jamk.fi

Cyber Security of Highly Automated Connected Machines

Design cyber security model for Ponsse group research's and development

Sami Ahonen

Master's thesis
November 2020
School of Technology, communication and transport
Master's Degree program in Information Technology
Cyber security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Ahonen, Sami	Type of publication Master’s thesis	Date November 2020
		Language of publication: English
	Number of pages 92	Permission for web publication: x

Title of publication

Cyber security of highly automated moving machines

Design cyber security model for Ponsse group research and development

Degree programme

Master’s Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Saharinen, Karo; Hautamäki, Jari

Assigned by

Ponsse Oyj, Epec Oy

Abstract

Rapid integration and interconnection of information systems creates new cyber security related threats for information systems around the world. Today, these threat scenarios are also present in mobile work machines in various industries.

This study examines the cyber security of the Control Platform system developed jointly by Ponsse and Epec. The work examines various protection methods, threats to mobile work machines and information security controls necessary to prevent threats. In addition to the external threats to information systems, this work focuses in part on threats from within the organization and their prevention.

The study has been implemented in part as an interview study to gather Ponsse's and Epec's views on the development of information security. During the study, a risk assessment related to cyber threats was also carried out to identify the threats and to define security controls. The work also identifies standards and guidelines for organizations to support the development of cybersecurity.

According to research, machine control systems for mobile work machines are as vulnerable to cyber-attacks as traditional information systems, for example in the office. Even in the case of mobile work machines, cyber threats today are real, and measures must be taken to prevent them.

Keywords/tags (subjects)

Mobile machinery cyber security, Cybersecurity, automotive ethernet, cyber security management system, cyber security of highly automated connected machines

Miscellaneous (Confidential information)

Attachments to the work are confidential and have been removed from public work. The basis for secrecy is section 24, item 17, of the Publicity Act 621/1999, the company's business or professional secret. The confidentiality period is five (5) years, the confidentiality expires on February 9, 2026.

jamk.fi

Kuvaus

Tekijä(t) Ahonen, Sami	Julkaisun nimi Opinnäytetyö, ylempi AMK	Päivämäärä Marraskuu 2020
		Julkaisun kieli: Englanti
	Sivumäärä 92	Verkkojulkaisulupa myönnetty: x

Työn nimi

Korkeasti automatisoitujen liikkuvien työkoneiden kyberturvallisuus

Kyberturvallisuusmallien kehitys Ponsse-ryhmän tutkimukseen ja tuotekehitykseen

Tutkinto-ohjelma

Master’s Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Saharinen, Karo ja Hautamäki, Jari

Toimeksiantaja(t)

Ponsse Oyj, Epec Oy

Tiivistelmä

Tietojärjestelmien nopea integrointi ja yhteenliittyminen luo uusia kyberturvallisuuteen liittyviä uhkia tietojärjestelmille ympäri maailmaa. Nykyään nämä uhkaskenaariot ovat läsnä myös eri toimialojen liikkuvissa työkoneissa.

Tässä tutkimuksessa tarkastellaan Ponssen ja Epecin yhdessä kehittämän Control Platform -järjestelmän kyberturvallisuutta. Työssä tarkastellaan erilaisia suojausmenetelmiä, liikkuvien työkoneiden uhkia ja tietoturvan valvontaa, jotka ovat välttämättömiä uhkien estämiseksi. Tietojärjestelmiin kohdistuvien ulkoisten uhkien lisäksi tässä työssä keskitytään osittain organisaation sisäisiin uhkiin ja niiden ehkäisyyn.

Tutkimus on toteutettu osittain haastattelututkimuksena Ponssen ja Epecin näkemysten keräämiseksi tietoturvan kehittämisestä. Tutkimuksen aikana tehtiin myös kyberuhkiin liittyvä riskinarviointi uhkien tunnistamiseksi ja turvatarkastusten määrittelemiseksi. Työssä käydään läpi myös soveltuvia standardit ja ohjeistuksia organisaatioille kyberturvallisuuden kehittämisen tukemiseksi.

Tutkimuksen mukaan liikkuvien työkoneiden koneohjausjärjestelmät ovat yhtä alttiita kyberhyökkäyksille kuin perinteiset tietojärjestelmät esimerkiksi toimistossa. Jopa liikkuvien työkoneiden kohdalla kyberuhat ovat nykyään todellisia, ja niiden estämiseksi on toteutettava toimenpiteitä.

Avainsanat / tunnisteet (subjects)

Liikkuvien koneiden kyberturvallisuus, kyberturvallisuus, automotive ethernet, kyberturvallisuuden hallintajärjestelmä, korkeasti automatisoitujen kytkettyjen koneiden kyberturvallisuus

Sekalaiset (Confidential information)

Liitteet ovat luottamuksellisia ja ne on poistettu julkisesta työstä. Salaisuuden perustana on julkisuuslain 621/1999 24 §, kohta 17, yhtiön liike- tai ammattisalaisuus. Salassapitoaika on viisi (5) vuotta, luottamuksellisuus päättyy 9. helmikuuta 2026.

Contents

Figures

Tables

Terminology

CAN	Controller area network
CIA	Tried Confidentiality Integrity and Availability
CSMS	Cyber Security Management System
CTL	Cut to Length
DDOS	Distributed Denial of Service
DMZ	Demilitarized Zone
DOS	Denial of Service
DTLS	Datagram Layer Security
E/E	Electrical and electronic
HMAC	Hashed Message Authentication Code
HSM	Hardware Security Module
HTTPS	Hyper Text Transfer Protocol Secure
IoT	Internet of Things
IPsec	Internet Protocol Security
ISMS	Information Security Management System
IT	Information Technology
IVN	In-vehicle network
SDL	Secure Development Lifecycle
SDN	Software Defined Networking
SFTP	Secure File Transfer Protocol
SL	Security Level
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSN	Time sensitive networking
UDP	Use Datagram Protocol

1. Introduction

Today's information systems and technologies are evolving really fast and more and more systems are integrating with each other using Internet connections. Data transfer methods enable a completely new kind of development, for example by utilizing data collected from various devices and analyzing it with data analytics tools or with the help of artificial intelligence. However, this high degree of integration poses new threats to companies and their customers and their operations. Cyber risks are becoming one of the most important issues to consider in the development, operation and maintenance of systems. (Schmittner, 2019)

The rapid development of vehicle technologies also brings new technologies into vehicles that do not normally work on the road, such as Automotive Ethernet bus solutions. On the automotive side, cyber risks, their identification and prevention have been taken into account and new standards are constantly being created. Cyber threats are a reality in all systems using the internet today as well as in mobile work machines. (Schmittner, 2019) This work examines cyber threats as well as their response from the perspective of mobile work machines.

Focus of this thesis is the cyber threats of mobile highly automated connected work machine control systems and their protection. The client of the work is Ponsse Oyj and its subsidiary Epec. The aim of this study was to find a comprehensive cyber security implementation model suitable for Ponsse and Epec needs.

Ponsse is one of the world's leading manufacturers of forest machines. The company's operations are very customer-oriented, driven by the wishes and needs of forest machine entrepreneurs. PONSSE forest machines. PONSSE forest machines are based on environmentally friendly wood harvesting (CTL), where trees are felled, handled and cut into various log assortments before they leave the forest. Ponsse’s produces multiple different type of harvesting needs for example first thinning and the harvesting of forest energy to heavy-duty regeneration felling, as well as all logging sites, from soft soil to steep slopes. All machines produced by the company are manufactured in Vieremä, where the company's factory is located. (Ponsse Oyj, 2020)

Epec Oy is a subsidiary owned by Ponsse. Epec Oy manufactures intelligent machine control systems for mobile work machine manufacturers for demanding conditions. The company supplies control systems for agricultural, stone processing, forestry, mining and waste handling machines, among others. (Raitis, 2018)

In this work, the researcher got to know in depth the joint Control Platform project between Ponsse and Epec. The aim of this project was to develop a next-generation control system for the product family, to the needs of Ponsse and Epec's customers.

2. Mobile connected highly automated machines

Globally, there are many industries that use mobile work machines for a variety of work tasks. This section provides an example of a few industries and the machines used in them.

2.1.1 Logging industry

Tree harvesting is the cutting and processing of trees to produce wood and pulp to supply the world market for example: furniture, construction, paper and other products. Timber harvesting practices vary between large timber plantations and firewood harvesters. (environment, 2020)

Nowadays trees are harvested from the forest by using big forest machines such as harvesters (figure 1), feller-bunchers and collected by using forwarders of skidders. In globally there are multiple machine manufacturers which produces these machines into world's markets. There is two different kind of methods for wood harvesting cut-to-length and whole tree logging. (Orange, 2020)

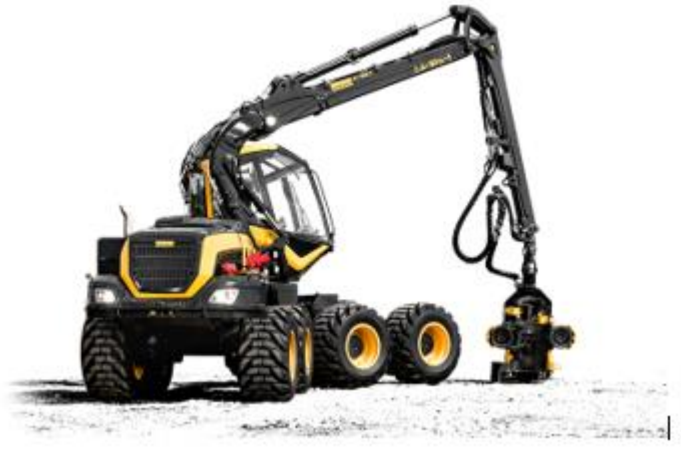


Figure 1. Ponsse Scorpion (Ponsse, 2020)

The total amount of timber removed in 2010 was 3.4 billion cubic meters, which does not consider the amount of illegally removed timber. According to the 2011 FAO World State Forests Report, the amount of saw logs removed was 853 million m3, the volume of pulpwood was 527 m3 and the volume of other industrial roundwood was 157 million m3. Energy wood and household firewood accounted for 1.87 billion m3. (environment, 2020)

