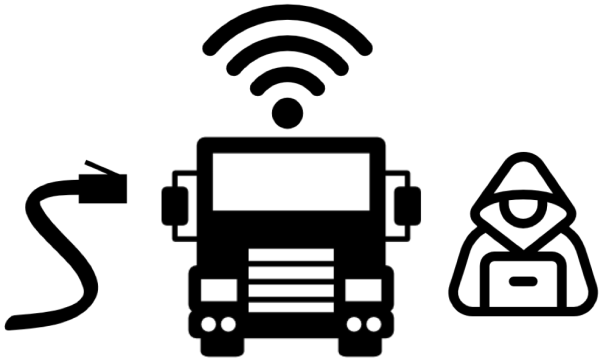
UNIVERSITY OF TWENTE
FACULTY OF ELECTRICAL ENGINEERING, MATHEMATICS AND
COMPUTER SCIENCE DESIGN AND ANALYSIS OF
COMMUNICATION SYSTEMS GROUP



MASTER OF SCIENCE THESIS

SECURITY RISK ANALYSIS OF AUTOMOTIVE ETHERNET NETWORKS

BY
AMIT GUPTA

COMMITTEE
Prof. Dr. Ir. Geert Heijenk
Mr. Niklas Wiberg (Scania AB)
Dr. Anna Sperotto

UNIVERSITY OF TWENTE. UNIVERSITY OF TRENTO SCANIA

23 OCTOBER 2017

SUPERVISORS:
Prof. Dr. Ir. Geert Heijenk (University of Twente, Netherlands)
Mr. Niklas Wiberg (Scania AB, Sweden)
SECOND READER:
Prof. Dr. Ir. Fabio Masacci (University of Trento, Italy)

SÖDERTÄLJE, SWEDEN

ABSTRACT

Modern vehicular systems house a number of high computation devices and fleets of sensory networks. While functional subsystems like Advance Driver Assistance Systems (ADAS), safety systems, Human Machine Interfaces (HMI) form the foundations to (semi)autonomy of vehicles, any possibility of a threat to safety and security are intolerable.

These progressive functional domains are tightly coupled with modern IT infrastructures and demand high bandwidth communication channels. By offering improved bandwidth over the single twisted pair, automotive Ethernet solves this problem over former Controller Area Network (CAN). However, it could also bring a variety of security threats which need to be examined.

Security risk assessment is an effective process of discovering, correcting and preventing the occurrence of unanticipated security threats. The Master thesis proposes a security risk assessment methodology for Ethernet-based vehicular networks. The methodology is a four-step iterative process model and offers a structured approach to design, analyze, assess, mitigate and record rationale behind assessments.

ACKNOWLEDGEMENTS

This Master thesis marks the end of my two-year graduate program in Security and Privacy. The work would not have been possible without the contribution and constant support of many great people. First and foremost, I would like to thank my supervisor at Scania, Mr. Niklas Wiberg. Niklas is a Senior Security Architect at Scania and has a distinguished research acumen. I learned many things from Niklas both scientifically and socially, and I look forward to keeping that up as I continue working full-time at Scania after I complete my masters.

Secondly, I had the honor to be supervised by Professor Geert Heijenk. I don't know many professors like Prof. Geert; he is a highly respected man in our field but still very modest and supporting. He has been kind in providing insights on my research when I needed his help.

I would also take this opportunity to thank my fellow members and Security Experts at Scania Mr. Lars Gunnar, Mr. Kristofer Frederiksen for their insightful discussions to help me understand the automotive domain.

My journey in the last two years would not have been possible without the continuous support of my family and friends. I would want to sincerely express my gratitude to my brother Manish Sonal for his guidance. I would be grateful to my parents, Mr. Raj Kishore and Janki Devi and my sisters Shweta, Manisha, and Neha for their unconditional love and support.

There were many other people involved in this research including my colleagues at University of Trento (Italy), University of Twente (Netherlands) and Scania (Sweden) and I would like to thank them all for motivating me socially, academically, and intellectually. Special thanks to Sina Davanian, Manish Kumar, Alexandra Goman and Mohit Ahuja for being there whenever I needed them.

Last, but by no means least, I would like to thank God for introducing such amazing people into my life. I dedicate this dissertation unto him.

LIST OF TABLES

LIST OF FIGURES

CONTENTS

ACRONYMS AND DEFINITIONS

ACU	The Automation Control Unit (ACU) houses the vehicle's on-board intelligence and executes all automation and assistance functions. Collects data from the vehicle's numerous sensors and combines them to give a comprehensive view of the surrounding area. The control unit also receives transport missions from the off-board logistics system and translates them into instructions that the vehicle systems can understand [11].
ADAS	Advance Driver Assistance System
ADC	ADAS domain controller
ASRAT	Adapted Security Risk Analysis Tool. This tool is one of the contributions of the master thesis and is further explained in chapter 3
CAN	Controller Area Network (CAN) is a serial field-bus communication network. CAN is mostly used in a vehicular network. The bus arrangement reduces the number of connections between nodes. Each node has a single 2-way connection to the bus. It is a message-based protocol, designed originally for multiplex electrical wiring within automobiles, but is also used in many other contexts [55].
DAAM	An acronym given to the tailored security risk assessment model that is proposed in the scope of this thesis. The acronym stands for four steps of the process, namely, Draw-Analyze-Assess-Mitigate
DEC	A Discrete Electric Circuit system (DEC-system) is a set of components such as sensors, actuators, cabling etc. with no ECU at all or an ECU not connected to any of the CAN-buses. Example: The power supply components constitute a DEC-system. The components for the electric seat control constitute a DEC-system.
ECU	In general, an Electronic Control Unit is a system that controls one or multiple other electrical systems/subsystems. A set of sensors connected to an ECU make an ECU System. e.g.: The coordinator ECU with the connected equipment (fuel level sensors, pedal-position sensors etc) constitutes an ECU system.

EMI/EMC	Electromagnetic compatibility (EMC) is the process of checking unintentional generation, propagation, and reception of electromagnetic energy which may cause unwanted effects such as electromagnetic interference (EMI), specially in electronic/electrical systems.
HCV	Heavy Commercial Vehicles. e.g. Trucks, Busses, Trolleys, etc.
HMI	Human Media Interface
IOCTL	IOCTL (an abbreviation of input/output control) is a system call for device-specific input/output operations and other operations which cannot be expressed by regular system calls. It takes a parameter specifying a request code; the effect of a call depends completely on the request code.
LCPV	Light Weight Commercial and Private Vehicles. e.g. Private cars, vans, etc.
LIN	Local Interconnect Network is a serial network protocol used for communication between components in vehicles. LIN was developed as a simpler, more cost-effective alternative field-bus technology for bit rates (Table 2.2) on par with Low Speed CAN [55].
MSTMT	Microsoft Threat Modeling Tool [43].
SOHO	SOHO is an acronym for 'small office or home office' networks. Typically, SOHOs are subnets with 1 to 20 nodes.
USE CASES	Use cases are defined as a set of well defined actions/events which are performed by actors/persona to achieve a given goal. The actor can be a human, an event generator or any other external stimuli. We assume that a vehicular network is a big system which is made by integration of multiple subsystems. Each subsystem has well-defined tasks and dependent processes. e.g. infotainment subsystem (information and entertainment), the ADAS [40] subsystem, breaking subsystem, etc. An example of use case can be the driver of the vehicle, a persona, playing his favorite song on the infotainment subsystem.
V2X	Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, collectively referred as V2X, is a wireless technology aimed at increasing road safety and improve traffic management, introducing a new concept of intelligent transport system (ITS), capable to reduce environmental impact.

1 INTRODUCTION

This chapter is an introduction to the master thesis project on defining a structured process for performing security risk analysis of vehicular Ethernet networks. The chapter provides a high level background about the growth of applied information technologies (IT) in vehicles and the aspects of cybersecurity around vehicular Ethernet.The chapter then throws some light on the motivations of the research and gives an insight on the research questions and methodologies that were followed in the project. The later chapters of the thesis provide an in-depth explanation of research steps, learning, experiments and contributions; however, with the knowledge of the overall document will help the reader understand the project better.

1.1 BACKGROUND

With time, the automotive industry has been housing revolutions of changes and developments at a very high pace. Since 1672 when Flemish Jesuit missionary Ferdinand Verbiest (1623-88) resorted the Italian engineer Giovanni Branca's steam-turbine idea (1624) [17], we have come quite far with todays high-tech smart vehicles running as fast as 430 km/h without lifting off the roads surface [21, 57]. Since then, a lot has changed in and around the vehicle. One of the most important developments that has made the advanced functionalities, user experience and safety features in a modern vehicle is the integration of cutting edge information technologies (IT).

Today's vehicle can be seen as a vehicular system which is a composite of mechanical, electronics and complex IT systems. A modern vehicle utilizes a wide range of sensors and actuators to convert the information from the physical surroundings into digital form and then take dependent decisions. In general, the processing of the readings from these sensors are executed in small computers called Electronic Control Units (ECU). There are numerous ECUs in a vehicle. ECUs can be seen as the building blocks of a modern vehicle's complex communication network. Ranging from better fuel consumption, opening the airbags on time, controlling the headlights, air-conditioners or assisting the driver for parking, ECUs are used everywhere.

Autonomous vehicles mark the most recent developments in this domain. Various global companies are working towards smart and autonomous vehicles and aim towards improved safety, user experience and security. These engineering trends bring about even more dependency and requirements on the vehicular IT and communication networks. The vehicles not only need to process a very high amount of data in real time, but also need to be connected to each other and to the internet.

To meet the high demands of communication bandwidth in the vehicular network, the need was to move from generation old CAN (Controller Area Network) to Ethernet. Ethernet brings in improved bandwidth, communication speed and security features to the vehicular network. The application of Ethernet in a vehicular network is also termed as vehicular Ethernet. Vehicular Ethernet is a big change to the existing IT in the vehicle and would baseline the next generation vehicular systems. As vehicular Ethernet brings

opportunities to build great features, it also brings the security risks and vulnerabilities to the context.

1.2 MOTIVATION OF RESEARCH

Modern vehicular systems house a number of high computation devices and fleets of sensory networks. This increased coupling of the vehicle's physical features with the IT infrastructure which contribute to build the foundations towards advanced driver assistance systems and ultimately towards full autonomy of the vehicle.

Security in vehicular networks

In earlier days, the vehicles used to be dominantly sophisticated mechanical wagons with wired electrical systems for meeting necessary functional requirements like headlights, breaks, throttle control, steering and similar fundamental functionalities.

One might say that these first generation vehicles were less reliable and more susceptible to safety risks and breakdown; However, it can be argued that with sufficient usage data and predictive analysis, the malfunctions parts have could be pro-actively replaced to minimize the safety risks. Today's vehicles abode numerous computational devices (ECUs) which are connected to each other and the internet through high-speed connections. In the case of modern vehicles, with advanced driver assistance systems (ADAS), pro-active prediction of malfunctioning parts is not the only challenge, but the more significant problem is to secure these electro-IT systems from unauthorized access infringements and unanticipated computational overloads. This need calls for a requirement to secure the vehicular network against cyber attacks and infringements.

Historically, to protect the vehicle against the attacker, the solution of preventing unauthorized physical access using hardened locks solved the purpose. However, for today's software-based vehicular networks, the security against physical access is just a part of the problem. With increased attack surface, the challenge is to secure the cyber-physical system from any possibility of being compromised.

To preserve the standards of security, there are many secure engineering practices have been actively adopted in the industry. Some of the techniques include writing secure code for the ECUs, perform rigorous penetration tests and most importantly, pro-active security risk assessment of the communication networks.

Automotive Ethernet at Scania

Scania is a European truck manufacturing company and is a part of Volkswagen group's Truck & Bus business. Scania is primarily known as a global supplier and a mass manufacturer of heavy-duty trucks and public transport buses. The company's R&D is working towards future-ready heavy commercial vehicles with advanced driver assistance (ADAS) features. Meeting the functional requirements involves a multitudinous use of sensory networks in the vehicle. To provide a suitable infrastructure, the heavy vehicles need to have high-speed communication channels. Hence, the vehicular networks are considering to utilize Ethernet in conjunction with the CAN network (or replace the CAN with Ethernet, in future). This adoption

is a significant change and in a way will lead to changes in many dimensions including architectural design, security, safety, EMI/EMC, etc.

To perform the experiments, as mentioned in Chapter 4, the functional domains of Scania's trucks were studied. Working in the organization's research center also helped in learning from the internal documents and discussions with subject matter experts (SME). Thus, apart from contributing to science, this research project also aims to support Scania (and other vehicle manufacturers) in the secure adoption of Ethernet for the communication networks.

While adoption of Ethernet enables possibilities of adding advanced functional features by serving higher bandwidth capacity, its introduction may also increase the attack surfaces for the vehicular networks. It is therefore crucial for the architects to perform a structured risk assessment of vehicular Ethernet and mitigate the risks before production.

1.3 RESEARCH QUESTION AND SUB-QUESTIONS

In its scope, the project explains a perspective of the high-level functional requirements of a heavy duty truck and the available tools to perform security risk assessment of a vehicular communication network, based on its network topology. The knowledge of the functional requirements of a vehicular communication network will help us in defining processes which are more specific to the needs or may also help us in tailoring the existing tools to suit the needs and empirically verify the contributions.

In this section, the research question and the sub-questions are proposed. The rest of the sections of the thesis attempts to answer the research question and the sub-questions. The sub-questions, in a way, contribute to the answers to the primary research question. In the later sections of the project, as we proceed, the sub-questions would be answered.

This brings us to the research question:

> **RQ:** *How to perform security risk assessment of a vehicular Ethernet network, based on its network topology?*

Sub-questions

However, to get the answers to the research question (RQ), the following sub-questions would be answered in the course of the thesis report. With the undermentioned sub-questions, the motive behind each question is also mentioned; this is just to make it easier for the reader to draw the links between each sub-question to the main purpose of the project:

> **SQ 1A:** What are the relevant models and tools that can be used to analyze security threats and security risks for vehicular networks?
>
> **SQ 1B:** Can we make use of the available security threat assessment tools to customize them for vehicular network
>
> ***Motive:***
> *To understand why an off-the-shelf tool can not be utilized to perform risk assessment for vehicular network. This knowledge will also help in making use of an available tool by customizing or amending it. This learning will help in designing the customized DAAM methodology in Chapter 3.*

SQ 2: What are the functional requirements of heavy commercial vehicles subsystems?

Motive:
To understand the requirements of the network components in terms of bandwidth, QoS, trust boundaries, channels, etc. This information will help in designing high level network topology for validation experiment in Chapter 4.

SQ 3: Based on the experimental study, what are the security recommendations for vehicular networks?

Motive:
We perform the experiment in Chapter 4 to run the DAAM process model. The motive behind this question is to objectively identify the security recommendations from the analysis. This information can be used to enhance Microsoft Threat Modeling Tool's (MSTMT; refer Chapter 3) template.

1.4 RESEARCH APPROACH

To seek answers to the above mentioned research question and sub-questions, the planned approach was followed.

We started with understanding the domain for which we wanted to perform the security risk assessment. One way to do this was to understand the functionality of the domains of vehicle's communication network. To understand the bigger picture of different functional domains of the vehicle (e.g. infotainment system, ADAS, powertrain, HMI, etc.) and considering the scope of the thesis, the intention was to read Scania's documents about their trucks and their communication network nodes in order to develop a high-level understanding of the functional requirements of the network components. After we come up with a proposal for the risk assessment methodology, we will utilize this knowledge to design a hypothetical network topology (refer Figure 4.3) which utilizes those network components and perform a cybersecurity risk assessment on it. This will not only help us get feedback on the good and bad parts of the process but will also validate the enhancements (refer Chapter 4).

The master thesis project was performed at Scania R&D facility in Sweden. As the thesis addresses problems in the domain of vehicular networks and security, working on the premises of a vehicle manufacturing organization was of great help. Throughout the research, apart from available literature from online sources, numerous Scania internal documents were referred (see section 1.5).

As mentioned in Chapter 2, we performed a structured literature review for existing security threat assessment methodologies and security risk assessment tools, in perspective of being utilized for an Ethernet-based network topology. A number of existing methodologies were found for security risk assessment of native networks and web applications, however none of the available tools met the demands of assessing the security risk for Ethernet-based vehicular communication networks, hence a customized methodology was designed by amending MS Threat modeling tool template and creating a risk assessment model called ASRAT.

