used for the messages sent through OBD communication are the assets.

Threat scenarios and attack surfaces: DOS and relay attacks are possible through OBD ports. Assets discussed in the asset section are the attack surfaces as well. Sensitive vehicle data like location, driver behaviors and maintenance history could be retrieved from various ECUs and data from the communication channels. Through OBD various vehicle control systems can be influenced. Threat-causing hardware could be installed on top of the OBD port.

Table 31: OBD port - total attack feasibility rating is
 $50+100+5+10+100+10+5+15+20 = 315 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Attackers shall know about OBD and vehicle networks and additionally cryptography for hacking encrypted keys and authentication mechanisms and brute force kind of algorithms which are used to find the passwords and more. Medium (50)
Information availability to the hacker	Standard OBD protocols, cryptography for encryption and password hacking brute force algorithms are openly available.

	Public information (100)
Hacking Equipment cost	<p>Diagnostic software is available freely while sophisticated diagnostic tools shall cost up to thousands of dollars. OBD adapter would cost a few dollars. Penetration tools may cost from 0 to many thousand dollars. Network analyzers and scanners would cost hundreds to thousands of dollars.</p> <p>Medium (5)</p>
Hacking equipment availability	<p>It is not illegal to have OBD -II scanners as they are used for diagnosis. But the same OBD-II scanner can be used for getting the diagnosis information.</p> <p>Easily available (10)</p>
Hacker proximity to the device	<p>Physical attacks are feasible while indirect remote attacks in connected vehicles are difficult.</p> <p>Remote (100)</p>
Number of hackers	<p>One hacker is enough for a basic physical attack through a diagnostic port. For a sophisticated attack and for preparation for</p>

	<p>basic attack multiple experts may be required. Considering the commonality of the diagnostic port usage and protocols, would conclude that a majorly one attacker would be enough.</p> <p>1 hacker (10)</p>
Number of equipment/tools	<p>For physical/local attacks a minimum of two kinds of equipment/tool would be needed with the most common being a laptop and on top of it an OBD-II adapter/scanner is needed.</p> <p>2 to 4 equipment (5)</p>
Opportunity window	<p>A vehicle need not be on for a basic diagnostic port attack though some sensitive information and additional vehicle data can be retrieved when ECUs are in a power-on state.</p> <p>Always (15)</p>
Elapsed time	<p>Simple physical attack for an expert needs a few minutes though sophisticated complex attacks may exceed even a day.</p> <p>< 1 day (20)</p>

Damage scenario and impact analysis: A compromised vehicle through a diagnostic port attack can cause personal and vehicle data breaches leading to legal issues and even vehicle safety and operation issues like influence on vehicle control operations like steering control, braking and acceleration systems control. For financial benefit, data required for insurance claims can be modified leading to the financial benefit to the owner and loss to insurance companies and thus such unethical activities are possible.

Table 322: OBD port - damage impact is High (SFOP total=100+50+10+25 = 185 (>100))

	S	F	O	P
Impact	High=100	High=50	High =10	High = 25

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: An intrusion detection system to monitor malicious activities in diagnostic channels is recommended. Majorly authorized access mechanisms to be in place with encrypted and more secure protocol communication. Software updates for freshly known new vulnerabilities shall be done immediately. Last but not the least, vehicle door locking mechanism shall be robust as it is majorly a physical attack.

4.4.8 Keyless door entry

Asset description: The key fob has an RF chip having a unique RFID with an antenna for transmitting the RF signals to/from the vehicle RF receiver in the vehicle. In an advanced keyless entry system, there will be a transceiver in the vehicle and key fob for mutual communication between the vehicle and the key fob. Here encrypted communication shall be used in more secured keyless door entry systems. An authentication mechanism is a must at the vehicle end for authorizing the key fob and unlocking the door after successful authentication.

Threat scenarios and attack surfaces: The communication channel is vulnerable to relay attacks, jamming, amplification attack, spoofing, MITM and eavesdropping kind of attacks. Also unauthorized access could happen in a vulnerable authentication mechanism in keyless door entry system. Quantum computing and AI-ML kind of trends could be of more threat soon in the near future.

Table 33: Keyless door entry - total attack feasibility rating is $50+100+10+10+100+10+5+5+20 = 315 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	Attackers should know about RF communication, signal analysis, cryptography and more which are not confidential information. Medium (50)
Information availability to the hacker	Standard RF communication, signal analysis, cryptography are publicly available like in

	<p>published papers, forums, standards, for specific information in user manuals and more.</p> <p>Open information (100)</p>
Hacking Equipment cost	<p>Readymade few dollar RF chips are available to hack a keyless door system in a vehicle. At least some open-source software is available which is used in hacking the keyless door system in a vehicle. For complex attacks we may need logic/RF signal/spectrum analyzers and oscilloscopes which may be costly but when used at large scale looks cheaper though like for preparation and for multiple attacks with those same devices.</p> <p>Cheap (10)</p>
Hacking equipment availability	<p>With technology upgrading older technology-based equipment, tools and software become more reachable. Basic tools, software and equipment required look cheaper whereas complex equipment is costly and software and tools used for sophisticated attacks may need a license and may be expensive.</p> <p>Easily available (10)</p>

Hacker proximity to the device	<p>It is majorly a local attack, meaning the attacker must be a few distance (in meters) away from the key fob and vehicle. It also depends on the attack type performed for the hacker's proximity requirement. Physical attacks are not much focused here as the emphasis is on communication channel attacks like amplification and relay attacks.</p> <p>Remote (100)</p>
Number of hackers	<p>One hacker would be enough to perform a relay attack though two hackers may be more convenient.</p> <p>1 hacker (10)</p>
Number of equipment/tools	<p>Majorly for relay attacks, a relay device and a receiver are enough.</p> <p>2 equipment (5)</p>
Opportunity window	<p>The best opportunity is when the vehicle is off, like when parked and the key fob is near to the vehicle. So, the best opportunity arises at a parking place near the home where the key fob is placed near to the vehicle.</p> <p>Medium (5)</p>

Elapsed time	A few seconds would be enough to perform a relay attack. < 1 day (20)
--------------	--

Damage scenario and impact analysis: Vehicle and/or inside vehicle things theft is the major issue with the compromised keyless door entry system, leading to financial loss to the vehicle owner and to the keyless door entry system supply chain companies, right from tier2 keyless door entry system electronic component manufacturing tier1company up to the OEMs which decide the security levels of the keyless door entry system. With the modern vehicles with vulnerable keyless door entry system, there also comes strict regulations from the vehicle and government authorities for enhanced security. With the increase in theft of modern vehicles with the keyless door entry system, insurance amount also must be raised, affecting the end user again.