2.2 Mining industry

Mining is the extraction of valuable materials and minerals from the earth. Usually mined materials are different kind of metals, coal, oil shale, gemstones, limestone, chalk, dimension stone, rock salt, potash, gravel, and clay. (What is Mining?, 2020)

At 2018 world’s mining production was 17,7 billion metric tons. Mining is done on all continents. Biggest producer is Asia (58,3%). Most mined material is iron ore, ratio of iron ore is 97,1% to 2,9%. (Reichl, 2020)

Mining techniques can be divided into two general types of mining: surface mining and underground surface mining (underground). Today, surface mining is much more common, producing, for example, 85% of minerals (excluding oil and natural gas) in the United States, including 98% of metal ores. (What is Mining?, 2020)

Today, the mining industry uses mobile machinery to perform mining. Commonly needed machines are mining drills (figure 2), blasting tools, earth movers, crushing equipment, feeding, conveying, and on-line elemental analysis equipment. (Gasdia-Cochrane, 2015)

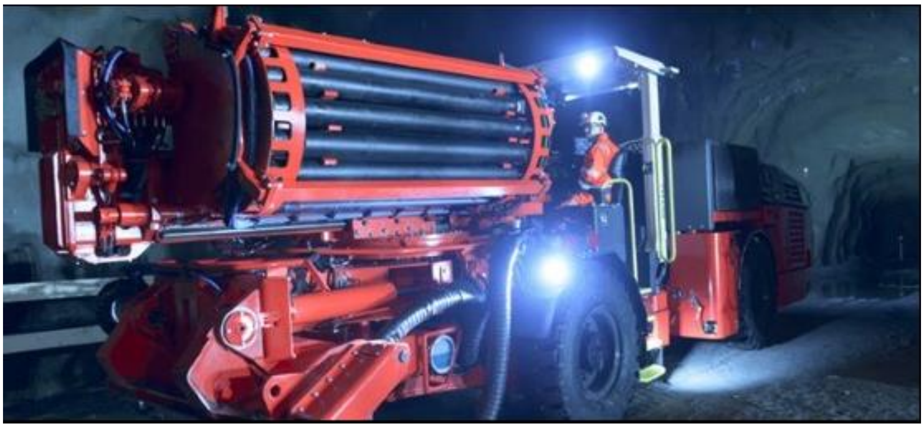


Figure 2. Longhole drill rig (Sandvik, 2020)

2.3 Maritime industry

Maritime industry in Finland is dominated by exports. It consists of different business operations related to ships, maritime technology, boats, maritime infrastructure, environmental technology and maritime functions. Industry is divided into four different sectors: newbuilding and repair shipyards, boar industry and trade, port and water building sector, environmental technology. (Meriliitto - Sjöfartsforbundet RY, 2020)

According to United Nations report 2019 Review of maritime transportation is estimated that total amount of transports in the world were 11 billion tons. And estimated total number of containers handled at worldwide is 793.26 million TEU's. Asia is the bigger producer of container traffic 64% containers were handled at Asia, second position is Europe with 16% share and the third biggest one is North America at 7% share. (United Nations Conference UNCTAD, 2019)

Maritime industry uses lots of different equipment's (like at figure x) and technologies for example to control ship loading, navigation, route planning and automatic ship control (KaranC, 2020). Common denominator for these equipment's is that at some way there is embedded control systems behind these solutions which are used perform actions that these devices operates

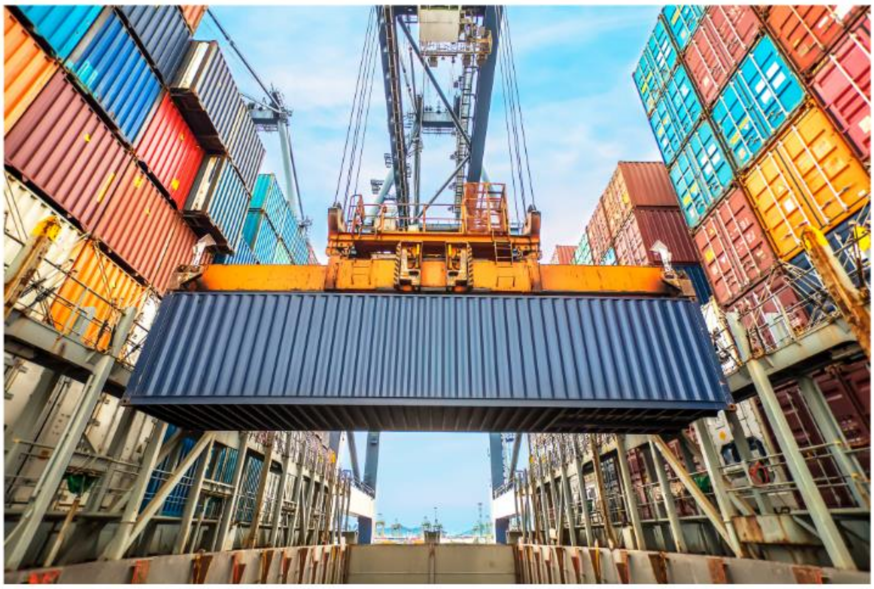


Figure 3. Maritime container handling equipment (Maritime Industry Foundation, 2020)

2.4 Common denominators in different industries

Common to all industries and the machines used in them is that today many devices and machines use some kind of information system, for example to measure and store production data and to analyze and collect various diagnostic data. In most cases, these systems also talk to each other between machines or transfer information to back-end systems, such as cloud services, or receive control information from back-end systems. This diversity exposes systems to hacking, hacking, or phishing.

Another common factor for these control systems is that usually the software update intervals for these systems are long, if the system works why update it. Correspondingly, IT systems are updated in a much faster cycle, for example, critical security updates are handled almost daily from the bottom up, which allows for better protection against cybercrime.

However, we must be remembered that embedded systems are not the most desirable target for cybercriminals. According to publication of Infradata (Infradata Inc, 2019), security has become a priority at industrial IT and Operational Technology OT because connectivity into external systems grows and this enables more wider attack vectors. Often companies that develop OT technology solutions do not have knowledge and awareness of cyber threats and attacks, compared to solution vendors that are working with traditional IT technology area.

Often Cyber-attacks main purpose is financial gain or intentional distribution of business activities or to damage industrial materials and equipment's. These attacks may also lead secondary consequences for safety and health. A good example of safety related cyber-attack in 2014 was attack against German steel mill. This attack caused lots of physical damage by preventing control systems for down blast furnaces properly. Target of the attack may have been sabotage of industrial control systems, but when discovering steel mill production environment is very dangerous place because of hazardous nature of the processes and materials involved and therefore attack could have caused serious damage to human lives. (Informa Markets, 2017)

Admittedly, the world is changing at a rapid pace and attacks on more and more information systems are possible. The interconnection of systems, for example through cloud services, also allows for an ever-increasing attack interface for cybercriminals, and it is simply very important to take this aspect into account in the development of today's information systems.

3. Control platform project

The goal of the Control Platform project is to develop a future-proof control system solution for Ponsse and Epec. On the automotive side, for example, autonomous cars are becoming, the trend in the world is rapid. One of the goals of this project is to build a system to which external devices and technology can be easily added in the future, such as camera technology or lidar sensor systems. Easy connectivity and machine diagnostics play an important role in the solution being developed.

3.1 System architecture

Initial version of Control Platform contains following control system devices. OptiPC (Windows 10 IoT Enterprice), Core unit (Linux based embedded device), multiple Gateway devices (ARM STM32 embedded control system device) and multiple CAN based devices to communication control system related sensors and control related to machine control. Also so called subcore devices can also be connected to Gateway devices.

Architechture is centralized system architechture where core unit contains all system intelligence and makes decisions and gateway devices at just dummy devices which commands actuators and sensors according to the core unit commands. Core and gateway units architechture is described at appendencies 2 and 3 and overall system architechture is described at appendix 4.

Machine control system communication and protocols

Communication between ethernet based control system devices inside the forest machine is planned to implement by using UDP instead of session based TCP. Serial communication ports are available at control system devices and CAN messaging is used to communicate between sensors and other componednts such as diesel engine.

For the connection from OptiPC to Core unit and filetransfer protocols SSH and SFTP is planned to be used.

IVN communication into external systems

Communication from machine to cloud services is implemented by using mobile connections 3G/4G internally or externally. Also control system modules contains Bluetooth and WLAN connection interfaces for example communication with mobile applications.

Other services

Architecture also describes some services that should be taken in account when planning security. It is planned that core unit contains web server implementation at some point for machine service operators use for example showing machine diagnostics views. Diagnostics view is going to be presented for use thru web page at browser.

4. Research implementation

4.1 Research questions and research framework

Three main research questions were investigated in this thesis. The main research questions are:

1) How control systems of mobile machines and their In-Vehicle Network communication should be constructed in order to make it safe from a cyber security point of view?
2) What are possible attack vectors/interfaces and what security controls should implemented to secure IVN?
3) What is a good cyber security model that can will be used at development and maintenance of control systems for mobile machines?

The aim of the study is to clarify cyber security aspects of connected machines and provide good overview into cyber security models for implementing cyber-secure systems at Ponsse and Epec.

In this thesis, qualitative research was used as the research method. The researcher collected research material through theme interviews from the target organization and conducted a covered literature review.

Theme interviews were conducted during study. The aim of the theme interviews was to gather information about the organization's cybersecurity expertise, experiences with the product development and maintenance of current systems, and the goals and requirements of the Control Platform project from a cyber security perspective. After interviews and literature review reseacher created different cyber security models for organizations needs.

Researcher selected qualitative research method to implementing research. As data collection method researcher selected two phase theme interview, but eventually decided to give up of second round interviews. Instead of a second round of interviews, the researcher decided to conduct a threat assessment for the system under study.

Figure 4 shows this work research framework, at center of figure are these three main questions and to get answer these questions. Researcher needs to get familiarize about cyber security standards and their relation into functional safety, get knowledge about automotive ethernet, perform literature study, perform theme interview into target organization's employees and conduct threat assessment.