There are two prime advantages of the DAAM (Draw-Analyze-Assess-Mitigate) process model. First is that DAAM is built by customizing one of the existing threat assessment tools which is widely accepted and used in the industry, so that offers better chances of the derived tool being accepted

by the industry; the other advantage is the constituent ASRAT tool which can be used to record and learn from security experts' feedback to provide automatic assistance for security assessments (refer Section 5.2). Chapter 3 describes the process of designing the customized process model in detail. Later in Chapter 4, we validate the proposed model and improve the process design based on the feedback from security experts.

1.5 REVIEW METHODS

As explained in Figure 1.1, a 5 step filtering process is followed to search for relevant literature in the domain. The search was done manually over the available data repositories like Google Scholar, Scanias internal data repositories. Apart from this a lot of information was also gathered from resources published on public Internet like keynotes, slides, presentations and videos by automotive manufacturers like BMW, Volvo, Daimler, etc. who have been working on using Ethernet for their light weight vehicles.

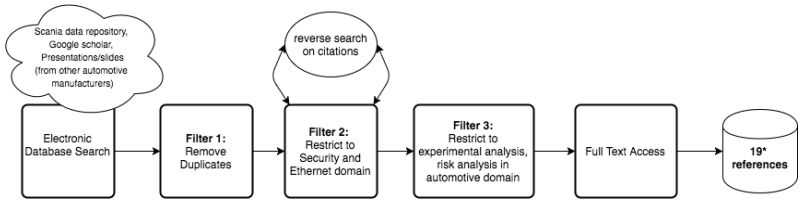


Figure 1.1: Selection of literature papers. Inspired systematic literature reviews in software engineering by Kitchenham et al. [29]

As explained in Figure 1.2, to perform a systematic review of the state-of-the-art documents, a 5-steps process was followed. In this "retrospect" step, the artifact was contemplated on two grounds:

1. Could the problem discussed in the paper, be approached any differently?
2. Is there an opportunity to support or challenge the results of the paper?

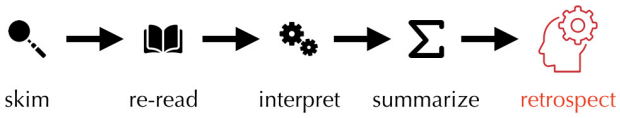


Figure 1.2: Strategy to read research papers.

The state of the art study (see Chapter 2) focuses on three aspects:

A. To understand the need of Ethernet in vehicular networks and the replacement of existing network protocols like CAN

B. To understand the challenges in the domain of cybersecurity and privacy with this transition

C. To understand the available tools which can help solving the problem of security risk assessment for Ethernet based vehicular networks based on their topology

1.6 RESEARCH CONTRIBUTIONS

This thesis aims to contribute in the domain of cybersecurity risk assessment of communication networks in a vehicle. The project was inspired by an existing problem in the vehicular manufacturing industry and hence offers a fusion of learning from state-of-the-art literature and experience from security experts from the industry.

The thesis project contributes to the science and industry, both in long term and short term.

Contribution to science

The literature (Chapter 2) draws that for meeting the advanced functional requirements of the vehicles of future, adoption of Ethernet is desired. Before vehicular Ethernet, CAN has been predominantly used in this domain. This transition is anticipated to bring a number of security risks to the automotive. As the prime contribution of this master thesis, a structured security risk assessment process model (Figure 4.4) is proposed. The DAAM process model is a 4 step iterative process which is built using a specially customized MS Threat Modeling Tool (MSTMT) template and an excel based Adapted Security Risk Assessment Tool (ASRAT).

Researchers working in the domain of vehicular security and security of communication networks can contribute to the developments by enhancing the logic, components, and design of MSTMT template and making use of the ASRAT to perform structured analysis for their risk analysis research. Since the ASRAT tool helps the security analysts keep a detailed log of the rationale behind security decisions, this data can be plausible used to catalyze the security recommendations and reduce risk, as explained in section 5.2.

An experimental validation of the DAAM process model was executed based on the functional requirements of a Scania truck (refer Chapter 4). As mentioned in Section 4.4, based on the experimental analysis the four-step DAAM process was improved.

Contribution to industry

The thesis project is inspired by the security risk assessment practices in the industry, hence, it finds and immediate use case. One of the outputs of the project is a security risk assessment tool which implements the four step DAAM process model. As described in Chapter 3, the security risk assessment process model consists of industry standards tools and techniques, specially tailored for security analysis of vehicular networks. For easier reference, we will refer the process model as the DAAM tool or the DAAM process model.

The DAAM tool aims to improve the process of assessing the cybersecurity risk for Ethernet based vehicular networks. The findings propose a structured cybersecurity risk assessment process customized for Ethernet based vehicular networks. The security architects in industry can thereby use the proposed risk assessment model to:

1. Perform structured security risk assessment of the Ethernet based network topology for the vehicular networks
2. Make use of the descriptive logging tool to persist details about their rational assessment decisions, which then can be easily consumed and enhanced by future groups in the organization

3. Contribute (and customize) to enhance the threat generation tool for the public use or for the internal use of their organization

In Chapter 4, we validate the DAAM tool by running it through high level functional use cases of a Scania truck. The security experts in the industry were also interviewed to retrospect and improve the tool (see section 4.3). Hence, it can be said that the thesis directly contributes to the industry by enabling a structure to the security risk assessment processes.

1.7 OUTLINE OF THE THESIS REPORT

The report is divided into five chapters followed by appendix and bibliography. Each chapter has some sections and subsections based on the information that is being discussed. In Chapter 1, the introduction of thesis project and motivations are explained. Chapter 1 also proposes the research question and sub-questions. In Chapter 2, we discuss the relevant state-of-the-art and concepts that constitute to the contributions. This Chapter also brings about the need to have a tailored risk assessment model for vehicular networks. Later in Chapter 3, the design of the four-step DAAM process model is proposed which is validated through an experiment in Chapter 4. The introspection and amendments to the design of the process model are also discussed in this chapter. To summarize the conclusions, in Chapter 5, the limitation, and possible future enhancements are discussed.

2 BACKGROUND AND RELATED WORK

2.1 RELEVANT CONCEPTS

2.1.1 Ethernet and CAN

Ethernet is a network protocol that controls how data is transmitted over a LAN. Technically it is referred to as the IEEE 802.3 protocol. The protocol has evolved and improved over time and can now deliver at the speed of a gigabit per second.

BroadR-Reach technology is an Ethernet physical layer standard designed for use in automotive connectivity applications. BroadR-Reach technology allows multiple in-vehicle systems to simultaneously access information over unshielded single twisted pair cable.

In many ways, it is not possible to directly compare the CAN protocol to Ethernet. As Ethernet alone does not provide many security features, apart from frame sequence check, it goes almost unmentioned that Ethernet comes with a higher level protocol suite, namely, TCP/IP. Henceforth in this document, unless mentioned, by Ethernet we mean Ethernet with TCP/IP.

As mentioned by [32], Ethernet is not a replacement for the CAN based network infrastructure but will be used in junction with the CAN. Based on the learnings from infrastructure requirements of heavy commercial vehicle (truck) at Scania AB, it is understood that the network design will observe significant changes. The components (or nodes) of the network in a vehicle are the ECUs. With introduction of Ethernet, the network nodes would be connected through network switches and routers. Apart from this, the availability of higher bandwidth will also support improved sensor data fusion, data processing and connectivity to infrastructures (V2X).

In his research on automotive Ethernet, Hank et al. propose that even though today, the vehicle communication networks appears as a heterogeneous system as a result of its historically grown nature, new vehicle communication systems without legacy would most likely have a domain based architecture like the one shown in Figure 2.1 where the ECUs are composed in a clear hierarchical architecture [19]. In this model, the application domains are connected through a 'data highway' where wired and wireless interfaces allow communication between the vehicle and its environment.

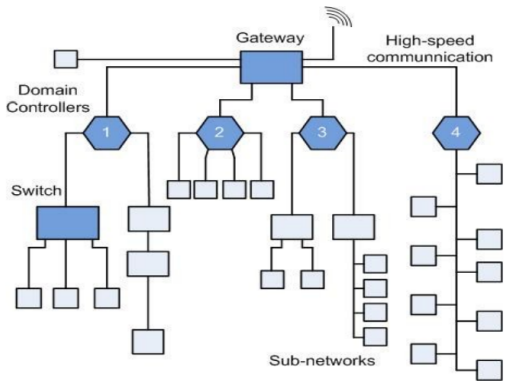


Figure 2.1: Domain based architecture in automotive Ethernet[19]

Konrad Etschberger [1] mentions a comparison between CAN and Ethernet frame speeds or FPS (Frames Per Second), as under:

Standard Ethernet

```
Start Frame Delimiter (1 Byte),
Destination MAC Address (6 Bytes),
Source MAC Address (6 Bytes),
IP-Header (20 Bytes),
TCP-Header (20 Bytes),
Padding Bytes (if Payload is less than 46 Bytes)(6 Bytes),
Frame Check Sequence (4 Bytes),

Inter-frame Gap (96 Bits) (12 Bytes):
Total Minimum Frame length (1 .. 6 Data Bytes Payload) = 84
    Bytes, 7 Data Bytes: 85 Bytes; 8 Data Bytes: 86 Bytes

With Standard Ethernet we have to consider an increased
    percentage of bus collisions when the bus load is higher
    than 20 percent (at about 50 percent bus load there are
    only bus collisions).

Therefore only about 20 percent of the bandwidth actually is
    available.

: 10 Mbps Ethernet :
Transmission of 1- 6 Data Bytes:
Maximum number of frames per second = (20 percent of
    10.000.000 bits/s) : 84*8 bits/Frame = 0,2 * 14.881 =
    2.976 Frames/s}
Transmission of 8 Data Bytes:}
Maximum number of frames per second = (20 percent of
    10.000.000 bits/s) : 86*8 bits/Frame =0,2 * 14.535 =
    2.902 Frames/s }

With 100 Mbps Ethernet the maximum number of frames per
    second is about 29.000 Frames/s.
```

Controller Area Network (CAN)

```
Total Frame Length: SOF (1 Bit),
Identifier+ RTR (12 Bit),
Data Length Code (6 Bits),
Data Field (0..64 Bits),
CRC (16 Bits),
ACK-Field (2 Bits),
EOF (7 Bits),
Inter-frame Space (3 Bits);

Stuff Bits (3 Bits)1 : Total Frame Length: 58 Bits (1 Data
    Byte Payload)  ..114 Bits (8 Data Bytes Payload)
```

1 Comparing CAN and Ethernet-based Communication - Konrad Etschberger

1 Mbps CAN
With CAN we can load a system theoretically up to a bus load of 100 % without no fear of collision; this is possible also practically if we have frames which are not very time critical. If there is a higher percentage of frames for which no longer delay are acceptable we also should reduce the maximum bus load. In the following 100% bus load is assumed.

```
8 Data Bytes
Maximum number of frames per second = 1.000.000 bits/s : 114
    bits/Frame = 8.772 Frames/s
```

Though CAN offered a better prediction in transmission lag and latency, Ethernet offers a great service on the frame transmission rate and process scheduling [9]. Based on its applications in intra-vehicular networks, it can be said that CAN was primarily designed for short distances in electrically noisy and generally hostile automotive applications. CAN signals runs at relatively slow speeds, but with high reliability, often using unbalanced power plus data wiring.

2.1.2 Ethernet in automotive

The heavy vehicle transportation industry plays an integral role in moving economies of the world. There have been constant attempts to make the transport system better - concerning safety and security. Human carelessness and lack of performance efficacy can result in threats to life and property. Experiments show that sleep is a significant cause of accidents in industry and transport [42]. Self-driving trucks are estimated to eliminate these incidents marginally and also increase the average speed of highway traffic. Gillberg et al. have recorded results from simulations of professional drivers that demonstrate remarkable differences in human driving behaviors for the day and night driving. The night driving was found to be slower, with high variation in speed and deviations in lane positions [16].

Researchers have been working on taking small steps towards autonomous driving. e.g., The truck platoon project developed under a Japanese National Intelligent Transport System (ITS) project named Energy ITS[2] [58] has been a great success. Given the test conditions, Tsugawa et al. claim that fuel consumption measurement on a test track and along an expressway can be reduced by about 14% [59].

The HCV industry, which has been a bit behind lightweight commercial and private vehicles to observe (semi)autonomous features, is in the limelight now and are seeking revolutionary enhancements.

Typically, in a vehicular network, the infrastructure is divided into functional domains. The communications in different functional domains are observed to be unique in multiple aspects like bandwidth, jitter, availability, data-type, etc. Table 2.1 summarizes the different functional domains and the type of data communicated over established channels in a vehicular network [16]. The effect of a large number of ECUs and fusion of data from sensors provide support to driver safety features like ADAS systems, powertrain, etc. are well captured Tuhoy et al. [60] - the research also elicits the need for ensuring and maintaining the security of such electrical networks.

Today the intra-vehicular communication channels in the heavy vehicles are dominated by the wired networks. Even Light-Weight Commercial and Private Vehicles (LCPV) like personal cars house generously long copper

2 NEDO: https://nedo.go.jp

Functional Domain	Communication
Advanced Driver Assistance System	Data for driving support operating without user intervention (rear-view, side-view and top-view services, night vision service, speed limit information, lane departure warning, etc.)
Body and Comfort	Driving unrelated data concerning the comfort of both driver and the passengers (climate control, windows lifts, seat control, mirrors, doors..)
Chassis	Data for control of the vehicle's stability and dynamics
Diagnostics	Data related to the ECU diagnostic sessions and services like security access, read memory data, diagnostic trouble/error codes, enable/disable normal message transmission, reset ECU services, etc. The Diagnostic services in CAN-based communication networks can be analyzed to understand a good deal of information; there are many available tools which help in translating CAN/LIN data dump into user-friendly information.
Infotainment	Driving unrelated data such as audio and video programs, rear seat entertainment, hands-free phones and personal connectivity. Also interactive information like navigation systems, route, and traffic related information, dashboard, head-up display, etc.
Powertrain	Data for control of the engine, transmission, gearbox, etc.
Telematics	Functions involving the technology of sending, receiving and storing information via telecommunication devices in conjunction with effecting control on remote objects. e.g. global navigation satellite system (GLONASS) technology integrated with computers and mobile communications technologies; other applications of telematics units could be - vehicle tracking, trailer tracking, container tracking, fleet management, wireless vehicle safety communications, etc.

Table 2.1: Functional Domains and allied communication data type [5]

Protocol	Data Rate	Latency	Message transmission type
LIN	20 Kbps	Constant	Synchronous
CAN	1 Mbps	Load dependent	Asynchronous
CAN FD	4 Mbps	Load dependent	Asynchronous
FLEX	10 Mbps	Constant	Synchronous and Asynchronous
MOST	24 Mbps	Data stream	Synchronous and Asynchronous
100Base-T1 Ethernet	100 Mbps	$< 3.2\mu s \pm 0.1\mu s$	Synchronous and Asynchronous

Table 2.2: Protocols in automotive networks [49, 20, 55]

wires which composes significantly to the net weight[3]. A substantial part of the cabling in the vehicle is CAN-buses which offers a communication speed up to 1 Mbps (extended up to 5 Mbps) [2], LIN which offers up to 20 kbps [1] and FlexRay which gives a transmission speed of up to 10 Mbps [10].

Table 2.2 summarizes the ratings of the available technology choices for automotive network connection protocols. As Sauerwald [48] mentions, it is not that there is one straight answer to the question - which one amongst CAN, LIN, FlexRay or Ethernet is the best choice for an automotive network; they are all good in their scope of use. The solution lies in the smart, logical use of the technologies according to the requirements, e.g., one of the possibilities could be to use Ethernet for communication between ECUs through switches/gateway and use CAN for use cases when the bandwidth requirement is limited like to control opening/closing vehicle's glass windows.

Hank et al. describe how automotive applications impose a considerably high degree of regulations on their electronics compared to general consumer products, mainly concerning Electromagnetic Compatibility (EMC) [ISO11452] and environmental conditions. Though BroadR-Reach has been accepted, so far, by the industry choice for automotive, there is a high demand for new optimized components which could meet the EMC guidelines [18].