Safety, privacy and operations are comparatively considered minor concerns compared to financial losses, in this case though possibility of personal information getting stolen from the vehicle and vehicle passengers and vehicle systems getting harmed physically. It very much depends on the intention of the hacker whether it is a personal attack or a generic stranger attack.

Table 34: Keyless door entry - damage impact is High (SFOP total=50+50+5+12 = 117 (>100))

	S	F	O	P
Impact	Medium=50	High=50	Medium =5	Medium = 12

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Key fob shall be placed in a faraday cage or aluminum/tin boxes to avoid electromagnetic interferences. Key fob should be switched off when not required like during night and whenever vehicle owner is sure he does not need to start the vehicle soon. The vehicle shall have an immobilizer to detect the key presence and then start the ignition.

Keyless door entry system shall have robust mechanisms to tackle the replay attack like frequency hopping, varying the authentications codes frequently and jamming the signal if key is far. The vehicle shall respond to the key fob only if it is near, by having key to vehicle distance measurement mechanism. Symmetric key encryption of communication data and asymmetric key for authentication/authorization shall be used.

4.4.9 Two-wheeler electronic systems

Asset description: Modern two-wheeler has many connected electronic systems and ECUs like infotainment system which has capability to connect to mobile for multimedia/music through bluetooth and Wi-Fi connectivity, telematics unit which connects to the cloud for telemetry, security alerts, software updates using cellular network, OBD port and GPS system to name a few major externally connected electronic systems. Sensors and actuators also are electronically controlled in modern two-wheelers. These

electronic systems need software to program them. Electric two wheelers are increasing day by day and need to be connected to electric charging systems for charging.

Threat scenarios and attack surfaces: Intrusion into the vehicle network can happen through OBD ports and Wi-Fi network. Malicious data can be penetrated through bluetooth. Malicious programs can be introduced through the OBD port. Sensors and actuators could be physically and remotely electronically tampered. Compromised vehicle functionalities can be altered. Vulnerabilities in protocols used during electric charging in electric two wheelers are a potential threat

Table 35: Two-wheeler electronic systems - total attack feasibility rating is $50+100+10+10+100+10+5+5+20 = 315 \rightarrow$ high attack feasibility

Attack parameters	Attack respective parameters rationale behind the rating
Hacker expertise	<p>Knowledge of either wireless communication, electric charging protocols, OBD-II protocols, software languages like python, c, c++ whichever used in automotive industry, vehicle networks, known software and hardware vulnerabilities tracking is a must. All this information is openly available.</p> <p>Medium (50)</p>

Information availability to the hacker	<p>Communication protocols, cryptography, known vulnerabilities, software languages and other needed information are all publicly available.</p> <p>Publicly available information (100)</p>
Hacking Equipment cost	<p>Free network tools also are available by paying a few dollars more for equipment's could help better in hacking.</p> <p>Cheap (10)</p>
Hacking equipment availability	Easily available (10)
Hacker proximity to the device	<p>It can be done remotely through cellular network for attacking related cloud server and the two-wheeler vehicle data in the cloud and for software vulnerabilities in the two-wheeler software if any. Local attack is possible through Wi-Fi and bluetooth network and as well physically, if using a wired cable for OBD-II port attack surface.</p> <p>Remote (100)</p>
Number of hackers	<p>One hacker would be enough to perform the simplest attack whereas hackers'</p>

	<p>experts in various domains like network, OBD, cryptography would be handy.</p> <p>Minimum one hacker (10)</p>
Number of equipment/tools	<p>There are multiple tools to scan the network and software vulnerabilities. Similarly, there are multiple attacking tools available in the market. At least two types of equipments may be required majorly where the attack surface is OBD port or any network, considering basic laptop/PC common for all attacks.</p> <p>2 equipment (5)</p>
Opportunity window	<p>The best opportunity is between the time the vulnerability is detected or known till it is patched. The best time to hack using OBD port is when it is parked whereas remote hacking is feasible when vehicle is running. Opportunity arises at compromised electric charging stations during charging of electric two wheelers.</p> <p>Medium (5)</p>

Elapsed time	Hacking within a day is very much possible for an expert with a known vulnerability. < 1 day (20)
--------------	---

Damage scenario and impact analysis: Two wheelers are often parked outside and easy to do physical attack using OBD port. Two-wheeler electronic systems are vulnerable to eavesdropping in the wired and wireless network with bad intentions. Button start vehicles can be compromised including the immobilizer system to start the vehicle and steal the vehicle. Through OBD-II port, vehicle functions like braking, acceleration and steering can be compromised leading to safety issues followed by legal and financial issues. Faulty electric charging process could damage the battery management system and may lead to overcharging causing fire too, which is the biggest safety concern for electric two wheelers.

Vehicle location and usage details and other personal details can be stolen leading to privacy issues, vehicle theft causing financial loss to the vehicle owner and thus may lead to insurance premium increase, with OEM losing the reputation/brand image followed by legal issues as well. Operations of the commercial two-wheeler usage is impacted like porter services, food delivery and bike taxi businesses if two-wheeler is compromised. Also, insurance and OEM business sales are impacted.

Table 36: Two-wheeler electronic systems - damage impact is High (SFOP
total=100+50+15+25 = 190 (>100))

	S	F	O	P
--	----------	----------	----------	----------

Impact	High=100	High=50	High = 15	High = 25
---------------	----------	---------	-----------	-----------

Damage impact (rows) vs attack feasibility = High vs High = High risk

Countermeasures: Using secure protocols like https and TLS kind of secure communication need to be practiced in apps, Wi-Fi and cellular communications. Authorized communication and message authentication using AES shall be practiced during Wi-Fi, electric charging and cellular communications and other sensitive intra vehicle communications. One shall follow secure coding guidelines, SAST and DAST kind for secure software processes. Secure testing shall be done. Need to have tamper detection and response in hardware and IDPS in network communications, with robust firewall in place.

Multi factor two-wheeler access like password and physical biometric and/or smart phone-based authentications to be in place as password can be hacked and need to have a multi-layer access control. Regular software updates for vulnerability patches shall be done. The latest software stacks for bluetooth, Wi-Fi, OpenSSL and other software modules shall be flashed.

4.5 Summary of Findings

Lets summarize the attack feasibility and damage impact SFOP scores of each use case and it's total for a rough informal risk comparison, though generally we use risk matrix. All use cases have given high risk as all use case damage impact SFOP score and attack feasibility score has exceeded hundred (100).