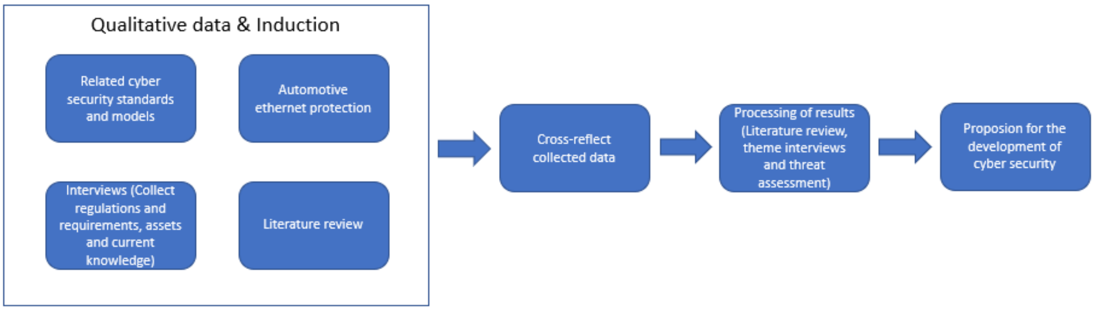

Qualitative data & Induction
Related cyber security standards and models
Automotive ethernet protection
Interviews (Collect regulations and requirements, assets and current knowledge)
Literature review
Cross-reflect collected data
Processing of results (Literature review, theme interviews and threat assessment)
Proposion for the development of cyber security

Figure 4. Research framework

Research framework describes outcome of this thesis. Outcome is to create comprehensive and understandable Cyber security models for Ponsse's and Epec's needs. This model should cover guidance how Control Platform projects outcome system should be secured to get it safe as cyber security point of view.

4.2 Research methods

The researcher began researching a collaborative project between Ponsse and Epec called Control Platform.

At the beginning of the study, the information on cyber security already available at Ponsse was examined, as well as the technology prestudy study ordered by Epec Oy from Ricardo. In addition to this, the researcher became acquainted with the same

Automotive ethernet material from Ponsse, which the company had acquired from the Automotive Ethernet Congress held in Germany in March 2020.

The researcher decided to carry out the study as a qualitative study, the literature data collection method used was a literature review, and information on the target organizations was collected through theme interviews at spring of year 2020.

In the literature review, the researcher searched for previous research and became acquainted with various cybersecurity guidelines and standards that could be valuable for target organizations. In addition, the study covered the operational safety standard and the processes used by the company.

In addition to this, the researcher was also able to participate in daily Scrum daily meetings with the people of the development team as well as other events and planning events related to the Control Platform project. This participation into daily Scrum’s was very helpful way of working.

During this thesis implementation researcher decide to conduct risk assessment for target control system, following instruction from NIST 800-30. Risks were classified by using impact of the risk and occurance of the risks. After threat classification risks we collected into risks matrix. The risk matrix provides a good picture of the worst threats, this information helps to select propriate security controls to stop threats or avoid them totally.

4.2.1 Theme interviews

For the theme interview, the employee received 10 people from Ponsse and Epec organizations from different positions. Of these individuals, 9 were interviewed from 5 Ponsse organizations and 4 from Epec's organization. The following is a table (table 1) of interviewees about their positions:

Table 1. Interviewed employees from Ponsse and Epec organizations

Ponsse	Epec
Information Security Manager	Data Security Manager
Project Manager I	FW Developer I
Project Manager II	FW Developer II
SW Designer	Epec IoT Solutions Manager
HW Designer	

For the theme interview, the employee selected the following topics:

1. Control Platform project (assets to secure)
2. Cyber Security aspects of hightly automated connected machines (cyber threats, risk and security controls)
3. Organizations current knowledge of Cyber Security
4. Development process security aspects (HW &SW)
5. Maintenance process security aspects (HW & SW)
6. Knowledgement of different Cyber security standards
7. What is good Cyber security model?

Purpose of the theme inteviews was to find out assets that needs to be secure. Discuss cyber threats, risks and currently planned security controls, map current cyber security knowledgement of organizations, gather information about current HW & SW development and maintenance processes. Discuss also about current knowledgement of different cyber security standards and lastly gather current organizations informations about different cyber security models.

4.2.2 Literature study

Beginning of the literature study researched walk thru Automotive Ethernet congress material to familiarize automotive ethernet security controls and future visions from automotive side. These materials very helpful for researcher to jump into automotive ethernet challenges and solutions.

One phase of the reseach was to examine existing cybersecurity standards and guidelines. No directly applicable standard or guidelines were found for mobile machinery. In this study, the researcher went through several exploitable standards related to industrial automation systems. The literature review also aimed to examine the various threats and safeguards associated with the target system.

4.2.3 Thread and risk assessment

During the implementation of these researcher conducted thread and risk analysis together with the Control platform development team. Researcher collected information from different sources about cyber security threats that affects into Control Platform type of system. Researcher present different cyber threats and risks for the team and then threats, and risks were classified into different levels by using thread and risk impact and likelihood. Risk method that were used into this exercise was taken from NIST SP 800-30: Guide for Conducting Risk Assessment, figure 5 shows the principle of risk determination.

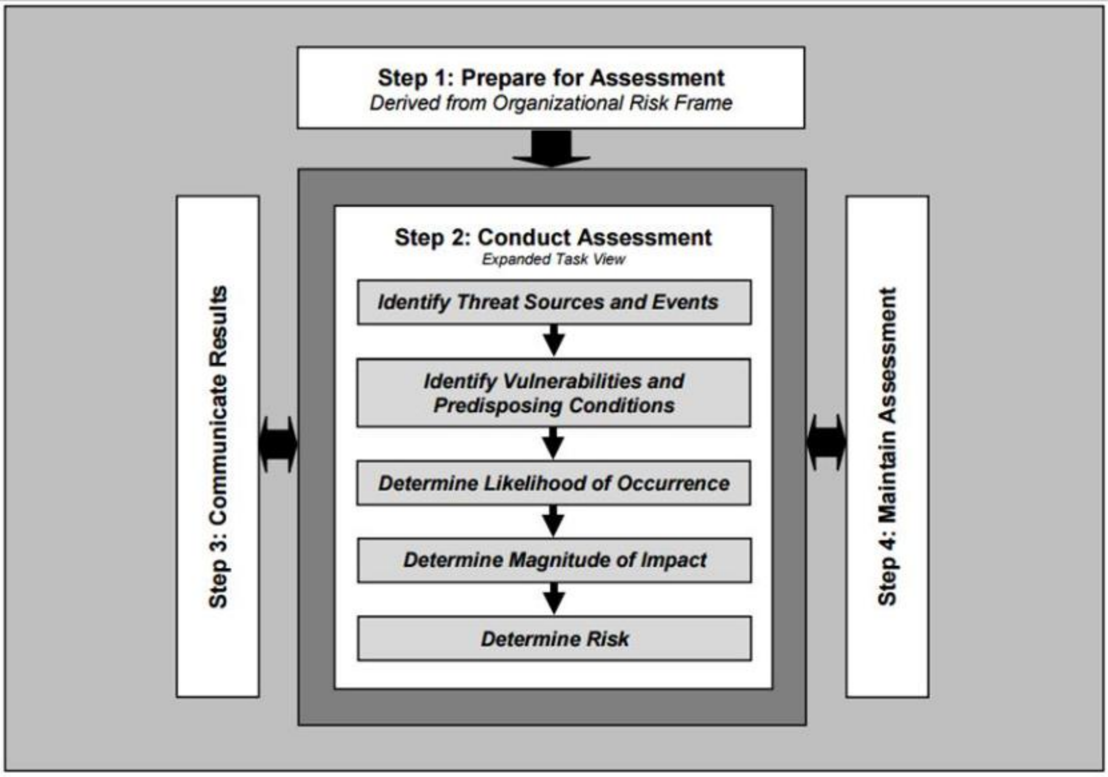

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Figure 5. NIST SP 800-30. Risk determination process (Technology, Guide for Conducting Risk Assessment, 2012)

After threat and risks classification, researcher forms cyber threat and risk matrix. This matrix was used to classify threats and risks into major, mediocre and minor risks. By using this thread and risk analysis method researcher were able to propose correct security controls for preventing cyber security threats and risks.

5. Theme interviews as data collection method

The theme interview is formally located between the form interview and the open interview. The interview does not proceed through precise, detailed, pre-formulated questions but more loosely focused on specific pre-planned themes. A theme interview is one degree more structured than an open-ended interview, as the topics, themes, prepared on the basis of previous research and familiarization with the topic, are the same for all interviewees, although they move flexibly without a strict path. (Hirsjärvi & Hurme, 2018)

The theme interview aims to take into account people's interpretations and their meaning. People are given free speech, although pre-determined themes are sought to be discussed with all subjects. (Hirsjärvi & Hurme, 2018)

A theme interview is a conversational situation in which pre-planned themes are reviewed. The order in which the themes are spoken is free, and not all interviewees are necessarily covered on the same scale. In the interview, the researcher has as short notes as possible on the topics to be addressed so that he or she can focus on the discussion, not on meeting the papers. Topics can be listed with French lines, for example, and you can also create some help questions or keywords to feed the conversation. The theme interview should therefore not be about asking petty questions in the exact order from the paper. The themes and their sub-themes are discussed quite freely. A theme interview is a suitable form of interview, for example, when you want information about lesser-known phenomena and issues (cf. semi-structured and structured interview). (Hirsjärvi & Hurme, 2018)

A theme interview requires careful familiarization with the topic and knowledge of the interviewees' situation in order to focus the interview on specific topics. Content and situation analysis is therefore important in a theme interview. The topics to be covered are selected on the basis of familiarity with the topic to be studied. The research topic and research questions must be changed to the form under study, Operationalize. In addition to considering the questions, the selection of the interviewees should also be considered with consideration: Participants in the study should not be randomly selected by sticking to any walker. People should be selected for research who are expected to obtain the best material on the issues of interest. (Hirsjärvi & Hurme, 2018)

The popularity of a theme interview is based, for example, on the fact that the freedom to answer gives the right to the interviewees' speech. In addition, theme interviews are relatively easy to analyze by theme. However, it is good to keep in mind that the themes set in advance by the researcher are not necessarily the same as the themes that, when analyzing the material, turn out to be essentially structuring the content and research topic of the material. From the theme design of the material, you can proceed to typing. The theme interview material can also be analyzed, for example, entirely quantitatively or by combining quantitative and qualitative. Linguistic approaches are also possible, depending on the research problem. Thus, a theme interview does not need to be analyzed in a particular way, although theme design and typing is a common and logical continuum for that type of interview. (Saaranen-Kauppinen & Puusniekka, 2006)

6. Cyber security basic models

There are lots of security models available, but most common security protection model is CIA triad. CIA Trial contains three elements confidentiality, availability and integrity (figure 6). All these three aspects must be reach for order to say that system under protection is secure.