Bottom-line is using Ethernet [37] as a technology of choice for the autonomous automotive has two prime advantages:

1. Ethernet is a great choice of communication technology due to its low cost, speed, flexibility and predictable impact on transmisssion latency.

2. Having standardization in the technology choices would accelerate research to make the design secure and robust

Since Ethernet was standardized by IEEE in 1983, we have had extensive utilization of the technology in Local Area Networks (LAN). It may seem like a familiar choice of technology to bring into the automotive network domain, but on a closer look, the automotive infrastructures are quite different than the legacy SOHO (small office or home office) network infrastructures.

While we had the delight of ensuring the security of legacy Ethernet networks by optimizing the arrangement of infrastructure completely hidden from the intended attacker, cyber-physical systems like vehicles would be in direct physical access to the attacker. However, hacking an automotive

3 http://copperalliance.org.uk/applications/transportation

system is not limited to having physical access to it - there have been incidences when hackers were able to remotely deactivate safety critical systems in an automotive system. e.g. In 2015 alone, there has been four significant failures in the embedded software systems that question their cyber threats, which Wolf termed as "Embedded software in Crisis" [64].

There is a need to shift the paradigm of mindsets of system designers to not just think about security after the product is out there, instead have security as an integral part of the product development life cycle and adopt security principles like design-for-security and design-for-privacy to ensure better modularity and hence security of next generation automotive [44, 45]. On the same lines, Olaf et. al outline the security requirements analysis process that have been applied for ensuring the security of use cases like V2X communication interfaces [46], nomadic device interfacing and on-board diagnostics. Their research has been a contribution to the EVITA project [61].

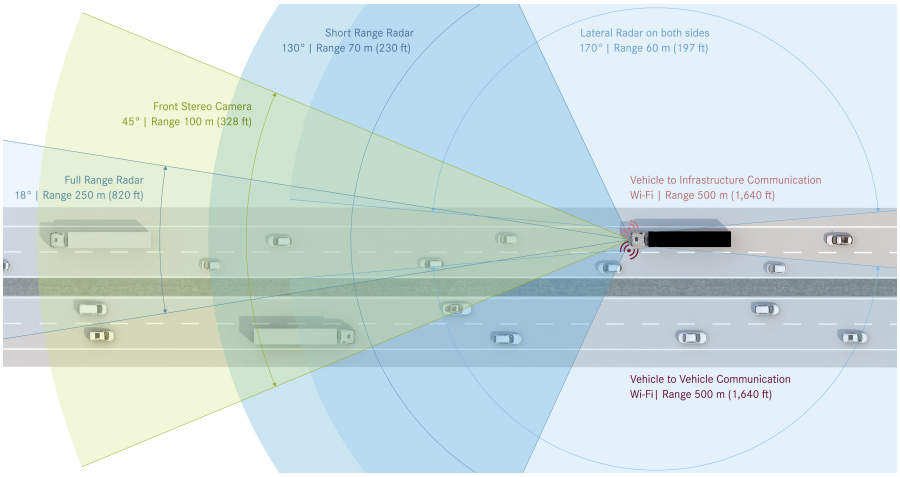


Figure 2.2: Use of multiple short and long range radars along with sensory networks provide a 360 neighborhood view to the HCV in motion. The data signals are transmitted/received at the rate of up to 10 signals/second [28]

.

Artifacts say that many Car manufacturing organizations like BMW [63], Tesla [12] and Mercedes [28] have invested a lot of efforts on R&D to make the vehicles smart and closer to being semi-autonomous. Figure 2.2 showcases the use of an array of radars and cameras for providing vision to an HCV. Daimler recently demonstrated how it could develop such technologies in its Mercedes-Benz Future Truck 2025 to assist drivers to make the right decisions especially in situations of potential road accidents.

The light weight commercial and private vehicles (LCPV) has started to use Ethernet in their communication network, however, advanced heavy commercial vehicles (HCV) are on the verge of adopting Ethernet to meet the high data and high-security demands.

Being used in the industry for a reasonably long time, Ethernet is one of the well-suited choices of technologies to be adopted into the automotive-stack. However, chances are that Ethernet would also bring with itself, the existing security threats and risks to the automotive network unless mitigated.

2.1.3 Security risk assessment

Information security risk assessment is a continuous process that is followed by organizations to pro-actively find the potential threats, estimate the in-

tensity of impacts that the threats can cause (cost), estimate its probability of occurrence and follow corrective steps for its mitigation and prevention. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for their information systems.

The security risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact of each risk. It is a complicated process, and its efficacy more often depends upon the level of expertise of the security analysts.

As mentioned in equation 2, a risk is a function of likelihood and impact of a threat. Nevertheless, there is a significant degree of uncertainty in the likelihood and impact values and thus the risk score, in somewhat subjective or qualitative terms [14]. One challenge in qualitative risk assessment is to estimate the states of likelihood and impact. In some cases, it is also essential that these values are in a manner that allows the same scales to be consistent across multiple risk assessments. Primarily there are six parts of a qualitative risk assessment, as under:

- Identifying Threats
- Identifying Vulnerabilities
- Relating Threats to Vulnerabilities
- Defining Likelihood
- Defining Impact
- Assessing Risk

Later in Chapter 3 we will see how the DAAM tool supports a structured way of keeping account of these methodologies to provide a proper structure to the security risk assessments.

Domain	Count	References
Theoretical Models	4	[53, 15, 24, 25]
Experimental Analysis	5	[6, 7, 22, 31, 41]
Threat Modeling Tools and methods	8	[51, 13, 23, 30, 26, 34, 38, 47]
Others	1	[35]

Table 2.3: Scientific references related security risk/threat analysis based on domains

Artifacts show that there has been a lot of research in the domain of security threat and risk analysis. Table 2.3 gives a snapshot of some of the relevant literature. An example of a theoretical and probabilistic model that signify two very different approaches to solve the problem of similar origin (security risk assessment) are pwnPr3d [24] and intention based threat modeling approach by Waldo et al. [15]. The next section describes the relevant risk assessment tools and scoring mechanisms.

2.1.4 Threat Models

Sub Question # 1

What are the relevant models and tools that can be used to analyze security threats and security risks for vehicular networks?

As mentioned earlier, the thesis project was conducted at Scania AB. Working on a problem in the vehicular domain with one of the well-established

organizations in the industry was helpful to answer this question. In the scope14 of the research, apart from the literature study (section 1.5), the models and tools used in industry were because the feedback from security experts from the industry gave an intense reflection of the best practices that are in training.

Primarily there are three aspects to understand the available tools and models to assess the security risks - threat models, methodologies, and risk assessment rating system. The following discussion explains our findings of the available methods. The target of assessment is to find the most suitable technique for assessing security risks for vehicular networks.

CIA Model Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The CIA-triad has for several decades been serving as a conceptual model of computer security and, later, information security. A wide range of reference materials based on the CIA-triad that explain the concepts usability are available online, despite the fact that the adequacy of the CIA-triad has sometimes been challenged [62, 39, 8].

STRIDE Model STRIDE is an acronym for six categories of threats (see Table 2.4), as coined by Microsoft. STRIDE classification methodology is used to anticipate the threats to a systems' attack surfaces.

As a part of MS Software Development Lifecycle tools, Microsoft also offers MS Threat modeling toolkit which implements STRIDE assessment. Table 2.4 enlists the threat categories under STRIDE.

STRIDE Threat List		
Type	Explanation	Security Control
Spoofing	Threat action aimed to illegally access and use another user's credentials, such as user name and password	Authentication
Tampering	Threat action aimed to maliciously change/modify persistent data, such as persistent data in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Repudiation is the ability of users (legitimate or otherwise) to deny that they performed specific actions/transactions. Without adequate auditing, repudiation attacks are difficult to track.	Non-repudiation
Information disclosure	Threat action to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat aimed to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system.	Authorization

Table 2.4: A threat list of generic threats organized in these categories with examples and the affected security controls (source: OWASP[4])

STRIDE assessment has been widely used in the industry, specially for the web based applications. Microsoft also recommends a step by step process to model the threats, as under:

1. Identify the known threats to the system.
2. Rank the threats in order by decreasing risk.
3. Determine how you will respond to the threats.
4. Identify techniques that mitigate the threats.
5. Choose the appropriate technologies from the identified techniques.

Security analysts are recommended to perform this process more than once as it is difficult to formulate all the possible threats in the first run. Also, technology changes over time, new issues arise, and the business and technical landscape may expose the system to new risks, or make existing threats irrelevant. All of these have an impact on the known threats to the system under consideration.

2.1.5 Modeling Tools

Multiple modeling tools have been considered for the scope of this project. Amongst the requirements to form a risk assessment tool for vehicular networks, having the feature of modeling to understand the variables and constants of the network were considered important. In all, we analyzed four modeling tools, as under:

CORAS [5] CORAS is an acronym for "A Platform for Risk Analysis of Security Critical Systems" and is a model driven method for conducting security risk analysis. It was developed by the European Union (EU) for the purpose of improving the security during the systems design process [36]. CORAS provides a customized language for threat and risk modeling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. In this respect CORAS is model-based. The Unified Modeling Language (UML) is typically used to model the target of the analysis.

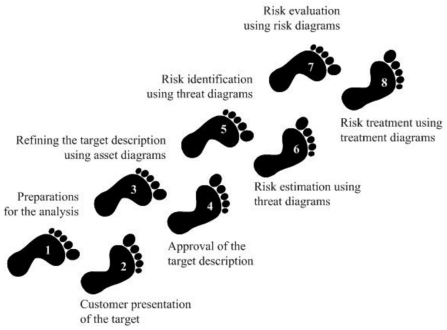


Figure 2.3: CORAS is a UML based security risk assessment methodology with 8 process steps

As explained in Figure 2.3, CORAS is an eight step process for conducting the security risk assessment. Though the process has a very well defined

5 CORAS Tool: http://coras.sourceforge.net/

instruction documentation and structure of implementing CORAS, the UML modeling was not seen as the best option to model the network topology of a vehicular network.

SESAR SecRAM [6] SESAR (Single European Sky ATM Research) is the technological pillar of the Single European Sky. It aims to improve Air Traffic Management (ATM) performance by improving and adapting ATM systems through the definition, development, validation, and deployment of innovative technological and operational ATM solutions [7].

SESAR developed SecRAM as a part of their 16.02.03 project4. The method was used by professionals in the SESAR program to conduct security risk assessments. This method gives a step-wise instruction set and can be applied to any operational focus areas of SESAR. Further, when we use SecRAM, we refer to SESAR SecRAM unless otherwise stated. SecRAM also comes with a detailed documentation which can help the security risk assessment process.

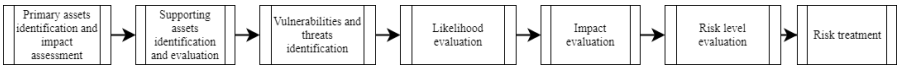


Figure 2.4: Seven step process for SecRAM risk assessment

As described in Figure 2.4, SecRAM process includes seven main steps. Even though the SecRAM process does not give a solution to model the topology of a network on a canvas, the process model for scoring the risks inspired this research project to develop a 3 step tabular structure to log the assessments from a security expert. The developed model is explained in detail in Chapter 3. It is known that the domain-specific security risk assessment catalogues are perceived as easier to use by the domain users [33], so a tool inspired from SecRAM would need to be specific and customized to vehicular network security analysts as they are expected to be the prime users, however, in the course of the research, the focus is to also make into consideration that the tool should have improved ways to log the feedback from the security experts.

OCTAVE [8] OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) "is a risk based strategic assessment and planning technique for security" [4]. OCTAVE is specially used by organizations for security risk evaluation because it both organizational and technological issues, examining how people use their organization's computing infrastructure on a daily basis.

Unlike the typical technology-focused assessment, which is targeted at technological risk and focused on tactical issues, OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues. It is a flexible evaluation that can be tailored for most organizations. When applying OCTAVE, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization, balancing the three key aspects illustrated in Figure 2.5.

Though the OCTAVE model solves security risk problems at operational and practices level, it was not found to be suitable for assessing security risks for vehicular networks, because of the following reasons:

6 SESAR ATM SecRAM: http://www.sesarju.eu/
7 SESAR SecRAM https://ec.europa.eu/transport/modes/air/sesar$_{e}$n
8 OCTAVE RAM: http://www.cert.org/resilience/products-services/octave/

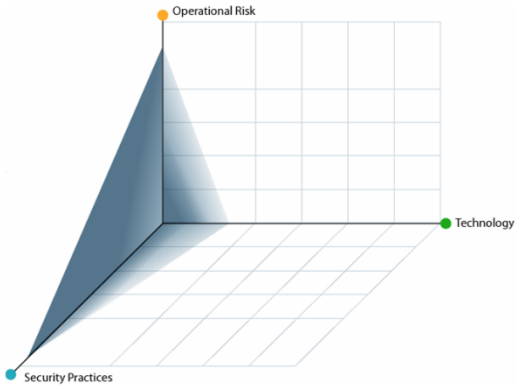


Figure 2.5: Three dimensional OCTAVE assessment model[4]

- **Organizational Evaluation:** While OCTAVE provides an organizational perspective of the security issues; a vehicular risk assessment methodology needs more of a system view of the risks and threats.
- **Focus:** The OCTAVE approach focuses on the security practices, while our need is to have more focus on technology
- **Expert led:** With the rapidly changing world of technologies, it is always preferred for the risk assessment tool to take into consideration the feedback from the security experts. OCTAVE lacks to deliver this.

Microsoft Threat Modeling Tool 2016 [9]
The Microsoft Threat Modeling Tool (MSTMT) is a part of Microsoft's Software Development Lifecycle suite of products. The tool is utilizes STRIDE assessment to perform the risk assessment.

As explained in section 3.3.1, MSTMT is an application which runs a graphical user interface on which a user can create the high-level map of the network and run the risk assessment on it. The drawing canvas offers a set of stencils (network components, connection type, rules for threat generation, etc.) using which a network topology is drawn. The unique part is that the MSTMT offers a customizable template. As a part of the project, customized MSTMT template was developed especially for vehicular networks.

2.1.6 Risk Assessment and Rating

DREAD model DREAD is a classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat. The DREAD acronym is formed from the first letter of each category below.

DREAD modeling influences the thinking behind setting the risk rating, and is also used directly to sort the risks. The DREAD algorithm, shown below, is used to compute a risk value, which is an average of all five categories.

According to DREAD model,

$$Risk = (Damage + Reproducability + Exploitability + Affectedusers + Discoverability)/5 \quad (1)$$

The calculation always produces a number between 0 and 10; the higher the number, the more serious the risk.

9 Microsoft SDLC Tools: https://www.microsoft.com

EVITA Model

CVSS Model The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

The CVSS allows organizations to prioritize which vulnerabilities to fix first and gauge the impact of the vulnerabilities on their systems. Many organizations use the CVSS, and the National Vulnerability Database provides scores for most known vulnerabilities. According to the NVD, a CVSS base score of 0.0-3.9 is considered "Low" severity; a base CVSS score of 4.0-6.9 is "Medium" severity; and base score of 7.0-10.0 is "High" severity.

OWASP Model The OWASP risk rating methodology is based on a number of different risk assessment methodologies. CVSS and DREAD are two that have contributed to it. However, this methodology is actually adaptable and applicable to most organizations and/or systems. Therefore, after reviewing it on a number of different test cases that have been done in the past, we felt that it would be a beneficial methodology to our project [27].

The OWASP model proposes the assessment on a standard risk model used by OWASP, mentioned in equation 2.

$$\mathtt{Risk} = \mathtt{Likelihood} * \mathtt{Impact} \tag{2}$$

OWASP then uses six steps [10] that include the factors that make up the likelihood and impact of each risk. From there the security analyst is able to combine all 6 steps in order to determine the severity of a particular risk to their system.

- Step 1: Identify Risk
- Step 2: Factors for estimating likelihood
  - Threat Agent Factors
  - Vulnerability Factors
- Step 3: Factors for estimating impact
  - Technical Impact Factors
  - Business Impact Factors
- Step 4: Determining severity of risk
  - Informal Method
  - Repeatable Method
  - Determining Severity
- Step 5: Deciding what to fix
- Step 6: Customizing your risk rating model

In summary, the OWASP model accommodates both technical and business impact factors for estimating the severity of the risk. This makes OWASP of good fit for our case. Further in Chapter 3, we will utilize the risk calculation equation (2) while validating the risk assessment process model.