Table 37: Summary of attack feasibility and damage impact SFOP score for each

use case				
Use case number	Use case	Attack feasibility score	Damage impact SFOP score	Attack feasibility + damage impact SFOP scores
1	Camera	250	132	382
2	Radar	135	132	267
3	Lidar	140	132	272
4	Ultrasonics	155	130	285
5	IVI to mobile communication	155	185	340
6	IVI miscellaneous interfaces	220	145	365
7	Telematics	310	185	495
8	V2X	315	172	487
9	Keys and certificates in-vehicle ECUs	200	185	385
10	EV (electric vehicle) electric charging	320	135	455

11	OBD – Onboard diagnostics port	315	185	500
12	Keyless door entry	315	117	432
13	Two-wheeler electronic systems	315	190	505

Highest attack feasibility is seen in EV (electric vehicle) electric charging with 320 score. Highest damage impact is seen in two-wheeler electronic systems with damage impact SFOP score being 190. Highest total of attack feasibility and damage impact SFOP score is of two-wheeler electronic systems with 505 score.

4.6 Conclusion

Most safety impacted use cases, due to security attacks are two-wheeler electronic systems, OBD port, keys and certificates management in-vehicle ECUs, V2X, telematics, IVI - miscellaneous, IVI - mobile communication, ultrasonics, lidar, radar and camera.

Here it will not be fair to compare mixing with two-wheeler attack feasibility and damage impact SFOP score with four wheeler electronic systems as two wheeler is far cheaper and smaller/portable compared to four wheeler and hence damage impact would be less compared to four wheeler though in above over all damage impact of two-wheeler considering worst case electronic systems of two wheeler and not a particular ECU or a electronic systems is considered.

So now in four wheeler use cases, highest attack feasibility seen is 320, being scored by EV (electric vehicle) electric charging use case. Highest damage impact in four

wheeler use cases is scored by several use cases like OBD – Onboard diagnostics port, Telematics, IVI to mobile communication and Keys and certificates in-vehicle ECUs with damage impact SFOP score being 185. Highest total of attack feasibility and damage impact SFOP score in four wheeler use cases is of OBD with 500 score.

Limitations were that STRIDE was not explained directly but in threat scenarios was explained subjectively. Also MITRE ATT&CK model is not followed here which explains about adversary behaviour on why and how the attack is planned which further helps in detection and mitigate the attacks. Also risk governance is not covered where in higher management decides on the mitigations actions approval based on resource, time, cost, performance, dependencies, reliability and other factors.

CHAPTER V:

DISCUSSION

5.1 Discussion of Results

Since the rough attack feasibility estimations and damage impact SFOP analysis are made here considering worst-case scenarios, it may not be fair to conclude with only one use case being critically risky among all the high-risk use cases. Let us think above 300 score for the attack feasibility plus damage impact SFOP score in four-wheeler use cases to be all critically risky. So let's assume the most critically risky use cases/assets are OBD, camera, IVI to mobile communication, IVI miscellaneous interfaces, telematics, V2X, Keys and certificates in-vehicle ECUs, EV (electric vehicle) electric charging and Keyless door entry.

5.2 Discussion of Research Question One: What is the automotive business/economic impacts? Who are all stakeholders impacted?

Here along with the business/economic impacts we can also see that lots of collaboration will be required among different automotive players across the supply chain like OEMs, Tier1s/2s and service providers like for example tools for development and

testing and more. Also just one new trend was covered i.e. electric charging. But other emerging trends are more of ADAS, HAD and AD as well to name a few, which impacts heavily automotive business economy.

5.3 Discussion of Research Question Two: What automotive processes to follow? What are the different aspects of automotive processes?

Here emphasis is given more on what processes are followed and related artifacts in respective vehicle life cycle phases. ASPICE, ISO21434 and other standards/models also explain on relation between the stages, dependencies and more. Also, not all details are covered like DAST and more details not given like audit, certifications and pen testing are recommended to be done at final stages by external recommended/recognised/authorized/related automotive service providers.

5.4 Discussion of Research Question Three: What are the various security goals, concepts, requirements and claims?

Here many of the security counter measures are covered in the name of security goals, security concept, security requirements and security claims. Real claims would happen in projects and here it is a suggestion though. Many are covered but may be few are left like in secure communication, V2X and telematics using cellular and DSRC communications, mobile to Infotainment systems wired and wireless communications and more is not covered. So in this thesis, many are covered but not all.

5.3 Discussion of Research Question Four: Roughly how is the extended TARA to be executed in automotive security for various electronic components in the vehicle?

Here for TARA major ECUs are covered. Still left are like ABS, steering controls, TPMS kind of electronic systems, which are major safety concern rather than security directly. But they are of major concern once attack is made on the electronic systems which makes the decision and sends the signals to ABS and steering controls kind of vehicle operation mechanisms and thus further causing safety issues.

CHAPTER VI:

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

Each use case has several assets to be secured against threats. Ideally Attack feasibility has to be done for each security asset with a particular attack and with a particular security properties under threat. Quantitative analysis was done on worst case scenario for each parameters in each use case. It was done this way to give a rough idea on many assets for the use case, many security properties, attack surfaces, threat and damage scenarios with emphasize given to critical once. This covers a quick TARA idea about the use case and not a detailed report.

6.2 Implications

TARA is applicable not only in automotive domain but various other domains where there is need for embedded security. TARA can be applicable in all security sensitive embedded systems like in Consumer electronics with one of the use case being smart TV and smart phones and in industrial, health care and more. In each domain there could various different security assets to be protected and also threat scenarios may vary.

For example, in smart TV, DRM contents are the major security asset to be protected and hence the related secure memory where the related video audio contents are stored after decryption of encrypted content.

6.3 Recommendations for Future Research

Further, could add more on security concepts/security countermeasures/security goals/security features like secure asset management, perimeter hardening, firewall and more. In TARA, could add interfaces like USB, JTAG and more. In TARA could also add electronic actuators like ABS, steering control, acceleration and more. In TARA could also add electronic systems like airbags, TPMS and more.

AI can be used in every ECUs and electronic components going further for runtime threat/anomaly detection, mitigation and responses. In AI based VSOC, entire vehicle security view could be achieved adding to better maintenance by runtime actions on risk mitigations. AI supported HWs shall be used to meet the performance needs in AI based vehicle security at edge/ECUs/electronic components and as well in the cloud.

6.4 Conclusion

In literature review we covered lots of papers on attacks, vulnerabilities and countermeasure in Automotive. In Research proposal, we had a detailed explanation on how security concept, goals, processes would be covered along with extended TARA coverage. In Research on TARA, covered many ECUs and electronic components and use cases and summarized as well on critical findings.

In future, also planned to publish a book on automotive security. In one of the appendix, could also add a TARA example on consumer electronics use case - smart TV for DRM AV content protection. Also can add terminologies in one of the appendix.

Whatever mentioned in secure concepts subjectively and in TARA qualitatively shall not be considered as final as it very much depends on the contexts which varies a lot from OEMs (vehicle manufactures), tier1/2 and other vendors) and also on the project and during what time. Changes in technology, standards and regulations also would impact the correctness of the details mentioned. Since this thesis is not done based on the survey and interviews, hence survey cover letter, informed consent and interview guide is not applicable.