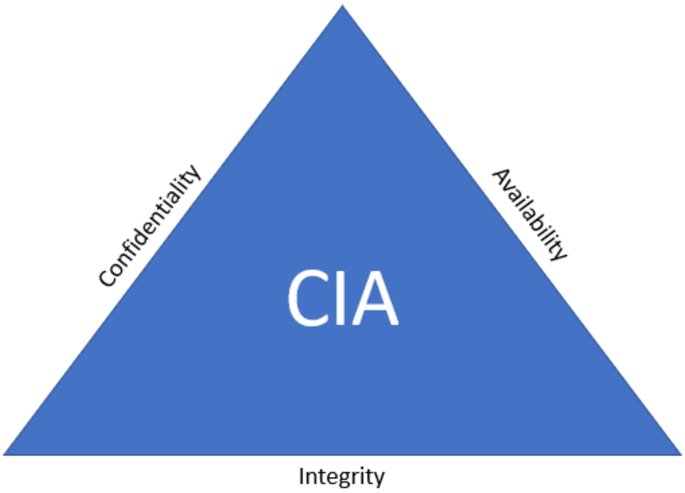


Figure 6. CIA triad and its three aspects

According to (Walkowski, 2019) confidentiality means that only authorized actors have to certain access into data and unauthorized persons are actively prevented from gaining access. Integrity ensures that data is not been tampered and therefore can be trusted. Availability other hand ensures that authorized actors have timely, reliable access to data when then need it.

Another good approach for security is layered security approach so called defense-in-depth which is military model. Layered security means that is one of security layers breached, the second layer is protected and then third, and so on. At this approach all systems are vulnerable at some point of the system lifecycle. These layers may consist from devices, networks, employee training, firewalls, antivirus software, monitoring etc. Figure 7 shows the principle of defense-in-depth model. (Gershwin, 2019)

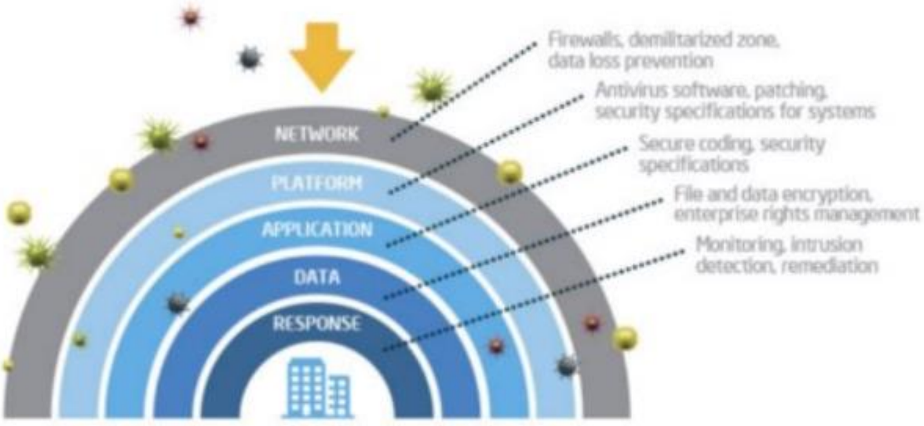

NETWORK
PLATFORM
APPLICATION
DATA
RESPONSE
Firewalls, demilitarized zone, data loss prevention
Antivirus software, patching, security specifications for systems
Secure coding, security specifications
File and data encryption, enterprise rights management
Monitoring, intrusion detection, remediation

Figure 7. Defense-in-depth layered security approach (Gershwin, 2019)

The purpose of the defense-in-depth is to protect the confidentiality, integrity and availability of the network and the data within. Individual protections cannot stop all cyber threats, but together they prevent a wide range of threats and incorporate redundancy if one mechanism fails. This approach significantly strengthens network security against many attack vectors. (Center for Internet Security, 2020)

7. Automotive ethernet security

Automotive industry is ever changing area. Automobile data rates are increasing rapidly because of higher data transfer needs. As data transmission needs grow, new bus technologies are needed to meet the needs. Traditional bus technologies for example CAN and FlexRay are not enough for changing big data amounts. Nowadays automotive industry has taken ethernet in use first at infotainment sector and now been used cross-domain vehicle systems. (N. Fabritius, 2017)

Ethernet has multiple advantages such as easy extensibility and it is widely used at IT sector and IoT systems. But because Ethernet is commonly used, it can be also easily accessed by malicious user, device or software, because of this expandability it makes ethernet based systems vulnerable to cyber security attacks. (N. Fabritius, 2017)

Implementing robust and secure ethernet based system where data buses work separately, independently and with each other, takes time and must be thought through well. In addition to ethernet most systems contain conventional buses at well. When designing ethernet based systems in vehicles, it is very important to follow requirements of different Ethernet standards. In-vehicle systems balancing between security and reliable time response behavior at Ethernet must be though well also. (N. Fabritius, 2017)

7.1 Ethernet problems and solutions

All the Ethernet network members has equal privileges this leads us to some problems: How to detect and ban traffic from members which are going to gain unauthorized access into network? and How to identify and prevent manipulation of network?

Best option for secure network from unauthorized access of network manipulation is divide network into different VLAN segments. Traditionally network ports were assigned to the switches on various VLANs. Newest IEEE 802.1Q standards offers ethernet package tagging capabilities, which can be used to mark ethernet frames and port independent VLAN. (N. Fabritius, 2017)

Logical network traffic separation itself does not prevent the participation of unwanted devices. It only protects the traffic from spying and manipulation. For securing traffic totally from spying and manipulation is to use cryptographic authentication of encryption algorithms. Initially many solutions have focused to secure traffic at upper protocol layers with data formats and standards such as Transport Layer Security (TLS) for TCP connections or Datagram Transport Layer Security (DTLS) for UDP connections. Later on solutions offers more security mechanisms to lower layers of OSI model, figure 8 shows other data securing mechanisms such as IP packet encryption (Layer 3) by using IPSec and securing Ethernet frames (Layer 2) with MACsec (IEEE 802.IAE). These solutions are regulated by industry standards. (N. Fabritius, 2017)

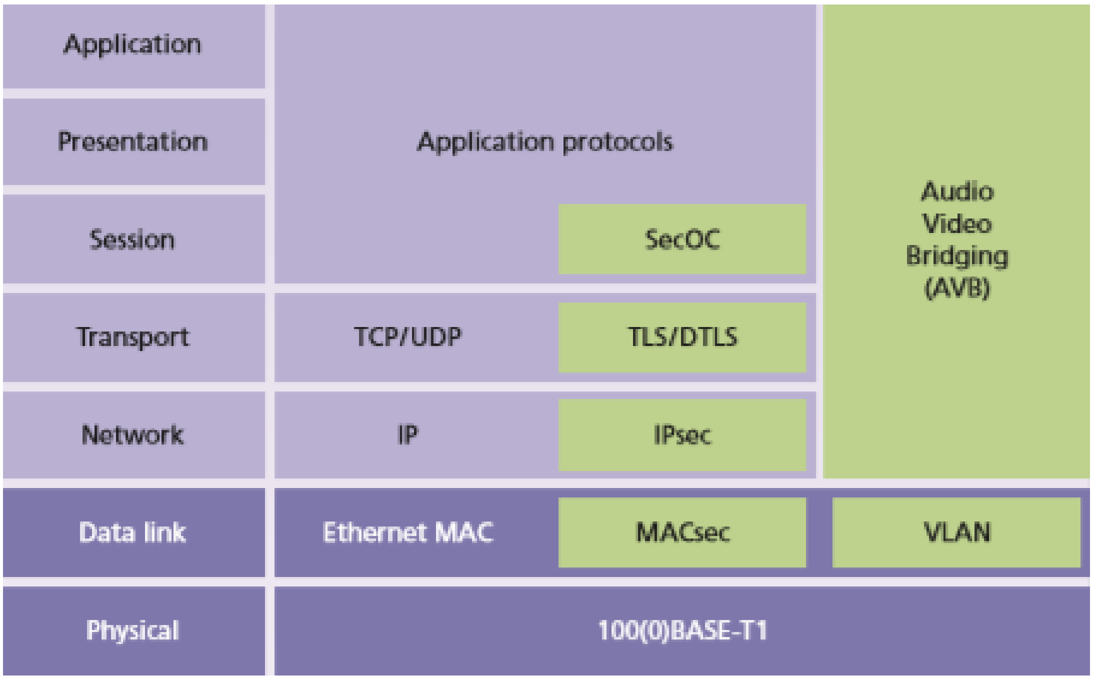


Figure 8. OSI layer and Safety relevant protocols (N. Fabritius, 2017)

Addition to these security methods it also possible to secure components using classic firewalls to filter traffic between different networks. Also, nowadays modern technologies can be used to analyze and evaluate traffic at the fly by investigating network package payloads these systems are called “intrusion detection systems” (IDS) and “intrusion prevention system” (IPS). (N. Fabritius, 2017)

7.2 In-vehicle control system requirements

The number of attacks on embedded devices is constantly increasing, requiring stronger security measures. Embedded systems must also be protected from physical, encryption, software, and network-based attacks.