10 OWASP: https://www.owasp.org/

2.2 FINDINGS

Based on the literature research, there has been many developed threat modeling tools and theoretical models to analyze safety and security risks. But none of them perform the security threat analysis, assess the security risks and register mitigation techniques for Ethernet based vehicular communication networks.

The existing literature shows that there have been attempts to develop modeling tools, experimental analysis and some probabilistic models for security of cyber-physical systems but none amongst the available tools provide a risk estimation for the topology of a network model.

Some guidelines like the TARA method [35] and SAE J3061 [54] guidebook provide high-level principles for designing security-aware systems, however there is a need to have a simple yet effective process model which could help the estimation of cyber risks for a vehicular network model.

Threat modeling methodologies like STRIDE [52] are well used with Microsoft Threat Modeling tool; risk modeling tools like CORAS [34], SESAR SecRAM. There are some defense modeling tools built on CAD, UML and attack trees [26, 13, 30]. Apart from this, there are some probabilistic and social engineering driven approaches as well [53, 15, 24]. Table 2.3 describes the summary of the relevant domains of research literature available which have inspired the thesis project.

2.3 CONCLUSION

In conclusion, the future vehicles with advanced driver assistance systems and driver-less capabilities need a faster communication backbone, and hence need an Ethernet based network infrastructure. To have better estimations of security risks in the Ethernet based network topologies in vehicles, we need a customized risk assessment tool. We analyzed the available tools for security threat assessment, risk estimations and defense modeling but realized that the tools are either generic or do not solve the problem for vehicular networks. In the next Chapter (Chapter 3, we will solve this by utilizing the available tools and methodologies to building a customized process for assessing the security risks in a vehicular network.

3 DESIGN AND DEVELOPMENT OF DAAM RISK ASSESSMENT PROCESS MODEL

In previous chapter, we explained how the available tools for risk assessment lack the specificity for vehicular Ethernet networks. We discussed how Ethernet based vehicular networks are different than the indigenous LAN networks; and that a customized risk assessment process, which could identify the threats and risks in a given network topology would be of a great use. In Chapter 2, we also discussed relevant tools (Table 2.3) that are used in industries and can be potentially customized for the vehicular industry (in reference to our scope).

In Chapter 2, we discussed how Microsoft threat modeling tool [43] can be enhanced for the vehicular domain. In this chapter, we will take a closer look at the possible opportunities to customize the tool. Later in the sections, we will also discuss designing a security risk assessment tool which will be utilized in Chapter 4 to capture the security threats, record risk estimation and rationale of the security expert.

3.1 OVERVIEW

By end of the chapter, we will be building a four step security risk assessment model. As mentioned in Figure 3.1, the four steps involve a. Drawing the topology, b. Assessing threats, c. Analyzing risks, and d. Mitigating risks steps, and hence is called DAAM security risk assessment model. Starting with drawing the topology of the network, every step of the process will solve a part of the risk assessment process. In step two, the topology would be run through the STRIDE [52] assessment and then use the specially designed Adapted Security Risk Analysis Tool (ASRAT) to decide the rational driven risk priorities. The fourth step is about making decisions to possibly mitigate the risks; The ASRAT would be utilized for logging the mitigation decisions and rationale from the security experts.

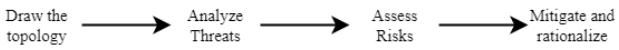


Figure 3.1: Overview of the four-steps DAAM process model

.

3.2 ASSUMPTIONS

Scope of the research

As mentioned earlier in section 1.3, the scope of the research is to design a structured process for performing security risk assessment of vehicular networks. After we define a tailored assessment model, we will validate it by running a hypothetical vehicular network topology through the steps.

Topology for Experiment

In Chapter 4, the designed process model is run through an experimental study for validation. In network topology of the vehicular network is based on the understanding from the functional requirements of a Scania truck (see Table 4.1), however, for simplicity of demonstration and security of Scania's IPR (Intellectual Property Rights), the topology has been kept simplified and hypothetical. It is hence assumed that the considered topology is not the real arrangement of network modules in a Scania truck; any similarity would be considered to be a mere coincidence.

Functional Domains

A commercially produced truck has more than 10 functional domains. Some examples of functional domains are infotainment subsystem, telemetry, powertrain subsystem, software updates subsystems, HMI subsystems, ADAS etc. Deep understanding of these subsystems can help in building the custom template for MS Threat Modeling Tool. However, due to limited time and resources, it was not possible to understand all the functional domains of the vehicle. For the scope of this research, a high level understanding of the functional requirements of the infotainment subsystem and the ADAS was taken into study.

Source of knowledge and ground truth

The basis of most of the knowledge in the research is based on the literature study process as explained earlier in section 1.5. Apart from the literature available through Google Scholar[1], numerous Scania internal documents were referred and reviews/interviews of security experts were taken into consideration. The feedback and knowledge from the domain experts in the industry were considered to be ground truth.

3.3 DESIGN OF THE 4 STEP ITERATIVE PROCESS

COMPOSITE TOOLS

As mentioned earlier in this chapter, the DAAM security risk assessment model is a four step process and makes use of a template for MS Threat Modeling Tool [43, 56] tailored for vehicular networks and a security risk assessment tool, built on Microsoft Excel (see section 1.6). The underlying sections explain the details about each of these tools, the customization and rationale in detail.

3.3.1 Adapted Microsoft threat modeling template

Microsoft's Security Development Lifecycle (SDL) offers a suite of products which support the assurance of security in software development processes to ensure a reduction in number and severity of vulnerabilities in software. Threat modeling is the core element of MS SDL. Microsoft Threat Modeling tool is one of the software applications in the same suite offered by Microsoft Inc.

1 Google Scholar: https://scholar.google.com/

The Microsoft Threat Modeling Tool (TMT) 2016 is designed to guide product teams in a software development organization through the threat modeling process. TMT functionality includes:

- An easy drawing environment.
- Automatic threat generation using the STRIDE (see Table 2.4) per interaction approach.
- Define your own template for threat modeling
- An option for user-defined threats to be added.

The Microsoft Threat Modeling Tool (TMT) can be utilized to graphically identify processes and data flows that comprise an application or service.

Why MS Threat modeling tool

There are two reasons why MSTMT is the most suitable choice of tool that can be used for our risk assessment process model.

1. *STRIDE Assessment:* The STRIDE approach [52] is an effective way to highlight and categorize threats specially for a software architecture which can be modeled using data flow diagrams. STRIDE classifies threats in accordance with their categories. By using these categories of threats, one has the ability to create a security strategy for a particular system in order to have planned responses and mitigations to threats or attacks. Hence STRIDE is well received specially for the industries in the domain of software and computer networks.
2. *Templates:* The templates can be seen as a set of logic rules on which the MS Threat Modeling tool's application works. Templates are the core on which the output of MSTM depends. As described in Figure 3.2, there are different categories of customizations that have been made in templates. The template permits the creation of specific automotive threat models which support:
   - creation of custom process and data stores related to ECUs, network switches, routers, etc.
   - *External Interactors* tailored to an automotive system
   - Custom *data flows* and *trust boundaries*. These trust boundaries take care of vehicle-to-vehicle (V2V and V2I) networks
   - Custom *Threat types* and *Threat categories* that follow the STRIDE classification, based on known and potential threats to the connected cars' components.
   - Tailored threat property creation including declared priority orders (high, medium and low)

Tailored Template

We have tailored a customized template for MS Threat Modeling Tool 2016 for vehicular networks. The customization has been imparted primarily in three aspects (see Figure 3.2), as under:

- **Components**
  e.g. ECUs, Network Switches, Routers, Firewall..

- **Processing**
  e.g. Data Flow like Ethernet, Bluetooth, IOCTL..
- **Threat properties**
  e.g. rules to generate custom threats, priority..

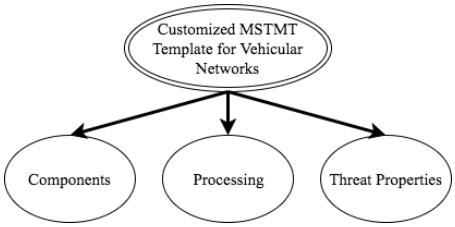


Figure 3.2: Categories of changes that have been imparted to the adapted version of threat modeling tool

.

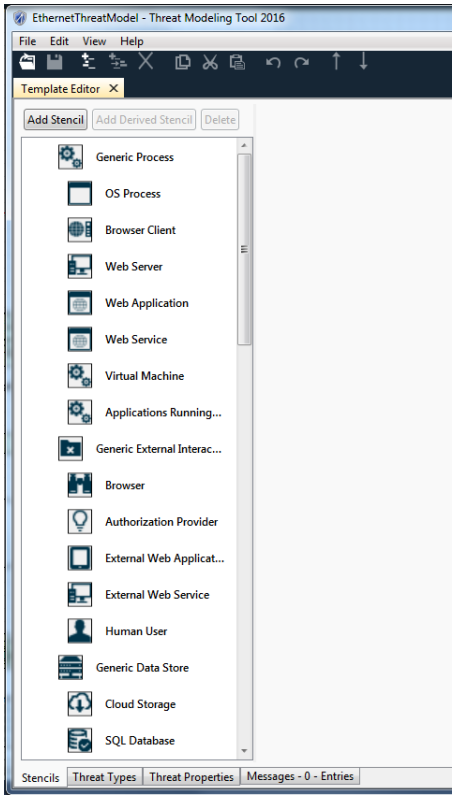


Figure 3.3: Stencils : MSTMT

.

A. Components

The MS Threat Modeling tool provides a canvas and a stencil f components (as shown in Figure 3.3. Some examples of components are ECUs, network routers, databases, etc. These components are grouped according to their nature of capability, e.g. process related components, storage related components, interaction based groups, etc.

These components can be used to draw a representative topology of of the vehicle's communication network. Every component in the stencil has

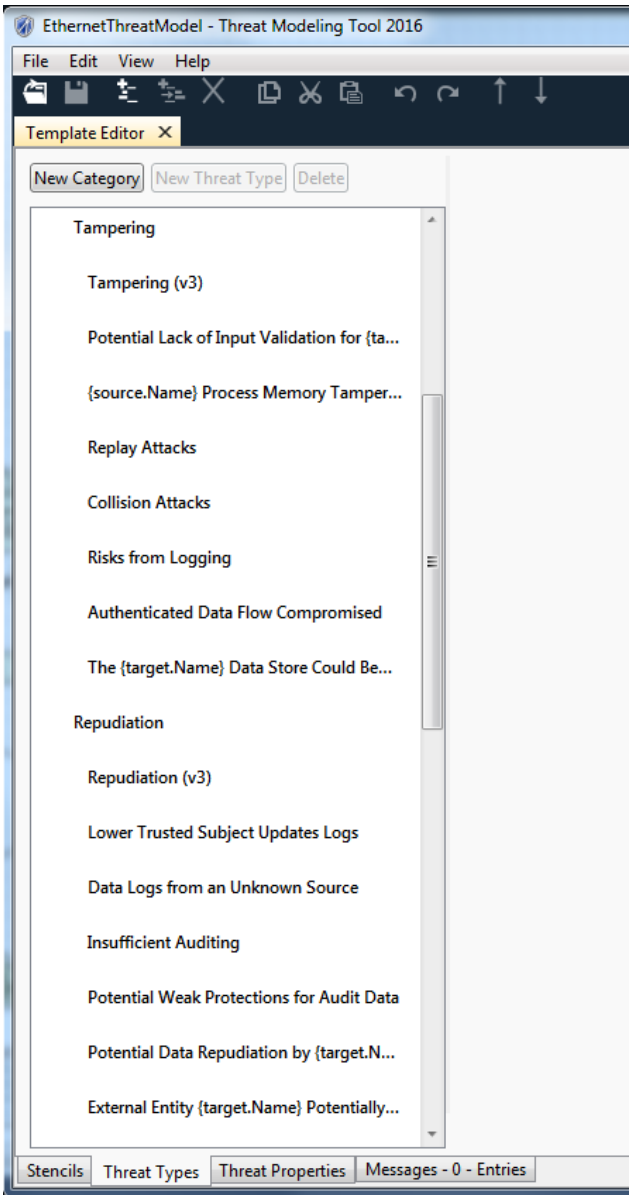


Figure 3.4: Threat types

.

its own definitions and properties. The rules for generation of threats are based on these properties.

The list of components is extendable by design and hence, it is possible to create and use customized components on the stencils. For the scope of this thesis project, we have created some components for vehicular networks and have also used generic components in the topology design (refer Figure 4.3).

In Chapter 4, we use the developed customized MSTMT template to implement a representative network topology and run an experiment for performing security risk assessment to validate the DAAM process model.

B. Processing

The components of the stencil which relate to or help in the logic of threat generations are kept under this category. As mentioned earlier, MSTMT

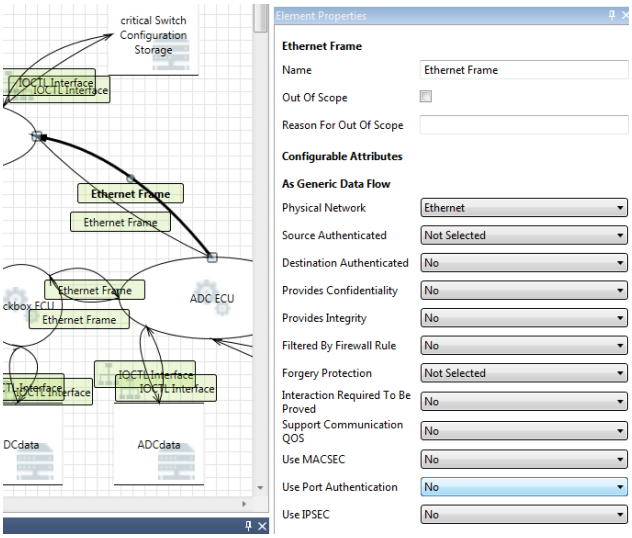


Figure 3.5: Element properties

.

offers a canvas which we use to draw a representative topology of the vehicular communication network.

The customization on processing methods on the template can be explained under three categories:

- **Data Flows**: The type of connection that is established between the components in a network
- **Trust Boundaries**: Trust boundaries show any location where the level of trust changes. For example, When a Bluetooth connection is established between the vehicles Infotainment system and users mobile phone, then the data flows across trust boundaries.
- **Threat Types:** The threat types and Categories that follow the STRIDE classification. The threat types are based on known and potential threats to the connected components in the vehicular network.

C. Threat Properties

As depicted in Figure 3.6, the threat properties can be configured in the third tab of the threat modeling template. This is an essential part of setting the threat generation engine with the right decision making logic. The threat properties allow adding detailed information to the threats. For example, the title of a threat, description or even list of values, priority, etc. can be defined as a part of threat properties. Properties can be of two types - descriptive texts or lists. For text, it will be possible to insert a specific content for each Threat. If you decide to create a List Property, then you will be requested to define the potential values, and you will be able to select the specific default value for each Threat using a drop-down.

In the scope of the project, a default threat model template was updated with new fundamental values and granular details to make it suitable for the vehicular domain. Depending on the generic connection types (refer data-flow in the previous section), configurations on the heads of priority, methods, rules, and mitigation techniques were amended. Inputs from Security experts at Scania were of great importance for this step. Based on the feedback and learning from previous threat modeling runs at Scania, the advice of the security experts were utilized to create the threat properties.