For performing TARA, now a days, even automated tools are available like from Vultara and Cyberphnix, ESCRYPT CycurRISK of ETAS, AVL ThreatGuard, Itemis Secure of Itemis, Ansys Medini Analyze of Ansys Incorporation and more. These automated TARA tools are faster, error free compared to manual, allowing dynamic changes by multiple people at the same time and version management.

Drone is vastly used in defense and has some similarity to ADAS, telematics and infotainment ECUs, which could be a great topic for researching as drones look to be more vulnerable than automotive as the nation is at stake.

From TARA quantitative outputs for attack feasibility values, damage scenario values and risk value, higher management can decide on which use case needs the highest priority and mandatory from security point of view considering economic impacts from safety, financial, operational and privacy impacts. Also for higher management to understand what it takes to implement security controls, security concept section and countermeasure mentioned for each use case would give a rough idea, thus helping further to getting closer to practicality. It helps business leaders to allocate appropriate resources, budget for countermeasures/mitigations/preventive implementations. Thus reputation, brand image, trust, stability, profitability and business continuity to the

company, is ensured by addressing critical risky use cases first. Majorly it helps in trade-off between security and resources allocation (budget, time, resources/man power...).

REFERENCES

Dudley-Nicholson, J. (2024). Electric car charging stations tipped to double again. [online] The Canberra Times. Available at: <https://www.canberratimes.com.au/story/8487582/electric-car-charging-stations-tipped-to-double-again/> [Accessed 17 Jan. 2024].

www.mygreatlearning.com., (2022). <https://www.mygreatlearning.com/blog/what-is-computer-vision-the-basics/> [Accessed 10th January 2022])

Mohammad Ali Sayed a et al., (2021). Electric vehicle attack impact on power grid operation, *International Journal of Electrical Power & Energy Systems*. Elsevier. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0142061521010048> (Accessed: March 15, 2023).

Mahmood *et al.*, (2021). When Trust Meets the Internet of Vehicles: Opportunities, Challenges, and Future Prospects, *2021 IEEE 7th International Conference on Collaboration and Internet Computing (CIC)*, Atlanta, GA, USA, 2021, pp. 60-67, doi: 10.1109/CIC52973.2021.00018.

<https://upstream.auto/>. (2022). <https://upstream.auto/2022-report-thank-you/?submissionGuid=3e5e9656-9817-4256-945e-cee8d2b35b3e>.

Upstream Security. (n.d.). (2022). Global Automotive Cybersecurity Report. [online] Available at: <https://upstream.auto/2022-report-thank-you/?submissionGuid=3e5e9656-9817-4256-945e-cee8d2b35b3e> [Accessed 22 Mar. 2023].

C. Miller. Lessons learned from hacking a car. Available at *IEEE Design & Test*, vol. 36, no. 6, pp. 7-9, Dec. 2019, doi: 10.1109/MDAT.2018.2863106.

Blum, B. (2022). Cyberattacks on cars increased 225% in last three years. [online] ISRAEL21c. Available at: <https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/>.

GREENBERG, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. [online] WIRED. Available at: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>, 2015.

Levillain, O. (2021). Implementation Flaws in TLS Stacks: Lessons Learned and Study of TLS 1.3 Benefits. *Lecture Notes in Computer Science*, pp.87–104. Available at: Springer. https://doi.org/10.1007/978-3-030-68887-5_5

Hammerschmidt, C. (2021). NXP certified to cybersecurity standard ISO 21434. [online] EENewsEurope. Available at: <https://www.eenewsautomotive.com/en/nxp-certified-to-cybersecurity-standard-iso-21434/> [Accessed 13 october. 2022].

Wolf, M. and Gendrullis, T. (n.d.). 2022). Design, Implementation, and Evaluation of a Vehicular Hardware Security Module. [online] Available at: <https://evita-project.org/Publications/WG11.pdf> [Accessed 11 Dec. 2022].

www.autosar.org. (2019).
https://www.autosar.org/fileadmin/user_upload/standards/foundation/19-11/AUTOSAR_TR_SecureHardwareExtensions.pdf.

Automotive ISAC. (n.d.). (2022). Best Practices. [online] Available at: <https://automotiveisac.com/best-practices> [Accessed 11 Dec. 2022].

Bush, S. (2022). Wireless-connected EV battery manager has ISO/SAE 21434 cybersecurity. [online] Electronics Weekly. Available at: <https://www.electronicsworld.com/news/design/legislation/wireless-connected-ev-battery-manager-iso-sae-21434-cybersecurity-2022-04/> [Accessed 11 Dec. 2022].

Computer Security Division, I.T.L. (2016). Cryptographic Algorithm Validation Program | CSRC | CSRC. [online] CSRC | NIST. Available at: <https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program> [accessed on 5th Dec 2022].

Computer Security Division, I.T.L. (2016). Cryptographic Module Validation Program | CSRC | CSRC. [online] CSRC | NIST. Available at: <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3556> [Accessed 11 Dec. 2022].

GlobalPlatform. (2020). SESIP – the building blocks to certified IoT products for Certification Bodies, regulators, laboratories, and device makers. [online] Available at: <https://globalplatform.org/sesip-the-building-blocks-to-certified-iot-products-for-certification-bodies-regulators-laboratories-and-device-makers/> [Accessed 11 Dec. 2022].

www.automotivespice.com. (2021). Quality Management in the Automotive Industry Automotive SPICE ® Process Reference and Assessment Model for Cybersecurity Engineering Title: Automotive SPICE ® for Cybersecurity Process Reference and Assessment Model Author(s): VDA QMC Project Group 13. [online] Available at: <https://www.automotivespice.com/fileadmin/software->

download/AutomotiveSPICE_for_Cybersecurity_PAM_1st_edition_2021.pdf [Accessed 11 Dec. 2022].

NIST Cybersecurity Risk Management Conference Risk Management for Automotive Cybersecurity Bill Mazzara -Global Vehicle Cybersecurity Technical Fellow -FCA US LLC. (2018). [online] Available at: https://www.nist.gov/system/files/documents/2018/12/06/risk_management_for_automotive_cybersecurity.pdf [Accessed 11 Dec. 2022], Nov 7, 2018.

jean.yoder.ctr@dot.gov (2016). NHTSA. [online] NHTSA. Available at: <https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity>, [Accessed 11th Dec 2022].