Embedded controls systems are different when compared to traditional computer systems for example personal computers. Typically, embedded system are smaller or larger devices or systems. These systems are designed to perform a specific task with real-time computing constraints. It is common that embedded systems often lack strong security measures for multiple different reasons for example smaller systems, often results in neglect of security. (Triassic Solutions, 2018)

There is also common misconception that these systems are not vulnerable to attacks by hackers, or that existing security is adequate. The security challenges that nowadays embedded systems face are:

- **Critical functionality** – Embedded systems drive the sophisticated features that modern society relies on. Disruption of these features can have serious consequences.
- **Attack replication** – Embedded systems are produced in mass production. If a hacker manages to attack one of these systems, it is easy to replicate the attack on other systems.
- **Security assumptions** – Previously, embedded systems were built on the assumption that they were not the target of hackers. Today, modern embedded systems include data security for the first time, and no previous experience can be built.
- **Longer file cycle** – The life cycle of embedded systems is usually much longer compared to computers or other consumer devices. A device that should be designed to withstand the safety requirements of the next two decades is a huge challenge.
- **Remote deployment** – Because many embedded systems are used outside of the normal security parameter, these systems can be connected directly to the Internet without security.
  (Triassic Solutions, 2018)

7.3 Examples of ethernet-based control systems and security in them

According to Vector publication about security of connected vehicles solutions (Vector, 2020) security solution requires multiple layers of security. Vector introduced this by layered security concept as seem at figure 9.

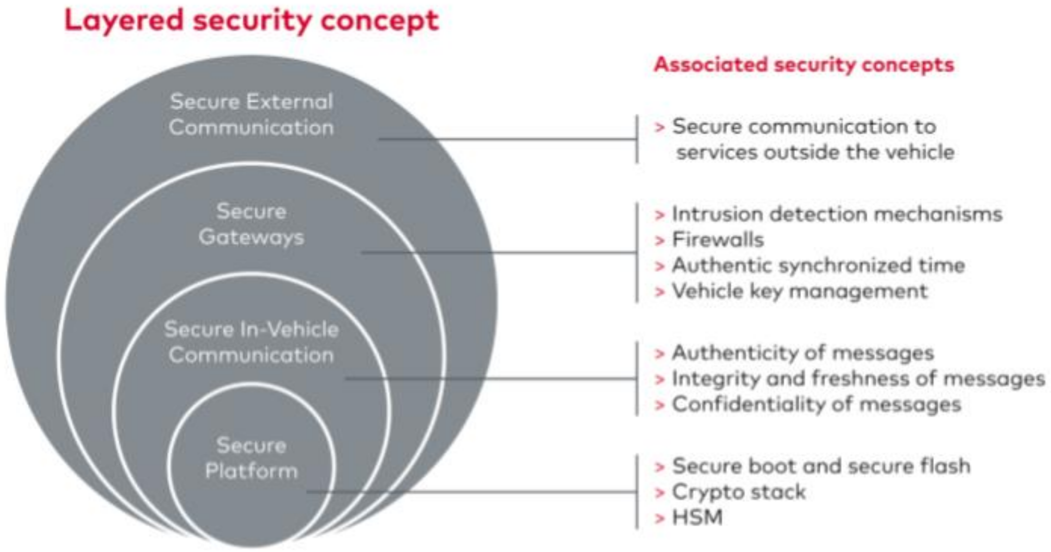

Layered security concept
Associated security concepts
Secure External Communication
Secure Gateways
Secure In-Vehicle Communication
Secure Platform
> Secure communication to services outside the vehicle
> Intrusion detection mechanisms
> Firewalls
> Authentic synchronized time
> Vehicle key management
> Authenticity of messages
> Integrity and freshness of messages
> Confidentiality of messages
> Secure boot and secure flash
> Crypto stack
> HSM

Figure 9. Vectors layered security concept (Vector, 2020)

Layer contains secure platform which contains; secure boot and secure flashing, crypto stack and HSM. Second security layer contains; authentication of messages, integrity and freshness of messages and confidentiality of messages. Third layer of security is security gateways which contains; intrusion detection mechanisms, firewalls, authentic synchronized time and vehicle key management. Fourth layer focus is to secure external communication and this contain secure communication from vehicle to outside world (Vector, 2020)

Vector introduces benefits of the Infineon products which can be used to enable multi-layered security concept. Figure 10 shows basic in-vehicle system architecture of connected vehicle solutions:

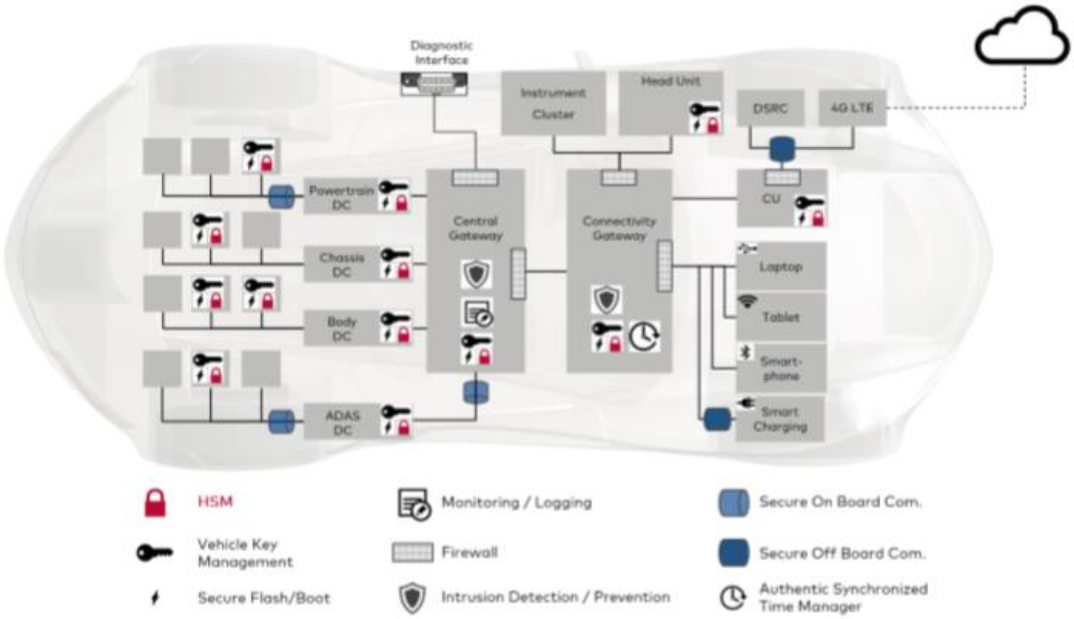
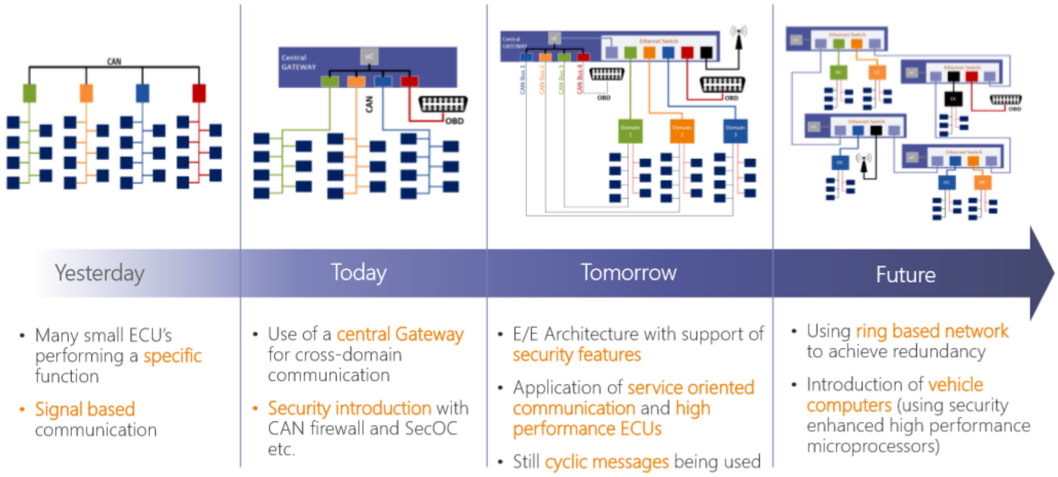


Figure 10. Vector layered security concept achieved by Infineon products (Vector, 2020)

Another interesting report were found from automotive congress 2020 Munich materials were found during research. S. Shukla & R. Jung presented Escrypt material about timeline of security at automotive vehicles. Figure 11 below shows the trend of automotive security development.



Yesterday

- Many small ECU's performing a specific function
- Signal based communication

Today

- Use of a central Gateway for cross-domain communication
- Security introduction with CAN firewall and SecOC etc.

Tomorrow

- E/E Architecture with support of security features
- Application of service oriented communication and high performance ECUs
- Still cyclic messages being used

Future

- Using ring based network to achieve redundancy
- Introduction of vehicle computers (using security enhanced high performance microprocessors)

Figure 11. Trend of security development of automotive (Jung & Shukla, 2020)

Figure 11 displays a timeline from yesterday’s CAN bus architecture where no security measures were introduced into yesterday’s CAN bus based systems. Today’s implementation is to use central gateway for cross-domain connections at these systems CAN firewalls and SecOC systems are used. Tomorrows E/E architecture supports security features by using ethernet switches and domain thinking. At future these solutions are using risk based networking to achieve redundancy and vehicle computers uses security enhanced high performance microprocessors. (Jung & Shukla, 2020).

At same presentation also describes full system overview of intrusion detection systems as seen at figure 12. It is very interesting to see that not only IT systems use these higher level of security controls which can be used to protect attacks even more by introducing the connectivity into backend systems and incident response capabilities to organizations.