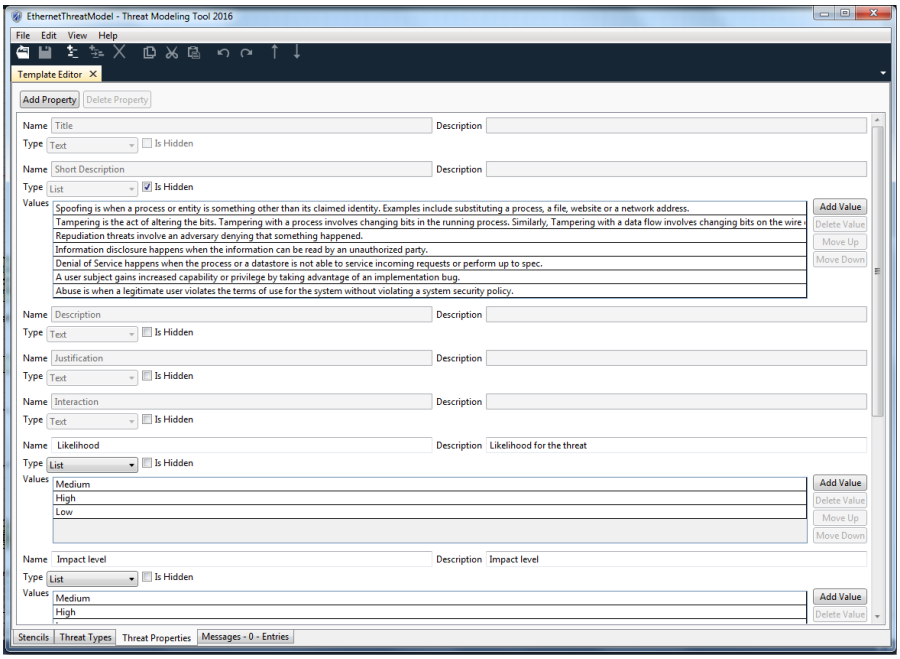


Figure 3.6: Third tab of the threat modeling template - Threat Properties

.

- **Priority**: The priority of every risk that is generated by the threat modeling tool based on the vulnerabilities on the attack surfaces
- **Methods**: The description of the attack methods that potentially exploit the identified threats
- **Rules of occurrence**: The systematic rule descriptions for the modeling tool to generate threats when run
- **Mitigations**: Impart mitigation techniques and recommendations for the known generated list of threats

Recommendations

Though the default MSTMT template comes with a set of default security recommendations and controls, it is a good practice to have additional suggestions on controls added to the list. A noteworthy advice from the security experts is that an organization's decisions on the gravity of the mitigation of the security may vary, depending upon their evaluations of risk to the assets. However, it is recommended for the practitioners and security architects to define preventive controls, mitigation categories, corrective measures and accepted levels of residual risks for the assessments. Some of the recommended practices are as under[2]:

- Recommended Preventive Controls – security controls that are recommended by the organization for preventing the threat.
- Recommended Detective Controls – security controls that are recommended by the organization for detecting the occurrence the threat.
- Recommended Corrective Controls – security controls that are recommended by the organization for addressing the threat as soon as it occurs.

2 Secure SDLC: https://simoneonsecurity.com

- Recommended Recovery Controls – security controls that are recommended by the organization for recovering from the consequences of the threat.
- Mitigation Type – Accept, Avoid, Mitigate, Transfer – the usual four mitigation types.
- Preventive Controls – security controls that have been selected for the application, to prevent the threat.
- Detective Controls – security controls that have been selected for the application, to detect the occurrence the threat.
- Corrective Controls – security controls that have been selected for the application, to address the threat as soon as it occurs.
- Recovery Controls – security controls that have been selected for the application, to recover from the consequences of the threat.
- Description of Residual Risk – The residual risks are those threat scenarios which cannot be addressed by adopting the previous mitigations. This is needed by stakeholders to understand the residual risk of the solution.
- Residual Risk Evaluation – qualitative analysis of the residual risks.

3.3.2 Adapted security risk analysis tool

We have seen in the previous section how the Microsoft Threat Modeling Tool 2016 can be used to generate a list of possible threats for the given network topology. When run, the MS threat modeling tool makes a report. The report is an HTML5 based document which summarizes the possible threats, their description, mitigation, etc. based on the rules and configurations in the adapted Microsoft Threat Modeling Tool Template (see section 3.3.1). A significant drawback of the report is its inability to record the input from the user. The static HTML5 document does not let the security architect (or user) make a log of his assessment, prior and case-to-case that a user cannot write his rationale, recommendations, priority decisions and basis. This limits the MS Threat modeling tool's threat analysis report from offering reliable storage and transfer of security analysis knowledge. The adapted security risk analysis tool solves this problem and supports the risk analysis of the threats generated by the MS Threat modeling tool.

The adapted security risk analysis tool (ASRAT) is a simple and minimalist database model, built on Microsoft Excel, which enables the security analyst to use the results of the threat assessment performed in the previous step and conduct a structured risk analysis. With ASRAT, the security analyst can take a structures look at the assets, threat category (STRIDE), risks and most importantly, log one's rationale behind the decisions for the priority, likelihood and suggested mitigations if any. Figure 3.7 depicts a snapshot of the three parts of the ASRAT.

Inspired from SESAR Secram [50] and based on the usability, features of being scalable (refer section 5.2) and feedback from the security experts at Scania, the ASRAT tool was defined with a particular structure. In this section, we will explain the design of the tool and the rationale behind the design.

Figure 3.7 describes the SRAT tool. The SRAT tool is built on MS Excel [3] and has some inbuilt macros which simplify the usability further. As

3 Microsoft Excel: https://products.office.com/en/excel

mentioned earlier, the main idea behind development of SRAT is to have a simple yet powerful way of logging the risk assessments and the security analyst's rationale behind the ratings.

Asset Declaration Table	**Asset ID**	
	Interaction	
	Asset Association	Asset Name · Type/Description

A: First tab of ASRAT: Assets declarations

Risk Calculation Table	**Associated to Asset ID**	
	Threat	Threat ID · Threat Type · S,T,R,I,D or E · Description · Justification · Attack Method
	Impact	Impact Level · Rationale
	Likelihood	0-Unknown · 1(Unlikely)-5(Highly Likely)
	Risk	Risk Score(Impact X) · Priority Level · Justification

B: Second tab of ASRAT: Impact, likelihood and risk calculations

Mitigation Table	**Threat**	Threat ID · Category
	Mitigation	Recommendation · Rationale for Recommendation · Description · Rationale for Description
	Status	Mitigated/Not Mitigated/Does not need Mitigation · Rationale for Mitigation

C: Third tab of ASRAT: Mitigation

Figure 3.7: The Adapted Security Risk Analysis Tool (ASRAT): The structure of this tool is built in MS Excel application. There are three tabs in this tool (A,B and C) as described above.

First tab: Asset declaration

Asset ID: An identifier given to the subjected asset.

Interaction: The mode of interaction between two nodes of the network. For example Bluetooth, Ethernet, etc.

Asset Association: Identified asset that the threat is concerned to. Examples of threats can be the configuration data of network switch.

Second tab: Impact, likelihood and risk calculations

Asset ID: An identifier given to the subjected asset. This is same as in the previous tab.

Threat: The threat, as generated by the MS Threat modeling tool

Impact: To calculate the impact of the threat, we use the impact assessment matrics as represented in Figure 3.8. The metrics help the user to grade the amount of impact arising from a threat.

Likelihood: The anticipated likelihood of the threat and its rationale. The SRAT tool comes with a reference matrix for calculating the likelihood of occurrence of a threat. Based on multiple interviews with security experts and inspired by the SESAR SecRAM [50] risk assessment model, the matrix suggests the likelihood to be dependent on primarily two parameters - attacker's skill level and physical access to the network of the vehicle. As described in Figure 3.9, the likelihood of occurrence of a situation can be objectively seen as high, medium or low.

Risk: The risk score is calculated based on the values of likelihood and impact. The formulae for calculating risk is well is also practised in other risk assessment models (see Equation 2 and [50]) with an

exception that risk is always high when there is threat to human lives, i.e, impact is fatalities in the impact reference matrix (see Fig 3.8).

Listing 1: Algorithm to calculate risk score

```
IF (Impact.Personnel is Fatalities) OR (Impact *
    Likelihood) >= 15
    return Risk is HIGH
ELSE IF (Impact * Likelihood) is less than 5
    return Risk is LOW
ELSE IF (Impact * Likelihood) is more than 5 and (Impact
     * Likelihood) is less than 15
    return Risk is MEDIUM
```

		Impact Score				
		1 No Impact/NA	2 Minor	3 Severe	4 Critical	5 Catastrophic
Domain	Personnel	No Injuries	Minor Injuries	Severe Injuries	Multiple Severe Injuries	Fatalities
	Performance	No loss	Minor system quality loss	Severe Quality loss; System partially inoperable	Major Quality Loss; Some Systems Inoperable	Major Quality Loss; Multiple Major Systems Inoperable
	Branding	No Impact	Minor Complaints	Complaints and local attention	National Attention	Govt and international attention
	Economic	No Effect	Minor loss of income	Large loss of income	Serious loss of income	Bankruptcy or total loss of all income

Figure 3.8: Reference matrix to calculate the impact score (None/Minor/Severe/-Critical/Catastrophic). This matrix is used by the SRAT tool for security risk assessment for vehicular networks.

.

Likelihood		Attacker's skillset		
		Low	Medium	High
Physical Access	Required	**High** An attacker with low skill level is able to make use of the threat when he has physical access, this means that the threat complexity is low and it is highly likey for attackers to exploit this threat.	**Med** An attacker with medium skill level is able to make use of the threat with physical access, this means that the likelihood of this threat being exploited by any attacker is medium.	**Low** An highly skilled attacker can make use of the threat only when he has physical access to the network, this means that the threat is difficult to exploit and the likelihood is low
	Not Require	**High** An attacker with low skill level is able to make use of the threat remotely, this means that it is easy for any attacker to make use of the threat	**High** An attacker with medium skill level is able to make use of the threat remotely, this means that the threat is easy to exploit and the likelihood is high.	**Med** An attacker with high skillset is able to make use of the threat remotely, this means that the threat is of moderate complexity. Hence the likelihood of occurence is medium.

Figure 3.9: Reference matrix to calculate the likelihood of a threat. This likelihood model is used in SRAT tool for assessments of security risks for vehicular networks.

.

Third tab: Mitigation

Threat: The threat, as generated by the MS Threat modeling tool. This is the same as previous tab.

Mitigation: Mitigation techniques as mentioned by the security experts and the rationale.

Status: The status of the threat with reference to its identified mitigation. The rationale of the status also needs to be mentioned.

3.4 DEVELOPMENT OF DAAM SECURITY RISK ASSESSMENT MODEL

In Chapter 2 we looked at the state of the art of threat modeling techniques. In this chapter, we will propose the Draw-Assess-Analyze-Mitigate (DAAM) process model for security risk assessment of Ethernet-based vehicular networks. The DAAM process model performs security risk assessment on the designed topology of the network components.

As mentioned earlier in this chapter, the DAAM model is a composite of two tools that constitute security threat generation on the model and then risk assessment and rationale recording on the same. In this chapter, we will describe the process in further details.

Later in Chapter 4, we will use the first version of the proposed composite model on some of the use cases of a Scania truck which is are potential candidates to apply Ethernet in its network. The experiment will help us understand how the proposed process model works and the feedback from security experts at Scania will help us improve the model further. The improved model will be explained in section 4.4.

Design of the model

The DAAM process model is an acronym for four fundamental sub-processes to perform structured security risk analysis of a given network model. DAAM stands for the four steps, Draw-Assess-Analyze-Mitigate. Figure 3.10 gives an insight of these steps . The process model is a composite of two tools which are specially tailored to meet the requirements of security risk assessment of vehicular networks.

To perform the structured security risk assessment of Ethernet-based vehicular networks, we utilize the MSTMT (Section 3.3.1) and Threat Analysis tool (Section 3.3.2) to build the proposed four step process flow called Draw-Assess-Analyze-Mitigate (DAAM) Model.

Table 3.1 describes the four steps of the DAAM process model and also mentions the tools and techniques used for each step.

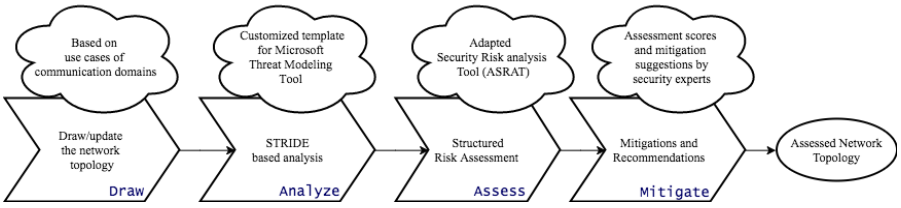


Figure 3.10: Four step DAAM process model for risk assessment (Ver 1.0)

.

3.5 DISCUSSION

Security is more of a qualitative than a quantitative concept. It has always been a challenge for security experts to quantify the level of security of a

Step No.	Name	Description	Tool Used	Techniques/Skills Involved
1	Draw	Based on functional requirements of the network, draw the topology diagram on MSTMT	MS Threat Modeling Tool	Human, Tool
2	Analyze	Using the customized template for assessing security of vehicular networks, run the assessment on MSTMT	Custom Template for MSTMT	Tool
3	Assess	Use the developed adapted security risk analysis tool (ASRAT) to capture the output of STEP 2	ASRAT Tool	Human
4	Mitigate	Based on feedback from Security experts decide the mitigations for the security threats generated in STEP 3 and use the ASRAT tool to capture the rationale	Advises from Security Experts	Human, Tool

Table 3.1: Four step DAAM process model

system. It is a common conception among security analysts that the efficacy of a security risk assessment depends on the knowledge and skills of the researcher who is analyzing the system. It is possible that only one round of security risk assessment is good enough to harden the system; it is also a common practice in the industry for the teams to perform multiple rounds of threat assessment and mitigation. In the next chapter, we present validation experiments to verify the effectiveness of the DAAM process model.

As discussed in previous sections, the DAAM process model offers a structured way of analyzing the risks of a system and importantly, the tool enables the user to keep a record of the rationale behind every risk scoring and assessment decisions. We will see in section 5.2 how this feature can empower future risk analysts to share knowledge and improve assessments with time.

As seen in Table 3.1, the DAAM process model involves multiple techniques/tools for each step of Draw, Assess, Analyze or Mitigate. In the first step, primarily the MSTMT canvas is utilized by the user (security analyst) to draw the topology based on the functional requirements of the network. Using the logic in the custom template, he can then generate the threats on this network topology. One significant advantage at this step is that the user can be flexible rearranging his network components or redrawing the topology by adding/removing structures from the stencil (see 3.3). This not only saves him time but also allows him the flexibility to minimize the threats. An example could be that depending upon the network topology, thoughtful use of trust boundaries can help in reducing some of the threats. Similarly, step 3 (Analyze) and step 4 (Mitigate) involves the utilization of human experience and knowledge. According to expert interviews, typically in industries, the teams prefer to perform the mitigation step in groups, i.e., more than one person - generally a group of two to three subject matter experts work together.

3.6 SUMMARY

In this chapter, we proposed an approach to perform the security risk assessment of vehicular Ethernet network in a structured way. We termed the four step process as DAAM (Draw-Analyze-Assess-Mitigate) process model for security risk assessment. In this chapter, we discussed each of these four steps in detail. The fact that the DAAM process model is a composition of two tools and makes use of human experience and knowledge for assessment makes it powerful. Added to that, a structured storage mechanism to keep record of the rationale behind design decisions make the DAAM model a great choice for industrial practices. In the next chapter, we will use the DAAM process model to perform security risk assessment of vehicular Ethernet network for Scania trucks to validate the efficacy. We will also take inputs from security experts in order to bolster the tool.

4 VALIDATION OF THE DAAM SECURITY RISK ASSESSMENT MODEL

4.1 OVERVIEW

In previous chapters, we understood how the vehicular industry is moving towards the next paradigm of driving experiences which involves increased usage of sensory networks and IT. With advanced driver assistance systems, in the future, the vehicles will have improved driving experience, and in a longer term, they will even have fully autonomous driving and decision-making capabilities. The research for light motor vehicles like cars have shown good progress in the last few years, however, because of higher potentials of impact, the for heavy commercial vehicles (e.g., trucks) need to be extra sure about the anticipation of potential risks before this transition. In the context of this project, we focus on heavy-duty vehicles.

In Chapter 3, we proposed the DAAM security risk assessment process model. The experiment in this chapter aims to validate the DAAM process model by performing security risk analysis for an Ethernet-based communication network of a Scania truck. To start with, we try to understand a high-level functional requirement of the vehicle's subsystems. This knowledge helps us to perform the first step of the process, that is to draw the network topology. In the later sections, we discuss the execution of the next steps of the assessment - analyze, assess and mitigate. Following the test run, we introspect the model and discuss possible improvements.