Cybersecurity Best Practices for Modern Vehicles. (n.d.). (oct, 2016). [online] Available at: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf.

www.sae.org. (n.d.). (2022). Cybersecurity Industry Factors | SAE International. [online] Available at: <https://www.sae.org/what-is-cybersecurity> [Accessed 11 Dec. 2022].

www.sae.org. (n.d.). (2022). Podcasts - SAE International. [online] Available at: <https://www.sae.org/podcasts/cybersecurity> [Accessed 11 Dec. 2022].

www.sae.org. (n.d.). (2022). Automotive Cybersecurity Certification: Level One. [online] Available at: <https://www.sae.org/learn/content/c2105/> [Accessed 11 Dec. 2022].

www.sae.org. (n.d.). (2022). Cybersecurity for Commercial Vehicles. [online] Available at: <https://www.sae.org/publications/books/content/r-464/> [Accessed 11 Dec. 2022].

www.iso.org. (n.d.). (2021). ISO/SAE 21434. [online] ISO. Available at: <https://www.iso.org/standard/70918.html>.

Unece.org. (2022). UN Regulation No. 155 - Cyber security and cyber security management system | UNECE. [online] Available at: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security> [Accessed 11 October 2022].

The Canberra Times. (2022). Cyber risk in adding electric cars to grid. [online] Available at: <https://www.canberratimes.com.au/story/7939810/cyber-risk-in-adding-electric-cars-to-grid/> [Accessed 15 October 2022].

<https://www.mckinsey.com/>. 2020. Cybersecurity in automotive: Mastering the Challenge. [online] Available at: <<https://www.mckinsey.com/~media/mckinsey/industries/automotive%20and%20assembly/our%20insights/cybersecurity%20in%20automotive%20mastering%20the%20challenge/cybersecurity-in-automotive-mastering-the-challenge.pdf>> [Accessed 11 October 2022].

Kaya, K. (2019). A Study of Vulnerabilities and Weaknesses in Connected Cars. [online] www.semanticscholar.org. Available at: <https://www.semanticscholar.org/paper/A-Study-of-Vulnerabilities-and-Weaknesses-in-Cars-Kaya/df0e6647716c16f41896988e52ce54a2f48f0129> [Accessed 5 Feb. 2023].

Rezeifar, Zeinab and Oh, Heekuck (2016). Analysis of Security Issues in Wireless Charging of Electric Vehicles on the Move. Journal of the Korea Institute of Information Security & Cryptology. 한국정보보호학회, 26(4), pp. 941–951. doi: 10.13089/JKIISC.2016.26.4.941.

Pupuweb.com. (2023). API Vulnerabilities Security Flaws Affect Millions of Cars. [online] PUPUWEB. Available at: <https://pupuweb.com/api-vulnerabilities-security-flaws-affect-millions-cars/> [Accessed 22 Mar. 2023].

Serban, A.C., Poll, E. and Visser, J. (2018). A Standard Driven Software Architecture for Fully Autonomous Vehicles. 2018 IEEE International Conference on Software Architecture Companion (ICSA-C).

J. F. Roscoe, O. Baxandall and R. Hercock. (2020). Simulation of Malware Propagation and Effects in Connected and Autonomous Vehicles. 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 2020, pp. 57-62, doi: 10.1109/iCCECE49321.2020.9231063.

www.spirent.com. (2020). How should the automotive industry test V2X systems? - Spirent. [online] Available at: https://www.spirent.com/campaign/testing-v2x-systems?utm_medium=digital+ppc&utm_source=google&utm_campaign=automotive&utm_term=c%20v2x%20technology&gclid=Cj0KCQiA54KfBhCKARIsAJzSrdjC7Wr6fsGcH9V1EYWwkUlf01smSmrLQX-ZI2FqPB0X2HQyICjET0aAoPuEALw_wcB [Accessed 6 Feb. 2023].

Wang, J., Shao, Y., Ge, Y., Yu, R. (2019). A Survey of Vehicle to Everything (V2X) Testing. *Sensors*, 19(2), 334, available: <http://dx.doi.org/10.3390/s19020334>.

Sommer, F., Dürrwang, J. and Kriesten, R. (2019). Survey and Classification of Automotive Security Attacks. *Information*, [online] 10(4), p.148. <https://doi.org/10.3390/info10040148>.

Schlösser, A., Nedospasov, D., Krämer, J., Orlic, S., Seifert, JP. (2012). Simple Photonic Emission Analysis of AES. In: Prouff, E., Schaumont, P. (eds) *Cryptographic Hardware and Embedded Systems – CHES 2012*. CHES 2012. Lecture Notes in Computer Science, vol 7428. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33027-8_3

L. Pike, J. Sharp, M. Tullsen, P. C. Hickey and J. Bielman. (2017). Secure Automotive Software: The Next Steps. Available at *IEEE Software*, vol. 34, no. 3, pp. 49-55, May-Jun. 2017, doi: 10.1109/MS.2017.78.

Rumez, M., Grimm, D., Kriesten, R. and Sax, E. (2020). An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures. IEEE Access, 8, pp.221852–221870

Specification of Communication Management AUTOSAR AP Release 18-03 Document
Title Specification of Communication Management. (2018). Available at:
https://www.autosar.org/fileadmin/standards/adaptive/18-03/AUTOSAR_SWS_CommunicationManagement.pdf [Accessed 25 Mar. 2023].

Specification of Secure Onboard Communication Document Title Specification of Secure
Onboard Communication. (n.d.). (2023) Available at:
https://www.autosar.org/fileadmin/standards/classic/19-11/AUTOSAR_SWS_SecureOnboardCommunication.pdf [Accessed 25 Mar. 2023].

Xun, Y., Liu, J. and Zhang, Y. (2019). Side-Channel Analysis for Intelligent and Connected Vehicle Security: A New Perspective. IEEE Network, pp.1–8.

cwe.mitre.org. (n.d.). (2023) CWE - CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) (4.10). [online] Available at: <https://cwe.mitre.org/data/definitions/1319.html> [Accessed 25 Mar. 2023].

ISO/SAE 21434. (2021) [online] ISO. Available at: <https://www.iso.org/standard/70918.html>.

Rao Kandimala, N. and Sojka, M. (2012). Safety and Security Features in AUTOSAR. [online] Available at: <https://rttime.felk.cvut.cz/publications/public/autosar-safety-security.pdf> [Accessed 4 Apr. 2023].

Bella, G., Biondi, P., Costantino, G. and Matteucci, I. (2020). CINNAMON: A Module for AUTOSAR Secure Onboard Communication. [online] IEEE Xplore. doi:<https://doi.org/10.1109/EDCC51268.2020.00026>.

Jadoon, A.K., Wang, L., Li, T. and Zia, M.A. (2018). Lightweight Cryptographic Techniques for Automotive Cybersecurity. *Wireless Communications and Mobile Computing*, 2018, pp.1–15. doi:<https://doi.org/10.1155/2018/1640167>.