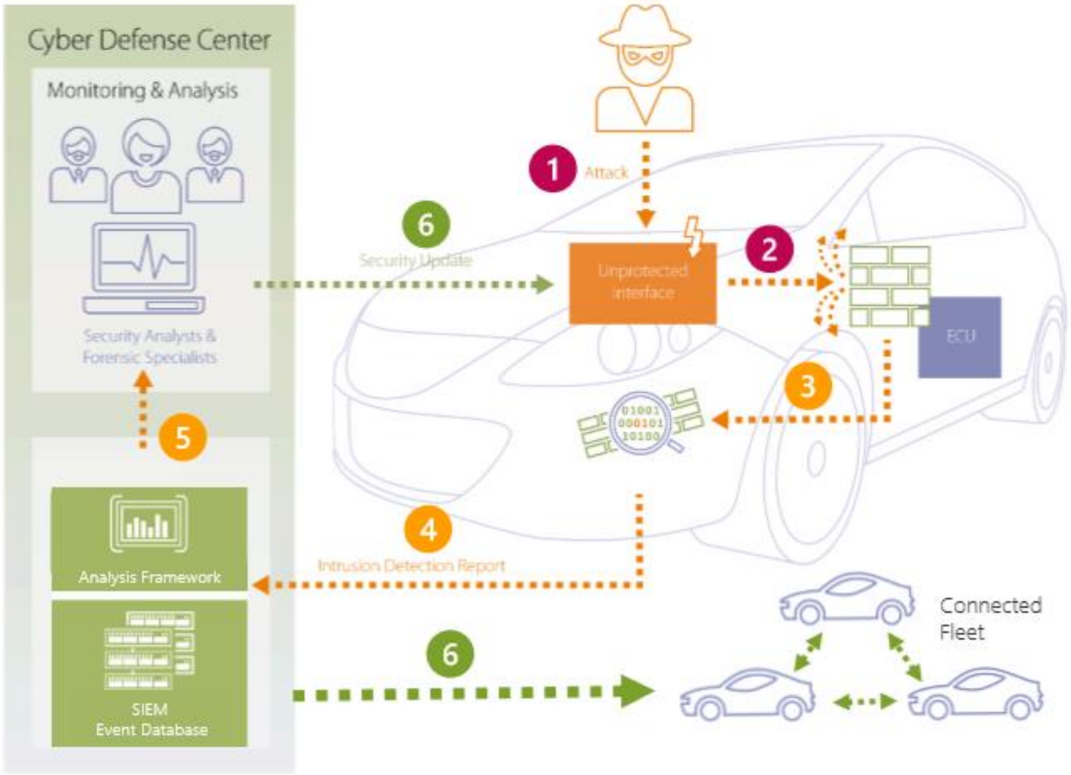


Figure 12. Full intrusion detection system overview (Jung & Shukla, 2020)

7.4 Safety versus security

Automobiles have been designed with safety in mind. However, you cannot have safety without security, if an attacker (or even a corrupted ECU) can send CAN packets, these might affect the safety of the vehicle.” (C Miller, 2013)

Safety and security are often grouped at people minds and they cannot articulate why and how these topics relate to each other’s. Grouping things is people’s natural behavior at situations where areas to discuss has overlapping functions.

Safety and security have a different focus, safety focuses on the proper functioning of a system and therefore worries about risks presented by the passive adversaries, randomness in nature and human-caused accidents of crashes. Security focuses in the system’s ability to resist intentionally malicious action and worries about the risks presented by active adversaries in the form of creative, determined and malicious human beings acting intentionally. (Safety first for automated driving, 2019)

Cyber security has been come one of the challenges of automated driving vehicles because the extreme growing needs of connectivity. This connectivity consists interfaces between control functions of connected vehicles, IT backend systems and other external information sources. These multiple connection points create large attack surface for malicious users with different goals. It is very important that cybersecurity principles and practices are applied to ensure that possible attacker cannot for example arbitrary control of a vehicles movements and that way put people at risk. (Safety first for automated driving, 2019)

When level of automation increases, security measures protecting vehicle functions should defend the system for unauthorized access and system manipulation to guarantee the integrity of the vehicle, its components, and the safe operation of its functions, especially functions that controls vehicles movements. (Safety first for automated driving, 2019)

8. Literature review

The aim of this thesis literature review was to give researcher a wide knowledgement about previous studies relation to target field which is highly automated connected machines. This chapter walks thru the finding about previous researhes, found publication, standards, dirrerent criterias and guidelines.

8.1 Previous found researches

Penttilä Olli investigated Cyber threads in maritime container systems of his Master thesis. The scope of this investigation was to find suitable security control for Kalmar maritime container handling system. (Penttilä, 2016)

(Roepke;Thraem;Wagener;& Wiesmaier) together write a surver of protocols securing the Internet of Things: DTLS, IPSec and IEEE 802.11i. In this survey they write quite good information about securing network communication. This survey is very good source thinging about securing TCP and UDP connections.

Martin Lang investigated (Lang, 2019) securing automotive ethernet at this thesis Secure Automotive Ethernet – Balancing Security and Safety in Time-Sensitive Systems. Martin focuses to investigate vulneravilities of Ethernet out-of-the-box and identifying which vulnerabilities can cause most significant threat conserning the safety of human lives of property.

8.2 Examination of standards and other guidance

Literature review also contains investigation of cyber security standards. During the examination of the standards, it turned out that no direct cyber safety standard was found that was specifically targeted to the needs of mobile work machines.

8.2.1 ISO/IEC 27001

ISO/IEC 27001 Information Security Management standard is part of the widely known standard for information security management ISO/IEC 27000 standard. This standard focuses to provide requirements for an information security management system (ISMS). (ISO, 2020)

8.2.2 ISA/IEC 62443

ISA/IEC 62443 standard specifies security capabilities for control system components. It is a series of standards, which has been developed by ISA99 committee and adopted by the International Electrotechnical Commission (IES). These standards provide a flexible framework to address mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). Following figure 13, shows standard divided into different categories.

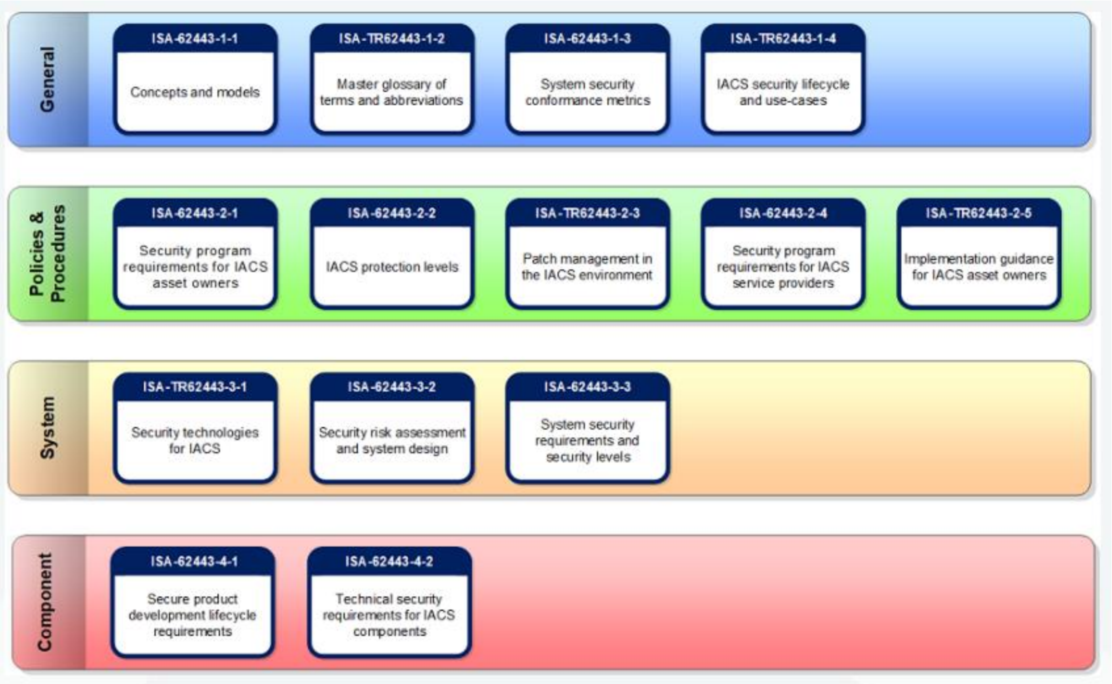

General
ISA-62443-1-1
Concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS protection levels
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Security program requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment and system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Secure product development lifecycle requirements
ISA-62443-4-2
Technical security requirements for IACS components

Figure 13. ISA/IEC 62443 standard family (Apampatzis, 2019)

ISA/IEC describes cyber security as an ongoing process, process that do not has a goal. Standard describes the integration of different components into an industrial environment must be govern by defense-in-depth policies and practices. (Apampatzis, 2019)

8.2.3 ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering

ISO/SAE 21434 is a new standard which is under development at now and first draft version is released at February 2020. It describes the security engineering process in the automotive environments. Because of the trend of greater networking capabilities of vehicles and the focus on embedded platforms. Because of this fact earlier know attack scenarios from IT environment will also threat automotive side. The purpose of the proposed standard is to ensure the systematic development of safe vehicles and to maintain safety for full lifecycle of vehicle. (Angermeire, 2020)

8.2.4 ISO 13849 Safety of machinery

ISO 13849 will contain two individual standards, ISO 13849-1 standard provides safety requirements and guidance on the principles of design and integration of safety-related control system components, including software development. The standard defines the characteristics of these safety-related parts of the control system, which include the level of performance required to perform the safety function. The standard applies to safety-related parts of the control system for all types of machinery in dense and continuous operation, regardless of the technology or energy used (electrical, hydraulic, pneumatic, mechanical, etc.). (SFS, Standardit ja julkaisut - SFS-EN ISO 13849-1, 2020)

ISO 13849-2 standard specifies the procedures and conditions to be followed when applying for approval by means of analyzes and tests of safety-related control system components designed in accordance with ISO 13849-1; defined safety functions, the category achieved, and the level of performance achieved. (SFS, Standardit ja julkaisut - SFS-EN ISO 13849-2, 2020)

8.2.5 CEN ISO/TR 22100-4:2020:fi Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

CEN ISO/TR 22100-4:2020:fi technical report includes instructions for machine manufacturers to consider IT security (cyber security) aspects when implementing machine control systems. Report purpose is to give machine manufacturers a guidance on potential security aspects and relation with safety of machinery. The report provides essential information for identifying and addressing security threats that may affect machine safety. (ISO, 2020)

8.2.6 NIST 800-82 Guide to Industrial Control Systems (ICS) Security

National Institute of Standards and Technology has produced lots of publications relating to cyber security. One of these publications is “Guide to Industrial Control Systems (ICS) Security, this guide provides guidance how to secure Industrial Control Systems (ICS), Distributed Control Systems (DCS) and includes also Supervisory Control and Data acquisition (SCADA) systems and other control system configurations such as Programmable Logic Controllers (PLC). Document provides an overview of ICS and these systems typical topologies, it identifies typical threats and vulnerabilities of these systems, it also provides recommended security countermeasures to eliminate and mitigate associated risks. (Stouffer;Pillitteri;Adrams;& Hahn, 2015)

8.2.7 NIST Cyber Security Framework

NIST Cyber Security Framework is voluntary guidance. It is based on different standards, guidelines and practices for organizations to manage and reduce cyber security risks. Framework consists three main components: The Framework Core, Implementation tiers and profiles (figure 14).