4.2 EXPERIMENT

4.2.1 Assumptions

While conducting the experimental validation of the iterative-DAAM model (Figure 4.4), the following assumptions have been made:

- **Topology**
  Based on our the knowledge about the subsystems of a Scania truck, in the section 4.2.3, we draw a high-level network topology of the communication network. For simplification, generality and protection of intellectual property rights, this network design in section 4.2.3 is a simplified and hypothetical version (refer Figure 4.3). It is also assumed that no CAN-based communication channels would be present in the network infrastructure and Ethernet constitutes dominantly.

  It is also declared that the referred topology, not the exact topology that is implemented on a Scania trucks and is used solely for the demonstration of validation experiments for the DAAM risk assessment process model (refer Figure 4.4) process model.

- **Sub-systems of a truck**
  Like other heavy-duty vehicles, Scania's truck is also a complex system to understand, given the limited period for the master thesis project.

It was therefore decided that a high-level understanding of the functional requirements of subsystems like infotainment systems and advanced driver assistance systems (ADAS) would help in drawing the topology of the communication network (with assumptions). However, since the purpose of this chapter is to validate the process model, the hypothetical topology was seen as a great way to conduct the experiment. Since this developed tools (as a part of DAAM) are scalable, therefore it is highly likely that a user can use the same process for a complex network topology too.

- **Number of iterations**
  For the experiment, we use the DAAM process model that has been proposed in Chapter 3. Following the design, the security risk analysis was run for only one iteration and the results were shared with the security experts. In retrospect, it was observed that an iterative execution of DAAM may improve the results of assessment, however due to time limitations, only one iteration could be performed.

4.2.2 Functional requirements of a Scania truck

Sub Question # 2

What are the functional requirements of heavy commercial vehicles subsystems?

To answer this question, a couple of sources of information has been referenced. Primarily, the Scania-internal library was referenced; the engineering design documents, functional requirements documentation, use case documentation and network architecture documents gave a genuine understanding of the functional requirements. Apart from the Scania internal data, resources on the public Internet were referred, and discussions with technical architects were utilized to build the understanding of the functional domains of the HCV.

As depicted in Figure 4.1, there are six functional domains in a truck. However, this classification of the division of domains can often be relevant and different models of trucks can have an even granular division of domains. For example, for some trucks may also have a functional domain called "Driver Comfort" which consists of infotainment subsystem and auxiliary functions which are secondary to the drive requirements.

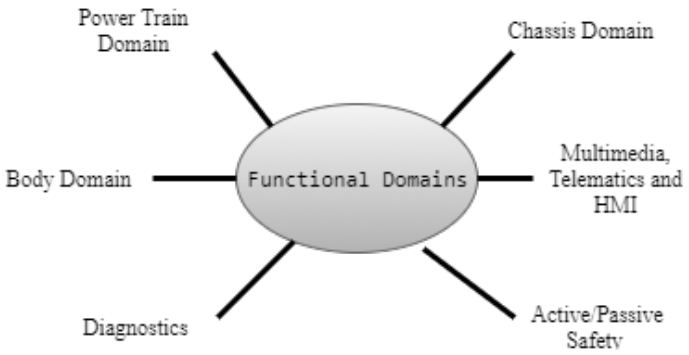


Figure 4.1: Functional domains of a Scania truck

The functional domains of the truck in principle are clusters of ECUs and dependent sensors which are responsible for taking care of a more significant and collective task. These ECUs and their dependent data creation endpoints can be considered as nodes in the network. Since safety is deemed to be the fundamental requirement (prime importance), each node can be

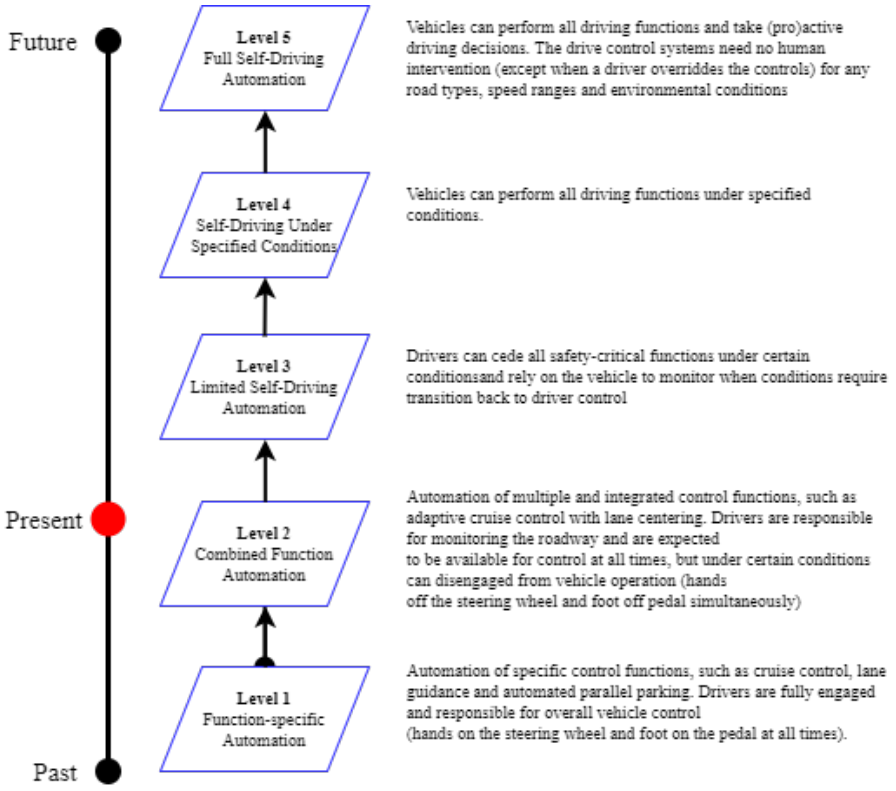


Figure 4.2: Levels of vehicle automation, features[3] and time line depicting present generation of automotive autonomy

further categorized as safety critical or not. Table 4.1 summarizes the information about different network nodes and them being safety critical or not.

Understanding the functional requirements of the vehicular network components also enables optimal physical arrangement of the nodes (can be ECUs) in the network and deciding the kind of communication channel (Bluetooth, radio, Ethernet wire, etc) that are required between the components and information required to group nodes into trust boundaries. These information pointers help the security architect draw a more realistic network topology, like the one drawn in Figure 4.3.

A defined network topology is the foundation stone for the next rounds of security risk assessments. We proposed a security risk assessment process model in Chapter 3 and in the later sections, we will be validating the DAAM model (Fig. 4.4) based on our understanding of the functional requirements of the network components, as described in Table 4.1.

4.2.3 Draw the network topology

Based on the functional requirements of the network we designed the network topology. The network topology is drawn on the MS threat modeling tool canvas using the tailored template. The customized template offers a custom stencil for vehicular networks (see Chapter 3). The stencil is composed of network elements (or network nodes), a suite of connection types and subnet grouping elements like trust-boundary tools.

As mentioned in Figure 4.3, the network topology has a central gate which has two switches connected to itself which in turn serve a number of ECUs

Component	Functionality	Safety Critical
Remote Server	Remote connection to the Scania servers, software updates, fleet management (FMS)	Yes
Diagnostic Tester	Diagnostic tester typically has physical access to the OBD port of the vehicle. Diagnostic testing is done at the service station, by a trained and reliable professional, generally, through data read (also data write/software update) access over a wired connection or through service stations wireless connection	No
Infotainment ECU	Provides information and entertainment functions. Comprises of map data, speaker & sound management, external connections to users devices over wired/wireless protocols	No
TCM	Transmission Control Module (TCM) controls electronic transmission using data from sensors and the Electronic/Engine Control Module (ECM) to determine when and how to change gears.	Yes
HMI ECU	Human Machine Interface is responsible for the visualization of critical running information to the driver's dashboard and controls to functionalities that are available on the steering wheel (headlights, AUS controls, wiper, etc.)	No
Diagnosis ECU	The diagnosis ECU provides the functionality of reading the diagnostics data from the ECUs. This ECU is different from the Diagnostic tester ECU because it does not have write permissions.	No
SDM	Sensing and Diagnostic Module (SDM) is an inflatable restraint sensing and diagnostic module which controls airbags and seat belt pre-tensions	Yes
Engine ECU	Also called ECM (Engine Control Module) Controls the engine using information from sensors to determine the amount of fuel, ignition timing, and other engine parameters	Yes
Breaking ECU	Controls the Anti-lock Brake System (ABS) pump motor and valves, preventing brakes from locking up and skidding by regulating hydraulic pressure	Yes
Steering ECU	Steering ECU provides steering support functionalities to the drive and its control	Yes
Black-box ECU	Black box ECU is responsible for recording the log of all the activity and process decisions from the ECU	No
ADC ECU	The ADAS Domain Controller (ADC) ECU takes care of the fusion of data from the sensors and decisions from its processing	Yes
Sensor data and fusion	Most of the real-time drive decisions taken by the autonomous vehicle is dependent on the fusion of data from the sensors	Yes

Table 4.1: A snapshot of the ECUs used in a vehicle with autonomous features and their functional requirements

each. As the prime objective of the vehicle is to perform safe transportation (move), the switches are named to be critical or not critical, depending upon its application for the movement. ECUs like the engine, braking, steering, and ADC make it possible for the vehicle to perform its purpose, so they fall under the critical switch. Infotainment, HMI and diagnosis ECUs go on the non-critical switch. The network nodes also have an asset (data store/-

configuration) and are connected to the switch or another network node through communication channels like Ethernet, IOCTL, Bluetooth, etc.

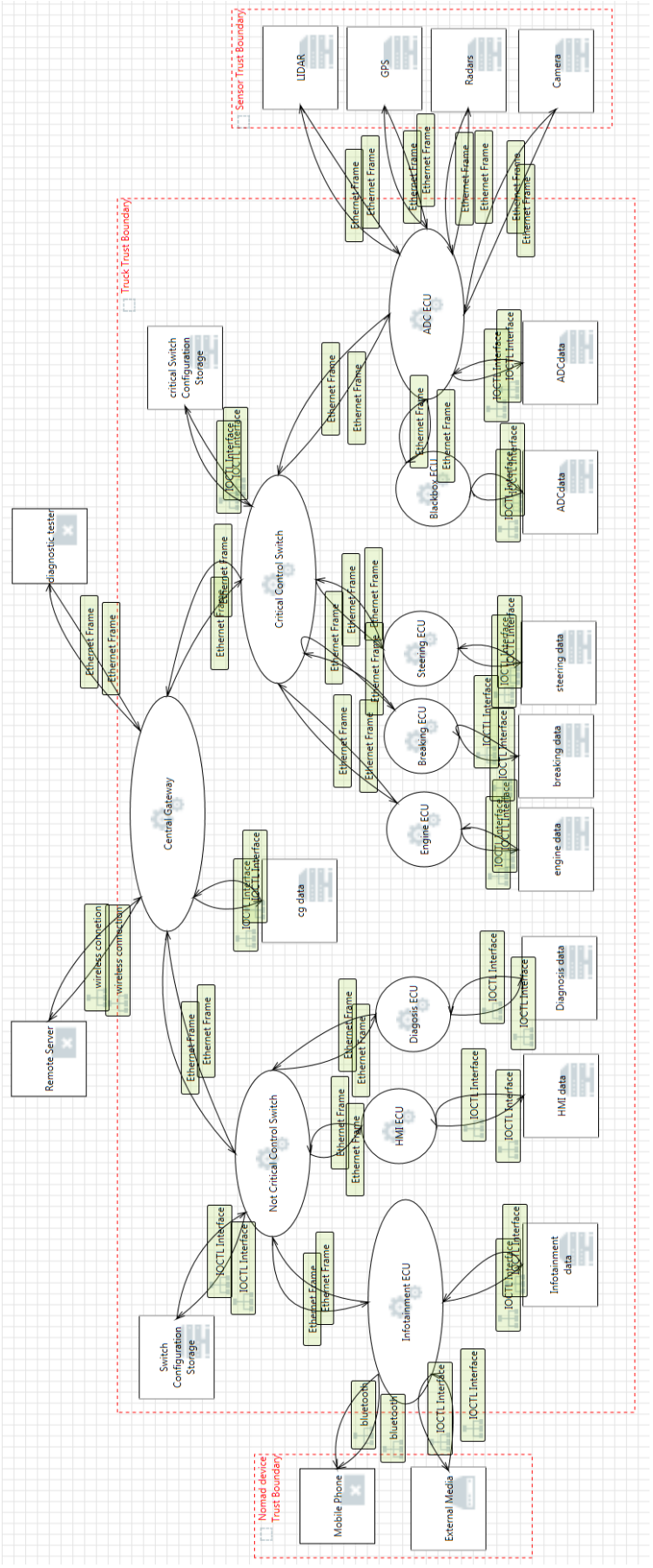


Figure 4.3: Network topology drawn based on the functional requirements of Scanias truck

4.2.4 Assess the security threats

The analysis of security threats is done using MS threat modeling tool's threat generation engine. The threat generation can be triggered through the graphical user interface in the MSTMT. The tool generates threats using STRIDE methodology. The threat generation is driven by rules that are described in the MSTMT template. Since these rules are a set of instructions with the logic for the inclusion, exclusion, and mitigation of the threat, we will henceforth call it a policy.

A typical policy in a MSTMT template has six parts to it - title, rules for inclusion, rules for exclusion, description, recommendation and mitigation techniques (if applicable). We have created policies for the tailored template for vehicular networks. In the example below, a sample policy for threat generation is mentioned. The policy uses hooks like source, target, flow, [Generic Process] to identify the network elements and use the language to construct rules.

Listing 2: An example of MS threat modeling tool's tailored template for the vehicular networks

```
Threat Class: Spoofing

Title:
    Spoofing the {source.Name} Process

Include:
    source is [Generic Process] and (target is [Generic Process]
        or target is [Generic Data Store]) and (flow crosses [
        Generic Trust Line Boundary] or flow crosses [Generic
        Trust Border Boundary])

Exclude:
    flow.[Source Authenticated] is 'Yes' or (flow is [Ethernet
        Frame] and (flow.[Use MACSEC] is 'Yes' or flow.[Use IPSEC
        ] is 'Yes'))

Description:
    {source.Name} may be spoofed by an attacker and this may lead
         to unauthorized access to {target.Name}.

Recommendation:
    Consider using a standard authentication mechanism to
        identify the source process.

Mitigate by:
    flow.[Source Authenticated] is 'Yes' or (flow is [Ethernet
        Frame] and (flow.[Use MACSEC] is 'Yes' or flow.[Use IPSEC
        ] is 'Yes'))
```

Listing 3: Another example for a threat that involves tampering of memory data is given below. Also Figure **??** shows how does this threat look like in the output of MSTMT HTML listing.

```
Threat Class: Tampering

Title:
    {source.Name} Process Memory Tampered
```

```
Include:
    source is [Generic Process] and target is [Generic Process]
        and target.[Code Type] is 'Unmanaged'

Exclude:
    (source.[Isolation Level] is 'Sandbox' or source.[Isolation
        Level] is 'AppContainer') and  (target.[Isolation Level]
        is 'Sandbox' or target.[Isolation Level] is 'AppContainer
        ')

Description:
    If {source.Name} is given access to memory, such as shared
        memory or pointers, or is given the ability to control
        what {target.Name} executes (for example, passing back a
        function pointer.), then {source.Name} can tamper with {
        target.Name}. Consider if the function could work with
        less access to memory, such as passing data rather than
        pointers. Copy in data provided, and then validate it.

Recommendation:
    Use domain separation feature on the run-time system (OS or
        RTOS) on both the {source.Name} and {target.Name} in
        order to protect process memory from being directly
        access by external processes.

Mitigate by:
    (source.[Isolation Level] is 'Sandbox' or source.[Isolation
        Level] is 'AppContainer') and  (target.[Isolation Level]
        is 'Sandbox' or target.[Isolation Level] is 'AppContainer
        ')
```

The output of the analysis is an HTML file which has a list of threats, each one with a descriptive text and a snapshot of the interaction between the nodes under consideration. The formatting of this output is controlled by the MSTMT but new threats, rules for their generation, their description, suggested mitigation and priority can be defined in the MSTMT template.