E.Lagnf, F.M. and Ganesan, S. (2022). The Improved Implementation of the Message freshness on CAN XL using FPGA. [online] IEEE Xplore. doi:<https://doi.org/10.1109/eIT53891.2022.9813763>.

Strang, T. and Röckl, Dipl.-I. (n.d.). Vehicle Networks V2X communication protocols. [online] Available at: <https://www.sti-innsbruck.at/sites/default/files/courses/fileadmin/documents/vn-ws0809/11-VN-WAVE.pdf> [Accessed 3 Jul. 2023].

Christoph Schmittner, Ma, Z., Schoitsch, E. and Gruber, T. (2015). A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems. Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. doi:<https://doi.org/10.1145/2732198.2732204>.

McLachlan, S., Schafer, B., Dube, K., Kyrimi, E. and Fenton, N. (2022). Tempting the Fate of the furious: cyber security and autonomous cars. International Review of Law, Computers & Technology, 36(2), pp.181–201. doi:<https://doi.org/10.1080/13600869.2022.2060466>.

Fowler, D.S., Bryans, J., Shaikh, S.A. and Wooderson, P. (2018). Fuzz Testing for Automotive Cyber-Security. [online] IEEE Xplore. doi:<https://doi.org/10.1109/DSN-W.2018.00070>.

Sim, K.-Y., Kuo, F.-C. and Merkel, R. (2011). Fuzzing the out-of-memory killer on embedded Linux. doi:<https://doi.org/10.1145/1982185.1982268>.

Zhao, W., Lu, K., Wu, Q. and Qi, Y. (n.d.). Semantic-Informed Driver Fuzzing Without Both the Hardware Devices and the Emulators. [online] doi:<https://doi.org/10.14722/ndss.2022.23345>.

Muench, M., Stijohann, J., Kargl, F., Francillon, A. and Balzarotti, D. (2018). What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices. Proceedings 2018 Network and Distributed System Security Symposium. [online] doi:<https://doi.org/10.14722/ndss.2018.23166>.

Wilson, T. (19 Apr. 2018). Evaluation of Fuzzing as a Test Method for an Embedded System. [online] Available at: <https://core.ac.uk/download/pdf/161427746.pdf> [Accessed 11 Jul. 2023].

Macarie, M. (n.d.). Fuzzing Android Automotive's CAN interface. [online] Available at: http://essay.utwente.nl/95607/1/Macarie_MA_EEMCS.pdf [Accessed 11 Jul. 2023].

Fioraldi, A., Maier, D., Zhang, D. and Balzarotti, D. (11 Nov, 2022). LibAFL: A Framework to Build Modular and Reusable Fuzzers. [online] Available at: https://www.s3.eurecom.fr/docs/ccs22_fioraldi.pdf [Accessed 11 Jul. 2023].

Fowler, D. (n.d.). A Fuzz Testing Methodology for Cyber-security Assurance of the Automotive CAN Bus. [online] Available at: https://pure.coventry.ac.uk/ws/portalfiles/portal/37979533/Fowler_PhD.pdf [Accessed 15 Jul. 2023].

Fowler, D., Bryans, J. and Shaikh, S. (n.d.). Automating fuzz test generation to improve the security of the Controller Area Network. [online] Available at: https://pure.coventry.ac.uk/ws/portalfiles/portal/11566144/Fowler_Bryans_Shaikh_ECU_Fuzz_Testing.pdf [Accessed 15 Jul. 2023].

Zuo, Z., Yang, S., Ma, B., Zou, B., Cao, Y., Li, Q., Zhou, S. and Li, J. (2021). Design of a CANFD to SOME/IP Gateway Considering Security for In-Vehicle Networks. *Sensors*, 21(23), p.7917. doi:<https://doi.org/10.3390/s21237917>.

Xu, W., Yan, C., Jia, W., Ji, X. and Liu, J. (2018). Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles. *IEEE Internet of Things Journal*, [online] 5(6), pp.5015–5029. doi:<https://doi.org/10.1109/JIOT.2018.2867917>.

Lou, J., Yan, Q., Hui, Q. and Zeng, H. (n.d.). SoundFence: Securing Ultrasonic Sensors in Vehicles Using Physical-Layer Defense. [online] Available at: <https://par.nsf.gov/servlets/purl/10290264> [Accessed 17 Jul. 2023].

Shoukry, Y., Martin, P., Yona, Y., Diggavi, S. and Srivastava, M. (2015). PyCRA. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. doi:<https://doi.org/10.1145/2810103.2813679>.

Cemil, A. and Ünlü, M. (2022). Analysis of ADAS Radars with Electronic Warfare Perspective. *Sensors*, [online] 22(16), p.6142. doi:<https://doi.org/10.3390/s22166142>.

Neng-Jing, L. and Zhang Yi-ting (1995). A survey of radar ECM and ECCM. 31(3), pp.1110–1120. doi:<https://doi.org/10.1109/7.395232>.

Yeh, E., Choi, J., Prelcic, N., Bhat, C. and Heath, R. (n.d.). Security in Automotive Radar and Vehicular Networks. [online] Available at: https://www.caee.utexas.edu/prof/bhat/ABSTRACTS/SecurityOverview_mmWave_V2X.pdf.

insights.sei.cmu.edu. (2016). On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle. [online] Available at: <https://insights.sei.cmu.edu/blog/board-diagnostics-risks-and-vulnerabilities-connected-vehicle/> [Accessed 18 Aug. 2023].

Klinedinst, D. and King, C. (2016). On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle. [online] Available at: https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf.

Sato, T., Shen, J., Wang, N., Jia, Y., Lin, X. and Chen, Q.A. (2020). Security of Deep Learning based Lane Keeping System under Physical-World Adversarial Attack. ArXiv. [online] Available at: <https://www.semanticscholar.org/paper/Security-of-Deep-Learning-based-Lane-Keeping-System-Sato-Shen/84ca9af1bedbfa5921ee813fd0ebcca9a7b5d52> [Accessed 1 Sep. 2023].

Zhang, H., Pan, Y., Lu, Z., Wang, J. and Liu, Z. (2021). A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units. IEEE Access, 9, pp.149690–149706. doi:<https://doi.org/10.1109/access.2021.3124565>.

Sun, J., Cao, Y., Chen, Q.A. and Mao, Z.M. (2020). Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures. ArXiv. [online] Available at:

<https://www.semanticscholar.org/paper/Towards-Robust-LiDAR-based-Perception-in-Autonomous-Sun-Cao/9d13c6b39f7ea80b5b91dff29f5e682ed1436893> [Accessed 1 Sep. 2023].

El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D.F., Plathottam, S.J. and Ranganathan, P. (2020). Cybersecurity Attacks in Vehicular Sensors. *IEEE Sensors Journal*, [online] 20(22), pp.13752–13767. doi:<https://doi.org/10.1109/JSEN.2020.3004275>.