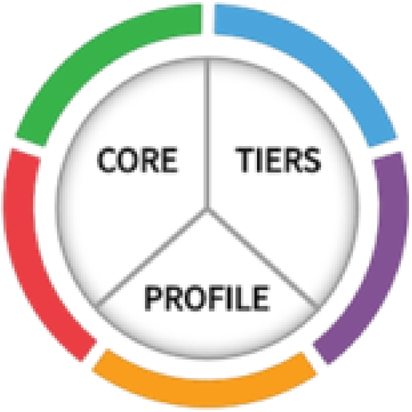


Figure 14. NIST Framework core components (Technology, 2020)

Purpose of Framework core provides common easy understandable language for setting desired cyber security activities and outcomes. Framework implementation tier provides context for organization into cyber security risk management. Framework profiles are used to identify and prioritize opportunities for organization to improve cyber security. (Technology, 2020)

8.2.8 VAHTI instructions

Finnish ministry of finance has published multiple general security instructions for ICT sector for example guide for managing security incidents. This guide is aimed at operators providing services to public authories and public administrators. Aim of the guide is to harmonize and develop security breaches for authories increase co-operation in the management of anomalies and improve in general government information security. (Valtionvarainministeriö, Tietoturvapoikkeamatilanteiden hallinta, 2017)

Another interesting instruction published by Finnish ministry of finance is Change and security the regionalization outsourcing a – a controlled process. This publication addresses the security of outsourced projects and the risks and threats they pose to the outsourcing organization. It provides good guidance and background information for the life cycle of the outsourcing process from an information security perspective (Valtionvarainministeriö, Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen - hallittu prosessi, 2006)

8.2.9 PiTuKri

When implementing cloud services, a good guidance for this is PiTuKri which is published by Finnish Ministry of Transport and Security named Traficom. PiTuKri comes from Finnish words and it is an abbreviation and means cloud security evaluation criteria.

The aim of this criteria is to boost the security confidential information of public authorities in situations where data is processed in cloud services. The criteria are intended as a tool for cloud security evaluation. The criteria have been prepared from the perspective of Finland's national needs. The drafting of national legislation has been considered in the drafting so that the criteria support what was renewed at the beginning of 2020 legislation. In particular, the BSI cloud security criteria, the CSA cloud security community security matrix, ISO270015 and ISO270176 standards, as well as the Katakri criteria. The criteria take a position on both the authority's national classifieds and those classified Class IV confidential information. The criteria also ignore the general principles of protection of classified information at the international RESTRICTED level. (Traficom, 2020)

8.3 Cyber attacks on mobile machines

This section describes cyber threats to mobile work machines. The section compiles a theory of threats that may have an impact on control platform architecture. For mobile work machines, threats to machine safety are the most important, in addition to data security. the aim of this thesis is to find the main threats that can have a negative impact on machine safety.

8.3.1 Denial of Service- and Distributed denial of service attacks

Purpose of the Denial of Service (DOS) attack is to disrupt service normal functionality and prevent other service users from accessing it, this can be achieved several ways. Flooding means sending so much traffic or data that no-one else can use service until malicious flow has been handled. Denial of service attack can also overload service's physical resources to send it so many requests at short period of time this can overwhelm all the available memory, processing or storage space. Some extreme cases, this may even lead to damage of the physical components for these resources. Denial of service attacks can be performed thru multiple communication interfaces. (F-Secure, 2020)

More dangerous version of an individual Denial of service attack is Distributed denial of service (DDOS) attack. Figure 15 describes difference of these attacks.

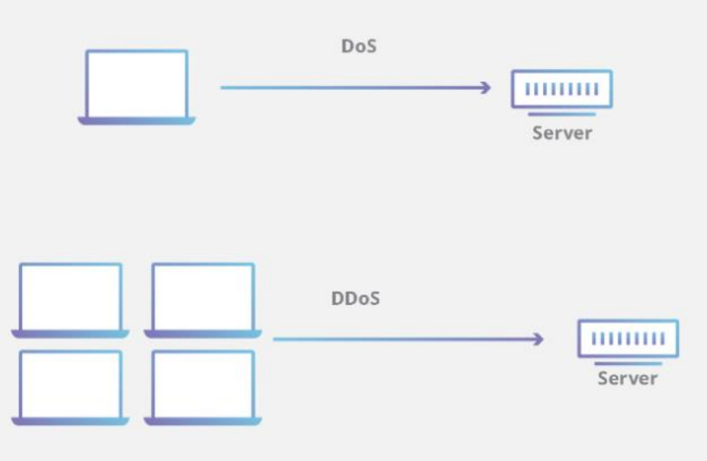


Figure 15. DOS and DDOS attack comparison (Cloudware, 2020)

The main difference is that DOS attack and DDOS is that DOS attack uses single connection endpoint and DDOS attack uses multiple endpoints to when performing attack. Often these attacks come from botnet, botnet is group of computers which have been infected by malware and then malicious user can get control over them. (Cloudware, 2020)

Execution of denial of service attack requires certain level of technical skills and knowledge. Nowadays however cyber criminals can easily to gain access simple programs that can be used to perform DoS attacks and because of this even unskilled malicious user can easily perform attacks. (F-Secure, 2020)

There are some techniques to prevent denial of service attacks, such as:

- **Traffic analysis and filtering**
- **Sinkholing**
- **IP-based prevention**

(F-Secure, 2020)

8.3.2 Reply attack

Reply attack is attack where cybercriminal eavesdrops on a secure network communication, attacker can intercept communication and then fraudulently delays or resends it to receiver. Reply attacks are quite start forward to implement, attacker does not need to have any skills to decrypt message after capturing it from the network, attacker can only just simply resend the whole package. (Kaspersky, 2020)

Best methods for securing systems from reply attack is select correct encryption methods and implement message counter calculation into sender and receiver systems. This means that communication parties use random session keys, which helps to identify is message already handled by communication parties. Another preventative measure for these attacks is to use message timestamping. (Kaspersky, 2020)

8.3.3 Eavesdropping attack

Eavesdropping attack is easy to perform it can be done by a piece of software which is sitting somewhere at network path and listening communication by capturing all the network traffic. Idea is that malicious user passively listens traffic and can use this information later to perform more advantaged attacks such as reply or man-in-the-middle attack. (ScienceDirect, 2020)

The standard defense against eavesdropping attack is cryptography. Cryptographic functions need computing power and because of this this may not be implemented all embedded control applications. (ScienceDirect, 2020)

8.3.4 Data breach

Incident that exposes secret confidential information or protected information is called data breach. Data breach can be intentional of accidental. Cyber criminals can for example hack company database to steal customer confidential information's intentional or employee in that company may accidentally leak information into Internet. (Symanovich, 2017)

8.3.5 Unauthorized Access

Unauthorized access means that when unauthorized person or computer system gain access into organization's data, networks, endpoints, applications or devices without permission. The main cause of unauthorized access is misconfigured or broken authentication mechanisms. (Cynet, 2020)

Common causes for authorized access are weak passwords, social engineering attacks, phishing emails, compromised accounts, insider threats such as privilege leveraging. (Cynet, 2020)

8.3.6 Spoofing

Spoofing is an attack where malicious user, software or device impersonates as another communication partner. Purpose of spoofing is to launch attacks against network hosts, steal data, spread malicious software or bypass access controls. (Veracode, 2020)

Most common spoofing attacks are:

- **IP address spoofing attack** – Attacker sends IP packages from faked or spoofed address to victim. This can be used to bypass IP-address-based authentication.
- **ARP spoofing attacks** - As an ARP spoofing attack, a malicious member must have fake ARP messages over the LAN to link the attacker's MAC address to the legitimate member's IP address. This type of spoofing attack results in data destined for the host's IP address, all of it sent to the attacker
- **DNS server spoofing attacks** - In a DNS server spoofing attack, the malware changes the DNS server to reroute a specific domain to another IP address. (Veracode, 2020)

8.3.7 Man in the middle attack

Man-in-the middle attack requires three communication parties. Sender, receiver and attacker. The attacker's goal is to interrupt the flow of the message between the parties involved in the communication. There are 7 type of man-in-the-middle attacks

- **IP address spoofing attack –** Every ethernet device is capable to connect by using IP address. At IP spoofing attacker tries to trick victim to this that he or she is discussing with receiver.
- **DNS spoofing –** DNS Spoofing is technique that forces victim to connect fake resource than real one. The attacker's goal is to drive traffic from the actual site or capture the user's login information.
- **HTTPS spoofing** – At HTTPS spoofing attacker's goal is to fool browser to believe that it is visiting a trusted website. By using this attacker can monitor website traffic and possibly steal information that victim is sharing.

- **SSL hijacking** – At SSL hijacking attacker uses another and secure server and intercepts communication between server and victim's computer.
- **Email hijacking** – At email hijacking attack attacker has access to email communication between victim and sender. Attacker can alter senders' message by spoofing.
- **Wi-Fi eavesdropping** – At this attack attacker wants to victim to connect this wifi endpoint to for example steal credentials, payment card information and other confidential information.
- **Steal browser cookies** – A browser cookie is small piece of information that website often store into computer. Cybercriminal can steal these session browser cookies and possible to access victims' passwords, address and other confidential information.