On running the threat generation logic for our topology design (Figure 4.3), about 186 threats were generated by the MSTMT. Some of the examples of the threats generated by the tool is given in Appendix A.

4.2.5 Asses the security risks and costs

In this step, we use the customized tool for security risk assessment that is developed specially for the DAAM process model. The Adapted security risk analysis tool (ASRAT) as explained in Chapter 3 takes as input the output of step two of the DAAM process model (see Table 3.1) and enables the security analyst to input and record his rationale and contributions. As explained, the first section of risk assessment involves scoring the impact and likelihood of a threat. In the next step, the risk score is calculated. For ASRAT, the risk score is the product of impact level (1 to 5; One being low, five being catastrophic) and likelihood (1 to 3; Low-Med-High). The risk function then is referenced to find the priority of the threat. The risk function is described in Section 3.3.2.

4.2.6 Mitigation and logging

In this step of DAAM risk assessment process, we use the recommendations from the tailored MSTMT template to fix the known threats. The method of grading the threats based on the matrices of the adapted security risk assessment tool helps in developing an ordered list of threats. The security analyst (or the decision maker) can then prioritize the list of risks for their mitigation based on other dependent variables. The other dependent variables could be the complexity of mitigating the risk, cost of mitigation, the time taken to implement the mitigation or even to skip the mitigations.

The advantage of the ASRAT tool is that the user/analyst would be able to log all his choices and rationale into the databases. This information can henceforth be referred in the future if required. When the ASRAT tool was used for a test run, it was observed that the security analysts prefer to have brainstorming sessions with subject matter experts to make decisions on complex risks (medium/high impact); it is equally essential for them to persist the mitigation related choices for future references.

While the users can use custom MSTMT template for threat generation and mitigation suggestions, ASRAT helps the users with a structured way to store the rationale. As we discuss later in section 5.2, these persisted rationale data has the potential to enhance the quality of security risk assessments.

Recommendations from the experiment

This section also answers one of the sub-questions of the project, as mentioned below:

Sub Question # 3
Based on the experimental study, what are the security recommendations for vehicular networks?

While performing the validation experiment, on the first run, the subjected network topology (fig 4.3) generated 186 threats. The tailored MSTMT template for vehicular network also suggested some of the mitigation techniques with the threats. The following is a summary of the security recommendations for each class of (STRIDE) based on risk assessment run using the DAAM process model.

The security recommendations for each class (STRIDE) of threats generation by MS threat modeling tool are as under:

- *Spoofing* A spoofing attack occurs when an attacker impersonates the message/instruction creator or digital source to send spoofed signals. The general method to protect against spoofing attacks is to use authentication and several forms of authentication mechanisms exists:
  - Basic authentication
  - Message Digests e.g. MAC (Message Authentication Codes)
  - Kerberos
  - Public Key Infrastructure (PKI) systems
  - IPsec (Internet Protocol Security)
  - MACsec (Media Access Control Security)
- *Tampering* By definition, tampering is the act of altering the bits of a stream to cause damage or to make unauthorized alterations to the steam in order to execute unauthorized instructions. Both processes

and data streams are prone to being tampered by an intruder. Tampering attacks occur when the attacker modifies data in transit. The standard mitigations for tampering attacks are:

  - Using digital signatures or message authentication codes
  - Using a strong cryptography technique for storing or transmitting data

- *Repudiation* Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise, e.g., a user performs an illegal operation in a system that cannot trace the prohibited operations.

  Non-repudiation refers to the ability of a system to counter repudiation threats and provide an assurance of data being genuine. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package. One mitigation that is recommended to prevent repudiations is to have secure and authenticated event logging mechanisms in place.

- *Information Disclosure* Information disclosure happens when the information can be read by an unauthorized party. Information disclosure attacks occur when a sniffer can read sensitive information without the sender/receiver having any knowledge about it. Standard mitigations include:

  - Encryption of data transmitted on a wire
  - Using access control lists (ACLs)

- *Denial of Service* Denial of service (DoS) attacks deny service to valid users—for example, by making the ADAS ECUs computation power utilized 100 percent one could bring an autonomous truck to a halt and hence unavailable for legitimate use. You must protect against certain types of DoS threats merely to improve system availability and reliability.

  - Use firewall filter rules to protect against some network based attacks
  - Using SYN Cookies to prevent SYN flooding attacks
  - Using reverse proxies to prevent HTTP flooding
  - Using disk and processor quotas to prevent excess disk or CPU consumption

- *Elevation of Privileges* In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

  - Using input validation schemes
  - Using access control lists (ACLs)
  - Using principle of least privilege to implement the access levels

4.3 INTROSPECTING THE MODEL

To understand the effectiveness of the DAAM process model and find areas to improve its assessments, we performed an introspection. Since the DAAM process model is a composite of MSTMT and ASRAT (which is inspired by SESAR's SecRAM [50]), our target of evaluation is to understand the effectiveness of the composite tool from the outputs of the individual compositions.

MSTMT and DAAM

The Microsoft threat modeling tool 2016 runs on a template which contains the logic behind the threat generation. The MSTMT offers a canvas which is used to draw the topology of the network that is being analyzed. The DAAM process model makes use of the default MSTMT 2016 template and amends to its stencils with specialized components (e.g., ECUs) for a vehicular network. The customized template also offers threat properties and process-controls (e.g., Ethernet connections between ECUs) which are specific to vehicular networks. With the use of the DAAM's tailored template, MSTMT's engine can be used to generate a list of security threats for the vehicular networks.

The DAAM process model offers customized tools which enhance the threat generation of Ethernet-based vehicular networks.

SESAR's SecRAM and ASRAT

The SecRAM model is based on *ISO 27005* and focuses on two types of assets - primary assets and supporting assets. SecRAM focuses on finding the threat scenarios around the assets based on the *CIA Traid*[1] and offers a set of guidelines for the security risk assessment. The CIA stands for

- *Confidentiality* The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- *Integrity* The property of safeguarding the accuracy and completeness of assets
- *Availability* The property of being accessible and usable upon demand by an authorized entity

The adapted security risk assessment tool (ASRAT) is inspired by the SESAR's Security Risk Assessment Model (SecRAM). ASRAT offers a structured way of recording the information around the different steps of security risk assessment.

Number of iterations in the DAAM process

As discussed in the sections above, an iteration of assessment of the topology (Figure 4.3) using the DAAM process model lead to the generation of about **186 threats**. These threats are then ranked for being mitigated in accordance with multiple variables like the priority of mitigation, cost of mitigation, the effort required, the time needed to implement the mitigation and allied aspects that may be important to an organization. These variables may vary

1 CIA Triad: Confidentiality, Integrity, Availability

based on the organization and the kind of product (vehicular network) that is being subjected to the assessment.

To mitigate the issues, if required, the user can also alter the topology on the MSTM canvas (refer Figure 3.5). Thereby, running the topology through another round of assessment after fixing the issues can help the user to keep track of the changes. But it is also important to know *how many iterations is the most optimal choice*. Based on the validation run and the reviews from security experts, it was seen that:

- Besides the ability to track the changes and development, running the assessment for more than one iteration could also result in improving the maturity of security of the topology
- The number of iterations is relative to the complexity of topology and depends on case to case basis. e.g., two iterations were good enough for our validation run as we could reduce the count of security risks to a constant, however, for a complex network architecture this number may vary.

However, it is recommended that the users keep the following variables in mind while deciding the number of iterations required (value of n in Figure 4.4) for the assessment:

1. **Time complexity:** It is a time demanding task to perform an iteration of assessment using the DAAM model. Specifically for step 4 of the DAAM process may require discussions, literature study/references, and brainstorming.
2. **Redrawing topology:** Editing topology (step one of the DAAM process) in follow-up iterations may help in fixing some of the threats but a significant change (adding/removing components) may generate new threats. One of the advantages about threat generation in modeled environment is ease of backtracking.

4.4 IMPROVED DAAM PROCESS MODEL

As discussed in the previous sections, one of the conclusions of the validation run of the DAAM process model is to have the provision of iterations. Hence, the design of the process model is revised with an iterative loop that starts after the mitigation step and leads to draw/update the topology. The underlying Figure 4.4 represents a graphical view of the improved iterative-DAAM model.

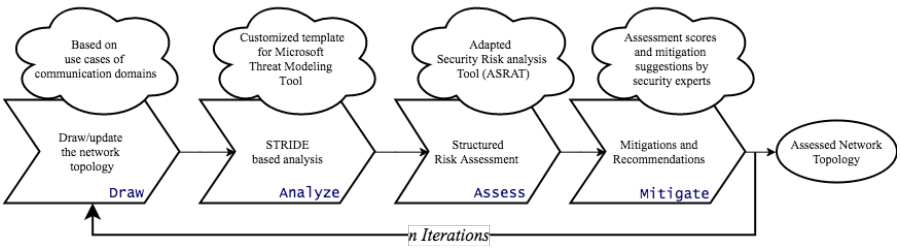


Figure 4.4: Enhanced iterative-DAAM process model for risk assessment (refer Table 3.1)

4.5 SUMMARY

In this chapter, we validated the DAAM security risk assessment process model which was proposed and designed in chapters 1 and 3. To perform the validation, we ran an experiment risk analysis on an Ethernet network topology of a vehicle, using the DAAM process model. The DAAM process model is a four-step process which, for the first step, needs us to plot the topology of the communication network of the vehicle. Our subject to run the experiment on was a Scania truck. Based on the understanding of the functional requirements of a Scania truck, we tried to plot a high-level diagram on MSTM canvas (section 4.2.3).

In Section 4.2.4 we performed the analysis of security threats, which marked the second step of the D.(Analyze).A.M process and utilizes MSTM template.

In the third step of the D.A.(Assess).M process, we assessed the security risks and estimated the impacts, as explained in Section 4.2.5. The next and the last step of the process was to log mitigation recommendations and the rationale of the security analysts. For the structured logging and tracking, we use the ASRAT (refer). Further, in the chapter, an introspection of the DAAM model was conducted. The introspection concluded that the process model can be helpful for the assessment of security risks for vehicular networks but may require a considerable amount of time especially for suggesting mitigations. It was also foreseen that if there were ways to store and reuse the rationale of security experts, then the process would save a lot of time and effort for future assessments - we discuss this in next chapter (refer Section 5.2).

5 CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

This master thesis project aims to design a systematic process to perform the security risk assessment of Ethernet-based communication networks for vehicles.

The problem was then rephrased into a research question and four knowledge questions. The research question answered in the thesis is:
What could be a structured way to perform security risk assessment of a vehicular Ethernet network, based on its network topology?
The research question was further divided into four sub-questions. Based on artifact study, we tried to get answers to the sub-questions, which helped in finding answers to the main RQ.The sub-questions are as under

> *1a. What are the available tools that can be used to analyze security threats and security risks for vehicular networks?*
>
> *1b. Can we customize the available security threat assessment tools to make them for vehicular network*
>
> *2. What are the functional requirements of heavy commercial vehicle's subsystem ECUs?*
>
> *3. Based on the experimental study, what are the security recommendations for vehicular networks?*

We began with understanding the gradual technological growth in the vehicular domain. It was seen that owing to the rising use of communication technologies, with time, the performance and safety features are improving. Compared to the vehicles in the past, today's vehicles have an abundance of sensors, highly intelligent ECUs and ADAS.

We understood further that the rising demands of having an improvised bandwidth capacity of the communication systems lead to the transition from using CAN to vehicular Ethernet. Vehicular Ethernet was seen as a trusted choice of technology for meeting the rising bandwidth requirements. However, it was foreseen that the transition would also bring in new sets of cybersecurity threats and challenges. While Ethernet provides excellent communication features like improved bandwidths (for intra-vehicle and V2X communications), encryption possibilities, possible authentication mechanisms, etc., the advancement also brought in new attack surfaces to the vehicle's communication infrastructure (see fig. 2.1).

Future vehicles are also seen as mobile cyber-physical systems and hence a concern with its insecurity to cyber risks can directly translate to a safety risk. For example, a compromised ECU can lead to a catastrophic safety hazard and even imply a threat to life. Hence, it is crucial for the security architects to perform a thorough risk assessment of the vehicular networks, right from the design stage. The project proposed the four-step DAAM security risk assessment model, which was specially designed to serve the

purpose of performing a structured cyber risk assessment for vehicular networks.

The literature study (Chapter 2) shows that there have been continuous efforts in the domain of risk assessment of IT-based technologies. Apart from some experimental results and theoretical models, there are some threat modeling tools and risk assessment methodologies that are widely used in the industries for native IT-based communication networks like LAN. However, a mobile cyber-physical system like a vehicular network is not the same as native IT-based communication networks for multiple reasons. One of the main reasons is physical access to the system - a potential attacker can have full access to the infrastructure of network nodes and ECUs. Physical access to the network makes it a bit easier for an intruder to understand the system. Also because vehicles are used to carry good and services for humans, the worst case impacts of malfunctions can be fatal to humans. Hence, the need to have a specialized threat generation and risk assessment methodology for vehicular networks was realized.

In Chapter 3, we designed and developed a specialized security risk assessment tool for vehicular networks. In Chapter 4, an experimental validation of the risk assessment model was performed. The experiment was followed up by introspection and henceforth enhancements of the process. The following section discusses the limitations and future work of the DAAM process model. The sub-questions, as mentioned in Chapter 1 have been answered through the chapters according to the nature of questions and the sections of the document.

5.2 LIMITATIONS AND FUTURE WORK

Limitations

The following are some of the limitations of the DAAM process model.

1. Time is a limiting factor: It was observed that even though the DAAM process model offers a structured way of handling security risk assessments, for less complex assessments, the process may appear to be more time demanding than usual methods. Especially the steps to analyze and mitigate may appear to be effort demanding, as the user is expected to log the rationale.

2. STRIDE Only: The DAAM process model helps in performing the security risk assessment of using STRIDE only. As discussed in literature study (Chapter 2), there are a handful threat classification methodologies, e.g., CIA triad that would provide other perspectives of the assessment.

3. Multiple files: The fact that the DAAM process model is a composite of multiple tools may also make it appear like a cumbersome model with multiple tools. For example, the MSTMT consists of two files - the MSTMT application and MSTMT tailored template. On being triggered, the MSTMT generates an HTML page with the list of threats. In the next step, the ASRAT offers an excel based tool to perform the risk assessment, log rationale, and mitigation decisions.

One of the unique advantages of having a structured record of the assessment and rationale of analysis by security experts on the SRAT tool is persistence and sharing of data.

Future work in this regard could be to connect the excel sheet to a database and store the logged feedback from security experts. Based on case-dependent decisions like threat category, impact, likelihood, mitigations and the rationale behind each, a machine learning algorithm can learn the trends and provide intellisense[1]/recommendations to the users of the tool in future. In the future, as the dataset of SRAT grows, the machine learning algorithm may also use the previous knowledge to assist users in drawing secure topologies right from step 1 of the DAAM process model.

1 Intellisense: https://msdn.microsoft.com/

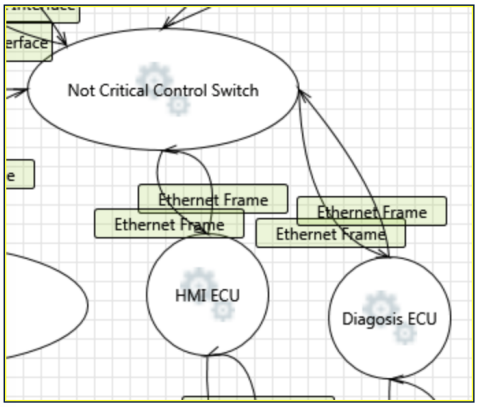
APPENDICES

A DAAM SECURITY RISK ASSESSMENT TOOL

SAMPLE OUTPUT FROM MS THREAT MODELING TOOL

The following are some of the examples of the threats generated by the MSTMT using tailored template for vehicular networks.