Sato, T., Shen, J., Wang, N., Jack Jia, Y., Lin, X. and Chen, Q. (n.d.). Security of Deep Learning based Lane Keeping System under Physical-World Adversarial Attack. [online] Available at: <https://arxiv.org/pdf/2003.01782.pdf> [Accessed 20 Sep. 2023].

LIST OF ABBREVIATIONS

Note: Some of the different abbreviations or have other meaning as well. It will be made clear in the context, and/or by adding additional wordings.

4G (4th generation cellular communication network)

5G (5th generation cellular communication network)

A

A (Accountable)

ABAC (attribute-based access control)

ABS (automatic braking system)

ACC (adaptive cruise control)

ACL (access control list)

ADAS (advanced driver assistance system)

AD (autonomous driving)

AEAD (authenticated encryption with associated data)

AES (Advanced Encryption Standard)
AGC (automatic gain control)
AI (Artificial Intelligence)
Algo (algorithm)
AM (amplitude modulation)
API (Application programming interface)
ARAN (Authenticated Routing for Ad hoc Networks)
ASLR (address space layout randomization)
ASPICE (Automotive Software Process Improvement and Capability dEtermination)
AST (application security testing)
A-SAODV (an extension of secure ad hoc on-demand distance vector)
AUTOSAR (AUTomotive Open System ARchitecture)
AV (audio video)

B

BMS (Battery management system)
BT (Bluetooth)

C

C (Consulted)
C-V2X (cellular-vehicle to everything)
CA (Certificate Authority)
CAN (controller area network)
CAN FD (FD-Flexible Data - Rate)
CAN XL (CAN extended length)
CapBAC (capability-based access control)

CFT (coherent false target)
CIA (cybersecurity interface agreement)
CIA (confidentiality, integrity, authenticity)
CI/CD (continuous integration/continuous deployment/delivery)
CINNAMON (Confidential, Integral aNd Authentic on-board comMunicatiON)
CMAC (cipher-based MAC)
CoT (chain of trust)
CPU (central processing unit)
CRL (certificate revocation list)
CSM (Crypto Service Manager)
CSMS (cybersecurity management system)
CVE (common vulnerability enumeration)
CVSS (Common Vulnerability Scoring System)
CWE (Common Weakness Enumeration)

D

DAB (digital audio broadcast)
DAC (discretionary access control)
DAST (dynamic application security testing)
DDoS (distributed DoS- denial of service)
DEP (data execution prevention)
DevSecOps (development, security and operations)
DIA (dependency interface agreement)
DMC (driver monitoring camera)
dm-verity (device-mapper-verity, a kernel feature, detecting memory block changes)
DoS (Denial of Service)
DPA (differential power analysis)

DRM (digital right management – paid and/or encrypted multimedia(audio video) contents)

DSRC (digital short-range communication)

DSSS (direct sequence spread spectrum)

E

ECU (electronic control units)

ECDSA (Elliptical Curve Digital Signature (ECDS)

ECC (Error Detection and Correction Codes)

EDCC (Error Detection and Correction Codes)

eMMC (embedded MultiMediaCard)

EM-FI (electromagnetic fault injection)

EMI (electromagnetic interference)

ETAS (empowering tomorrow's automotive software)

Eth (ethernet)

EV (electric vehicles)

F

F (Financial)

FHSS (frequency hopping spread spectrum)

FI (fault injection)

FIB (focused ion beam)

FlexRAY (Field Bus EXchange)

FM (frequency modulation)

FOV (field of view)

G

GCM (Galois/Counter Mode, AES GCM)

GMAC (galois/counter mode-based MAC – message authentication code)

GMSL (gigabit multimedia serial link)

GDPR (General Data Protection Regulation)

GPS (global positioning system)

GSM (Global System for Mobile communication)

GVS (ground view sensors)

H

HAD (highly automated driving)

HIL (Hardware In Loop)

HMAC (hash-based MAC – message authentication code)

HMI (human-machine interface)

HF (high frequency)

HSM (hardware security module)

HSE (hardware security extension)

HTTP (HyperText Transfer Protocol)

HUD (head-up display)

HW (hardware)

HVAC (Heating, Ventilation and Air-Conditioning systems)

I

I2C (inter-integrated circuit)

I (Informed)

IAST (interactive application security testing)

IC/s (Integrated Circuit/s)

ID (Identifier)

IDPS (intrusion detection and prevention system)

IDS (intrusion detection system manager, a AUTOSAR module, IDPS and IDS are almost the same)

IEEE (Institute of Electrical and Electronics Engineers)

IO (input/output)

IoV (Internet of vehicles)

IoT (internet of things)

IPC (inter-process communication)

IPv6 (Internet Protocol address Version 6)

ISA (intelligent speed assistance)

ISP (image signal processor)

ISO (International Organization for Standardization)

IVI (in-vehicle infotainment)

J

JTAG (joint test action group)

K

L

LAN (Local Area Network)

Leddar (LED + raDAR)

LIDAR (LIght Detection And Ranging)

LF (low frequency)

LIN (local interconnect network)

LKA (lane keep assist)

LLC (logical link control)

LRR (long-range radar)

LTE (long-term evolution - 4th generation cellular communication network)

LVDS (low voltage differential signaling)

M

MAC (mandatory/medium access control/message authentication code)

MACsec (media access control security)

MISRA (motor industry software reliability association)

MITM (man-in-the-middle (attack))

MITRE ATT&CK (adversarial tactics, techniques, and common knowledge)

ML (machine learning)

MRR (mid-range radar)

N

NAND (NOT-AND, logic gate)

NFC (near-field communication)

NHTSA (national highway traffic safety administration)

NIST (national institute of standards and technology)

NV (Non-volatile)

N/W (network)

O

O (Operational)

OBD (Onboard diagnostics)

OCPP (Open Charge Point Protocol)

OCSP (online status certificate protocol)

OOM (out of memory)

OpenSSL (open secure sockets layer)

OS (Operating System)

OTA (Over The Air - software update through wireless channel)

OTC (One-time cookie)

OTP (one-time programmable)

P

P (legal/Privacy)

PC (personal computer)

PCI DSS (Payment Card Industry Data Security Standard)

PEN (penetration testing)

PII (personally identifiable information)

PKI (public key infrastructure)

PLCP (Physical Layer Convergence Protocol)

PMD (Physical Medium Dependent)

P-RBAC (privacy aware role-based access control)

PQC (post quantum cryptography)

Q

R

R (Responsible)

RA (registration authority)

RBAC (role-based access control)

RASIC (Responsible, Accountable, Supportive, Informed and Consulted)

RF (radio frequency)

RFID (radio frequency identifier)

RO (read-only)

RootFS (Root File System)

RoT (root of trust)

ROW (Rest Of the World)

RSU (roadside unit)

RW (read write)

S

S (Supportive)

S (Safety)

SAODV (secure ad hoc on-demand distance vector)

SAST (static application security testing)

SCA (Side-channel attacks)

SCA (SW complexity analysis)

SD-card (secure digital card)

SDR (software-defined radios)

SDV (software-driven vehicles)

SEAD (Secure and Efficient Ad hoc Distance)

SecOC (secure onboard communication)

Serdes (serializer-deserializer)

SFOP (Safety, Financial, Operational, legal/Privacy)

SHE (secure hardware extension)
SID (session ID)
SIM (subscriber identity module)
SOC (system on chip)
SOME/IP (scalable Service Oriented Middleware over IP)
SOTA (secure over the air, update)
SPA (simple power analysis)
SPEA (Simple Photonic Emission Analysis)
SRR (short-range radar)
SSL (secure sockets layer)
SW (software)

T

TARA (threat analysis and risk assessment)
TCM (Telematics Control Module)
TCP (Transmission Control Protocol)
TCU (telematics control unit)
TEE (trusted execution environment)
TLS (transport layer security)
TP (trusted platform)
TPMS (tire-pressure monitoring system)
T-RBAC (task-role-based access control)

U

UART (universal asynchronous receiver-transmitter)
UDP (User Data Protocol)

UNR (united nations regulations)

USB (universal serial interface)

USS (ultrasonic sensor)

V

V2C (Vehicle to cloud)

V2G (vehicle to grid)

V2I (vehicle to infrastructure)

V2P (vehicle to pedestrian)

V2V (vehicle to vehicle)

V2X (vehicle to everything)

VANET (Vehicular Ad-hoc NETwork)

VKMS (vehicle key management system/virtual key management system of AUTOSAR)

VM (virtual machine)

VSOC (vehicle security operations centre)

W

WAN (Wide Area Network)

WiFi/Wi-Fi (wireless fidelity)

WO (write only)

WORM (write-once, read-many)

X

Y

Z

LIST OF TABLES

Table 1: V2*	11
Table 2: Generic cybersecurity attacks having major impacts. Source (Mohammad Ali Sayed a et al. , 2021)	50

Table 3:Artifacts concerning each phase of the vehicle lifecycle.....	52
Table 4:Sample RASIC matrix for the ADAS ECU (sub-system) TARA artifact.....	54
Table 5: Attack feasibility estimation	59
Table 6: Damage impact	61
Table 7: Risk matrix.....	62
Table 8: CA - total attack feasibility rating is $100 + 10 + 10 + 10 + 10 + 20 = 160$ -> high attack feasibility	63
Table 9: Sample damage impact is High (SFOP total= $100 + 50 + 10 = 160$ (>100))	64
Table 10: Automotive security process artificats.....	68
Table 11: Camera - total attack feasibility rating is $10 + 100 + 10 + 10 + 100 + 10 + 5 + 5 + 0 = 250$ -> high attack feasibility	86
Table 12: Camera - damage impact is High (SFOP total= $100 + 15 + 5 + 12 = 132$ (>100))	87
Table 13: Radar - total attack feasibility rating is $10 + 100 + 0 + 0 + 10 + 5 + 0 + 10 + 0 = 135$ -> high attack feasibility	89
Table 14: Radar - damage impact is High (SFOP total= $100 + 15 + 5 + 12 = 132$ (>100))	91
Table 15: Lidar - total attack feasibility rating is $10 + 100 + 0 + 5 + 10 + 5 + 0 + 10 + 0 = 140$ -> high attack feasibility	93
Table 16: Lidar - damage impact is High (SFOP total= $100 + 15 + 5 + 12 = 132$ (>100))	95
Table 17: Ultrasonics - total attack feasibility rating is $10 + 100 + 10 + 10 + 10 + 5 + 0 + 10 + 0 =$ 155 -> high attack feasibility	97
Table 18: Ultrasonic - damage impact is High (SFOP total= $100 + 15 + 15 + 0 = 130$ (>100))	99
Table 19: IVI – mobile communication - total attack feasibility rating is $10 + 100 + 10 + 10 + 10 + 5 + 0 + 10 + 0 = 155$ -> high attack feasibility	101

Table 20: IVI – mobile communication - damage impact is High (SFOP total=100+50+10+25 = 185 (>100)	103
Table 21: IVI – miscellaneous interfaces - total attack feasibility rating is 50+100+10+10+10+5+5+10+20 = 220 -> high attack feasibility	105
Table 22: IVI – Miscellaneous interfaces - damage impact is High (SFOP total=100+10+10+25 = 145 (>100)	108
Table 23: Telematics - total attack feasibility rating is 50+100+10+10+100+5+5+10+20 = 310 -> high attack feasibility	110
Table 24: Telematics - damage impact is High (SFOP total=100+50+10+25 = 185 (>100)	112
Table 25: V2X - total attack feasibility rating is 50+100+10+10+100+10+5+10+20 = 315 -> high attack feasibility	114
Table 26: V2X - damage impact is High (SFOP total=100+50+10+12 = 172 (>100)...	117
Table 27: Keys and certificates in-vehicle ECUs - total attack feasibility rating is 50+100+10+10+0+5+5+10+10 = 200 -> high attack feasibility	119
Table 28: Keys and certificates management in-vehicle ECUs - damage impact is High (SFOP total=100+50+10+25 = 185 (>100)	122
Table 29: EV electric charging - total attack feasibility rating is 50+ 100+10+10+ 100+10+5+15+20 = 320 -> high attack feasibility	124
Table 30: EV electric charging - damage impact is High (SFOP total=50+50+10+25 = 135 (>100)).....	126
Table 31: OBD port - total attack feasibility rating is 50+100+5+10+100+10+5+15+20 = 315 -> high attack feasibility	128
Table 32: OBD port - damage impact is High (SFOP total=100+50+10+25 = 185 (>100)	131

Table 33: Keyless door entry - total attack feasibility rating is	
50+100+10+10+100+10+5+5+20 = 315 -> high attack feasibility	132
Table 34: Keyless door entry - damage impact is High (SFOP total=50+50+5+12 = 117	
(>100).....	135
Table 35: Two-wheeler electronic systems - total attack feasibility rating is	
50+100+10+10+100+10+5+5+20 = 315 -> high attack feasibility	137
Table 36: Two-wheeler electronic systems - damage impact is High (SFOP	
total=100+50+15+25 = 190 (>100)	140
Table 37: Summary of attack feasibility and damage impact SFOP score for each use	
case.....	141

LIST OF FIGURES

Figure 1: Item definition sample.....	56
Figure 2: Attack tree	58
Figure 3: Sample attack tree for a digital certificate.....	65
Figure 4: (https://www.mckinsey.com/ , 2020)	67