Interaction: Ethernet Frame



3. Diagosis ECU Process Memory Tampered [State: Not Started] [Priority: High]

Category:	Tampering
Description:	If Diagosis ECU is given access to memory, such as shared memory or pointers, or is given the ability to control what Not Critical Control Switch executes (for example, passing back a function pointer.), then Diagosis ECU can tamper with Not Critical Control Switch. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification:	<no mitigation provided>
Impact level:	Medium
Attack Method:	
Recommendation:	Use domain sepearation feature on the run-time system (OS or RTOS) on both the Diagosis ECU and Not Critical Control Switch in order to protect process memory from beeing directly access by external processes Mitigate by: (source.[Isolation Level] is 'Sandbox' or source.[Isolation Level] is 'AppContainer') and (target.[Isolation Level] is 'Sandbox' or target.[Isolation Level] is 'AppContainer')
Impact type:	Functional

12. Data Flow Sniffing [State: Not Started] [Priority: High]

Category:	Information Disclosure
Description:	Data flowing across Ethernet Frame may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.
Justification:	<no mitigation provided>
Impact level:	Medium
Attack Method:	
Recommendation:	Consider encrypting the data flow. Mitigate by: flow.[Provides Confidentiality] is 'Yes' or (flow is [Ethernet Frame] and (flow.[Use MACSEC] is 'Yes' or flow.[Use IPSEC] is 'Yes'))
Impact type:	Functional

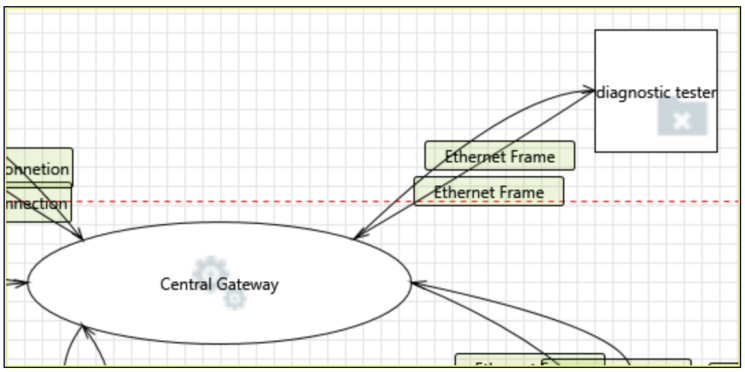
13. The LIDAR Data Store Could Be Corrupted [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Data flowing across Ethernet Frame may be tampered with by an attacker. This may lead to corruption of LIDAR. Ensure the integrity of the data flow to the data store.
Justification:	<no mitigation provided>
Impact level:	Medium
Attack Method:	
Recommendation:	Mitigate by: flow is [Ethernet Frame] and (flow.[Provides Integrity] is 'Yes' or flow.[Use MACSEC] is 'Yes' or flow.[Use IPSEC] is 'Yes')
Impact type:	Functional

B ADAPTED SECURITY RISK ASSESSMENT TOOL'S STRUCTURE

For the validation experiment the ASRAT tool was built on MS Excel sheet. The ASRAT tool has three tables and the structure of the tables are as under:

Interaction: Ethernet Frame



109. Spoofing of the diagnostic tester External Destination Entity [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	diagnostic tester may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of diagnostic tester.
Justification:	<no mitigation provided>
Impact level:	Medium
Attack Method:	
Recommendation:	Consider using a standard authentication mechanism to identify the external entity. Mitigate by: target.[Authenticates Itself] is 'Yes' or flow.[Destination Authenticated] is 'Yes' or (flow is [Ethernet Frame] and (flow.[Use MACSEC] is 'Yes' or flow.[Use IPSEC] is 'Yes'))
Impact type:	Functional

186. Potential Lack of Input Validation for Central Gateway [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Data flowing across wireless connetion may be tampered with by an attacker. This may lead to a denial of service attack against Central Gateway or an elevation of privilege attack against Central Gateway or an information disclosure by Central Gateway. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues.
Justification:	<no mitigation provided>
Impact level:	Medium
Attack Method:	
Recommendation:	Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. Mitigate by:((flow.[Provides Confidentiality] is 'Yes' and flow.[Provides Integrity] is 'Yes') or flow.[Use IPSEC] is 'Yes' or (flow is [Ethernet Frame] and flow.[Use MACSEC] is 'Yes') and flow.[Filtered By Firewall Rule] is 'Yes')
Impact type:	Functional

Asset ID	Interaction	Asset Association	
		Asset Name	Type/Description

A: First tab of ASRAT: Assets declarations

Associated to Asset ID	Threat						Impact		Likelihood		Risk		
	Threat ID	Threat Type	S,T,R,I,D or E	Description	*Justification*	Attack Method	Impact level	*Rationale*	0-unknown 1 (unlikely)-5 (highly likely)	Rationale	Risk Score (Impact X	Priority Level	*Justification*

B: Second tab of ASRAT: Impact, likelihood and risk calculations

Threat		Mitigation				Status	
Threat ID	Category	*Recommendation*	*Rationale*	Description	*Rationale*	Mitigated/Not mitigated/Does not need mitigation	*Rationale*

C: Third tab of ASRAT: Mitigation

The Adapted Security Risk Analysis Tool (ASRAT): The structure of this tool is built in MS Excel application. There are three tabs in this tool (A,B and C) as described above.

BIBLIOGRAPHY

[1] In: *International Standards Organization 17987-7:2016 Preview Road vehicles – Local Interconnect Network (LIN)* Revision 2.2A (2010), Part 1-7.

[2] In: *International Standards Organization 11898-1:2015, CAN* 2 (2015), Part 1-3.

[3] National Highway Traffic Safety Administration et al. "Preliminary statement of policy concerning automated vehicles." In: *Washington, DC* (2013), pp. 1–14.

[4] Christopher Alberts et al. *Introduction to the OCTAVE Approach*. Tech. rep. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2003.

[5] Lucia Lo Bello. "The case for Ethernet in automotive communications." In: *ACM SIGBED Review* 8.4 (2011), pp. 7–15.

[6] Rikard Blom et al. "Analyzing attack resilience of an advanced meter infrastructure reference model." In: *Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Joint Workshop on*. IEEE. 2016, pp. 1–6.

[7] Stephen Checkoway et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In: *USENIX Security Symposium*. San Francisco. 2011.

[8] Yulia Cherdantseva and Jeremy Hilton. "A reference model of information assurance & security." In: *Availability, reliability and security (ares), 2013 eighth international conference on*. IEEE. 2013, pp. 546–555.

[9] Siegfried Cojocaru, Constantin Rădoi, and Ştefan Stăncesu. "The Analysis of CAN and Ethernet in distributed real-time systems." In: *Scientificbulletin* ().

[10] FlexRay Consortium et al. "FlexRay Communications System Protocol Specification Version 2.1, 2005; ISO 17458." In: *Flexray* ISO 17458 (2005).

[11] Orjan Danielsson Hans-Ake Aslund. "Scania demonstrates autonomous transport system." In: *Scania Corporate Relations* (2016), pp. 1–3.

[12] Martin Eberhard and Marc Tarpenning. "The 21 st Century Electric Car Tesla Motors." In: *Tesla Motors* (2006).

[13] Mathias Ekstedt et al. "Securi cad by foreseeti: A cad tool for enterprise cyber security management." In: *Enterprise Distributed Object Computing Workshop (EDOCW), 2015 IEEE 19th International*. IEEE. 2015, pp. 152–155.

[14] Steve Elky. "An introduction to information systems risk management." In: (2006).

[15] Waldo Rocha Flores and Mathias Ekstedt. "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness." In: *computers & security* 59 (2016), pp. 26–44.

[16] M Gillberg, G Kecklund, and T Åkerstedt. "Sleepiness and performance of professional drivers in a truck simulator—comparisons between day and night driving." In: *Journal of Sleep Research* 5.1 (1996), pp. 12–15.

[17] Massimo Guarnieri. "When cars went electric, part one [historical]." In: *IEEE Industrial Electronics Magazine* 5.1 (2011), pp. 61–62.

[18] Peter Hank, Thomas Suermann, and Steffen Müller. "Automotive Ethernet, a holistic approach for a next generation in-vehicle networking standard." In: *Advanced Microsystems for Automotive Applications 2012* (2012), pp. 79–89.

[19] Peter Hank et al. "Automotive ethernet: in-vehicle networking and smart mobility." In: *Proceedings of the Conference on Design, Automation and Test in Europe*. EDA Consortium. 2013, pp. 1735–1739.

[20] Florian Hartwich et al. "CAN with flexible data-rate." In: *Proc. iCC*. 2012, pp. 1–9.

[21] Bernd Heißing and Metin Ersoy. "The Future of Chassis Technology." In: *Chassis Handbook*. Springer, 2011, pp. 557–578.

[22] Hannes Holm, Mathias Ekstedt, and Dennis Andersson. "Empirical analysis of system-level vulnerability metrics through actual attacks." In: *IEEE Transactions on dependable and secure computing* 9.6 (2012), pp. 825–837.

[23] Erik Johansson and Pontus Johnson. "Assessment of enterprise information security-an architecture theory diagram definition." In: *Proc. of CSER* 5 (2005).

[24] Pontus Johnson et al. "pwnPr3d: An Attack-Graph-Driven Probabilistic Threat-Modeling Approach." In: *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE. 2016, pp. 278–283.

[25] Pontus Johnson et al. "Time between vulnerability disclosures: A measure of software product vulnerability." In: *Computers & Security* 62 (2016), pp. 278–295.

[26] Jan Jürjens. "UMLsec: Extending UML for secure systems development." In: *International Conference on The Unified Modeling Language*. Springer. 2002, pp. 412–425.

[27] Sathya Prakash Kadhirvelan and Andrew Söderberg-Rivkin. "Threat Modelling and Risk Assessment." In: (2014).

[28] John Kendall. *Mercedes-Benz Future Truck 2025 demonstrates autonomous technology - SAE International*. [Online; accessed 07-May-2017]. 2014.

[29] Barbara Kitchenham et al. "Systematic literature reviews in software engineering–a systematic literature review." In: *Information and software technology* 51.1 (2009), pp. 7–15.

[30] Barbara Kordy, Ludovic Piètre-Cambacédès, and Patrick Schweitzer. "DAG-based attack and defense modeling: Don't miss the forest for the attack trees." In: *Computer science review* 13 (2014), pp. 1–38.

[31] Karl Koscher et al. "Experimental security analysis of a modern automobile." In: *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE. 2010, pp. 447–462.

[32] Charles M. Kozierok et al. *Automotive Ethernet: The definitive guide*. ISBN: 978-0-9905388-0-6. Intrepid Control Systems, 2014.

[33] Katsiaryna Labunets, Federica Paci, and Fabio Massacci. "Which security catalogue is better for novices?" In: *Empirical Requirements Engineering (EmpiRE), 2015 IEEE Fifth International Workshop on*. IEEE. 2015, pp. 25–32.

[34] Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.

[35] Georg Macher et al. "A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context." In: *International Conference on Computer Safety, Reliability, and Security*. Springer. 2016, pp. 130–141.

[36] D. Mellado. *IT Security Governance Innovations: Theory and Research: Theory and Research*. Advances in Information Security, Privacy, and Ethics: Information Science Reference, 2012, pp. 35–36. ISBN: 9781466620841. URL: https://books.google.se/books?id=R7WeBQAAQBAJ.

[37] Robert M Metcalfe and David R Boggs. "Ethernet: Distributed packet switching for local computer networks." In: *Communications of the ACM* 19.7 (1976), pp. 395–404.

[38] Xinming Ou, Sudhakar Govindavajhala, and Andrew W Appel. "MulVAL: A Logic-based Network Security Analyzer." In: *USENIX security*. 2005.

[39] Donn B Parker. *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons, Inc., 1998.

[40] Aneesh Paul et al. *Advanced Driver Assistance Systems*. Tech. rep. SAE Technical Paper, 2016.

[41] Jonathan Petit and Steven E Shladover. "Potential cyberattacks on automated vehicles." In: *IEEE Transactions on Intelligent Transportation Systems* 16.2 (2015), pp. 546–556.

[42] Pierre Philip and Torbjorn Åkerstedt. "Transport and industrial safety, how are they affected by sleepiness and sleep restriction?" In: *Sleep medicine reviews* 10.5 (2006), pp. 347–356.

[43] Bruce Potter. "Microsoft SDL threat modelling tool." In: *Network Security* 2009.1 (2009), pp. 15–18.

[44] Lars Regar. "The Road Ahead for Securely-Connected Cars." In: *ISSCC 2016 / Session 1 / Plenary / 1.4* 1 (2016), pp. 29–33. DOI: 978-1-4673-9467-3/16/.

[45] Lars Reger. "Securely Connected Vehicles-What it takes to make self-driving cars a reality." In: *21st IEEE European Test Symposium (ETS)* 21.1 (2016), p. 1. DOI: 978-1-4673-9659-2/16.

[46] Alastair Ruddle et al. "Security requirements for automotive on-board networks based on dark-side scenarios." In: *EVITA Deliverable D* 2 (2009), p. 3.

[47] Paul Saitta, Brenda Larcom, and Michael Eddington. "Trike v. 1 methodology document [draft]." In: *N/A* (2005).

[48] Mark Sauerwald. "CAN bus, Ethernet, or FPD-Link: Which is best for automotive communications?" In: *Texas Instrument Analog Appl. J.* 1 (2014), pp. 20–22.

[49] Jochen Schyma. *Big Data Rates in the Car: Ethernet & more over one single Link System*. 1st ed. IEEE.

[50] ATM SESAR. "SecRAM implementation guidance material." In: *Project deliverable* 16 (), pp. 03–D03.

[51] Adam Shostack. "Experiences threat modeling at microsoft." In: *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK*. 2008.

[52] Adam Shostack. *Threat modeling: Designing for security, ISBN 978-1-118-80999-0*. John Wiley & Sons, 2014.

[53] Teodor Sommestad, Mathias Ekstedt, and Pontus Johnson. "A probabilistic relational model for security risk analysis." In: *Computers & Security* 29.6 (2010), pp. 659–679.

[54] Marco Steger et al. "A security metric for structured security analysis of cyber-physical systems supporting SAE J3061." In: *Modelling, Analysis, and Control of Complex CPS (CPS Data), 2016 2nd International Workshop on*. IEEE. 2016, pp. 1–6.

[55] Steve C Talbot and Shangping Ren. "Comparision of fieldbus systems can, ttcan, flexray and lin in passenger vehicles." In: *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on*. IEEE. 2009, pp. 26–31.

[56] *The Automotive Threat Modeling Template - NCC Group*. July 2016.

[57] RICHARD Truett. "Automakers see promise in placing power at wheels." In: *Automotive News* 78.3 (2004), p. 8.

[58] Sadayuki Tsugawa. "An Overview on an Automated Truck Platoon within the Energy ITS Project." In: *IFAC Proceedings Volumes* 46.21 (2013). 7th IFAC Symposium on Advances in Automotive Control, pp. 41–46. ISSN: 1474-6670. DOI: https://doi.org/10.3182/20130904-4-JP-2042.00110. URL: http://www.sciencedirect.com/science/article/pii/S1474667016383409.

[59] Sadayuki Tsugawa, Shin Kato, and Keiji Aoki. "An automated truck platoon for energy saving." In: *Intelligent Robots and Systems (IROS), 2011 IEEE/RSJ International Conference on*. IEEE. 2011, pp. 4109–4114.

[60] Shane Tuohy et al. "Intra-vehicle networks: A review." In: *IEEE Transactions on Intelligent Transportation Systems* 16.2 (2015), pp. 534–545.

[61] B Weyl et al. "Securing vehicular on-board IT systems: The EVITA Project." In: *25th Joint VDI/VW Automotive Security Conference. Ingolstadt, Germany*. 2009.

[62] Michael E Whitman and Herbert J Mattord. *Hands-on information security lab manual*. Cengage Learning, 2012.

[63] Karsten Wittmack. *Introducing Automotive Ethernet - A project managers account*. 1st ed. 5th IEEE Standards Association (IEEE- SA) Ethernet & IP @ Automotive Technology Day, 2015, 2017, pp. 1–18. URL: https://standards.ieee.org/events/automotive/2015/00_Keynote_BMW_Introducing_Ethernet_v1.0.pdf.

[64] Marilyn Wolf. "Embedded software in crisis." In: *Computer* 49.1 (2016), pp. 88–90.