  (Norton, 2020)

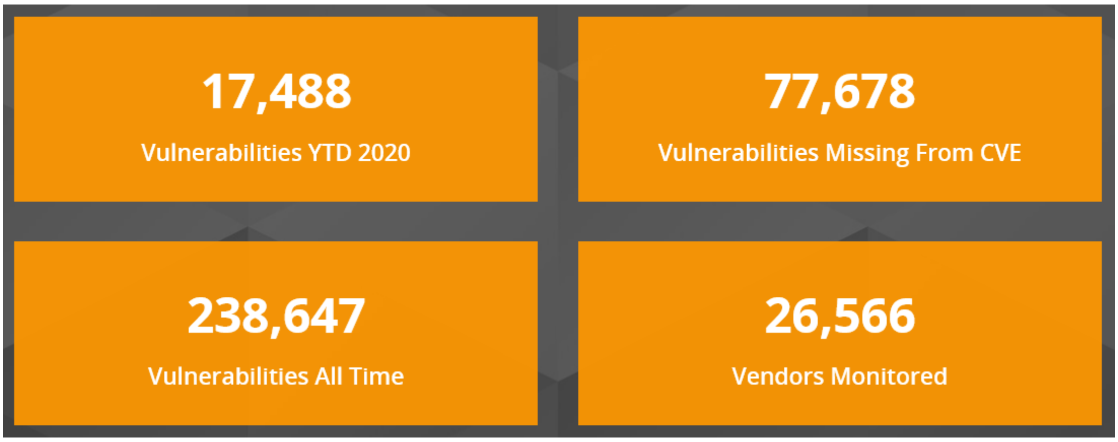
8.3.8 Software Vulnerabilities

Software vulnerability is a flaw, weakness or glitch at software of operation system. All software systems include vulnerabilities. Here is list of some available software vulnerabilities and attacks:

- **SQL injection** – By using SQL injection attacker can inject malicious code by using SQL statements into database based applications.
- **OS Command injection** – The attacker can execute OS commands if data is not checked correctly.
- **Buffer overflow** – Buffer overflow occurs when program tries to add data in the buffer more than its capacity allows. This leads memory overflows, programs crashes, data corruption and even cause execution of malicious code.
- **Uncontrolled format string** – This vulnerability happens when user input is not checked, this may crash systems or lead to execution of malicious code.
- **Integer overflow** – Happens when number calculation attempts to increment an integer values which is higher than integer variable which stores calculation result.

  (Mohanty, 2018)

Nowadays information systems contain lots of software. Vulnerabilities are big problem around the globe at different software vendors. Figure 16 shows vulnerability statistics that has been get from VulnDB cyber security analytics page.



17,488
Vulnerabilities YTD 2020

77,678
Vulnerabilities Missing From CVE

238,647
Vulnerabilities All Time

26,566
Vendors Monitored

Figure 16. VulnDB statistics (Risk Based Security, 2020)

Zero-day vulnerability is vulnerability at software that hackers can exploit to compromise programs for penetrating networks, gain unauthorized access to sensitive data. Vulnerability is called zero-day when there is not yet fix from software vendor and the vulnerability can be exploited by malicious actors. (Cybersecurity Help, 2020)

8.3.9 Hardware Vulnerabilities

Hardware vulnerability is a weakness at computer systems that can be exploited and enables attack through physical or remote access into system. These could be unexpected flaws in operations that allows attacker to gain access into system to execute code or elevating privileges. Hardware vulnerabilities could not be exploited by random hacking attempts, these targets are often known as high-value systems and organizations. (TechTarget, 2020)

8.3.10 Malicious software

Malware is a piece of software that can be downloaded, installed or unknowingly purchased. Malwares that exploits network vulnerabilities has continuously rising since 2009 as we see at figure 17. (Firch, 2020)

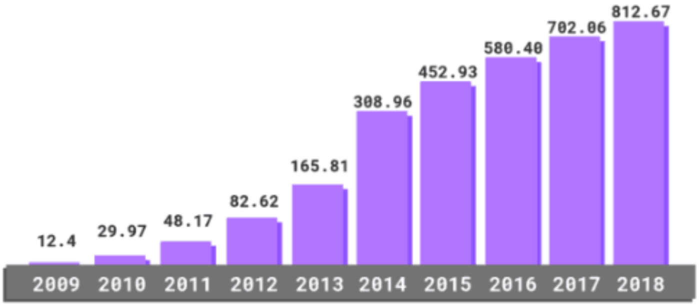


Figure 17. Total malware infection growth (millions USD) (Firch, 2020)

Most common types of malwares are:

- **Virus** – commonly known malware, which needs end user actions to infect system. Viruses can spread to another system by using email, instant messaging, website downloads, removable media such as USB and thru network connections.
- **Keyloggers** – can log user's keystrokes and send data to threat actor. These are often planned to steal passwords or other sensitive data.
- **Worms** – are quite similar as viruses, it can spread at same way as virus, but is do not need host file or program to run malicious code. Worms are commonly used to hack web- and mail servers and databases.
- **Trojans** – is a program that is disguised as legit software. Trojans often hide their existence and are activated when called, trojans can steal sensitive data and enable backdoors into infected systems. Trojans cannot replicate them shelves as viruses and worms can.
- **Ransomware / Crypto-malware** – are designed to lock legit users our of systems or deny access into data until ransom is paid. Crypto malware is a ransomware that encrypts user files and requires payment at certain time to be paid and often requires ransoms as digital currency as Bitcoins.
- **Logic bombs** – are malwares that will activate when triggered. Triggers could be specific date/time or example 25th logon on account of system.

- **Bots/Botnets** – Botnet comes from words roBOT NETwork, it is a group of bots which are any type of computer systems whose security is compromised. Botnets are commonly used for performing DDOS attacks.
- **Adware & Spyware** – Adware is designed to serve annoying harmless advertisement of screen example thru web browser. Spyware other hand is type of malware which is designed to do harm like gain access and damage computer systems.
- **Rootkits** – are back door programs that attacker can use to command and control infected system without user knowing. Some antivirus software can detect rootkits, but they are difficult to remove from the system. Many cases best options is re-install compromised system.
  (Firch, 2020)

8.3.11 Social engineering attacks

Social engineering attacks has been come very popular attack methods. Last years these attacks have increased significantly and has been one new business for hackers. Common factor for social engineering attacks is that in order to attack reach it’s goals human effort is needed at some point. (Firch, 2020)

Here is a list and explanation of some most common social engineering attacks:

- **Social engineering attack** – occurs when for example attacker calls for victim and pretends to be legit third party and ack some confidential information from victim directly.
- **Phishing emails** – is a scam where user is tricked to provide sensitive information such as username and password, download of opening an application or transferring money. Goal of phishing attack is to create false trust into victim.
- **Spear phishing** – attacks are very similar as phishing attacks, but they are designed to use victim’s personal information and to get victim click some sort of link. Also, these attacks are disguised as contacts requiring urgent action.
  (Firch, 2020)

8.4 Security controls for mobile machine

This chapter contains list of security controls that are widely used by automotive industry and associated with Control Platform architecture what this thesis studies. Automotive industry can be thought as a leader at this field because it is very strictly regulated, because any vulnerability in vehicle control systems can lead fatal results in case of cyber-attacks.

8.4.1 Network segmentation

Network segmentation is an architectural approach that divides a network into several segments or subnets, each operating as its own small network. Segmentation utilization allows administrators to manage the flow of traffic between subnets based on granular practices. Organizations use segmentation to improve monitoring, improve performance, locate technical issues and most importantly improve security. (Paloalto, 2020)

Security personnel then can utilize powerful tools which can prevent unauthorized access in case of malicious attackers getting access into valuable assets like corporate financial records and highly confidential intellectual property or customers personal information. For understanding security usage of network segmentation, it is vital to first consider concept of network security trust. Nowadays organizational assets are often spread across multi-cloud- or hybrid environments, public- or private clouds and software defined networks (SDNs). In these situations, all these networks needed to secure against attacks. (Paloalto, 2020)

8.4.2 Ethernet secure switches, routers and firewalls

According to (Escrypt, 2020) automotive ethernet solutions of secure switches and routers seems to be very new area of security controls at automotive industry. Many of ethernet-based E/E solutions does not yet use powerful security controls such as firewalls and routers, but in future many manufacturers has seen that firewalls and routers plays key role of security in the future. For example, Escrypt's CycurGate product is the firewall solution for ethernet communication, it offers protection against denial-of-service attacks and enforces permitted Ethernet communication into domain structure.

At January 2020 New-Tech Europe (New-Tech Europe, 2020) published an article about NPX accouchement of new ethernet switch NXP SJA1110 for time sensitive networking (TSN). At security point of view this switch has following security features; hardware assisted secure boot, denial-of-service prevention and distributed intrusion-detection capabilities. NXP SJA1110 switch validated every Ethernet frame that is reaching the ECU by validating it against HW-based security rules which collect statistics and can trigger escalations if rules are not met. These mechanisms are the basis for building best class intrusion detection systems and firewalls.

8.4.3 TPM & HSM

Hardware security module is a primary tool used for securing modern vehicles. It is used to secure to secure cryptographic keys and a secure connection environment for (cryptographic) operations. HSM ensures authentication and integrity of the platform and it adds extra line of defense to protect sensitive data, which is often called "Security in Depth". HSM can be placed into separate chip for the CPU or into same chip as CPU. (Petri, ym.)

The TPM can be implemented both on its own chip and using firmware in a secure environment on a so called System-on-Chip (SoC) system. TPM 's offer important aspect in a virtual based approach or firmware based, which serve chain of trust between device boot stages. Figure 18 shows example architectural overview of virtual TPM and its boot sequence. These devices can be used to implement so called "secure boot" or "verified boot", for ensuring Boot ROM hardware immutability. (Petri, ym.)

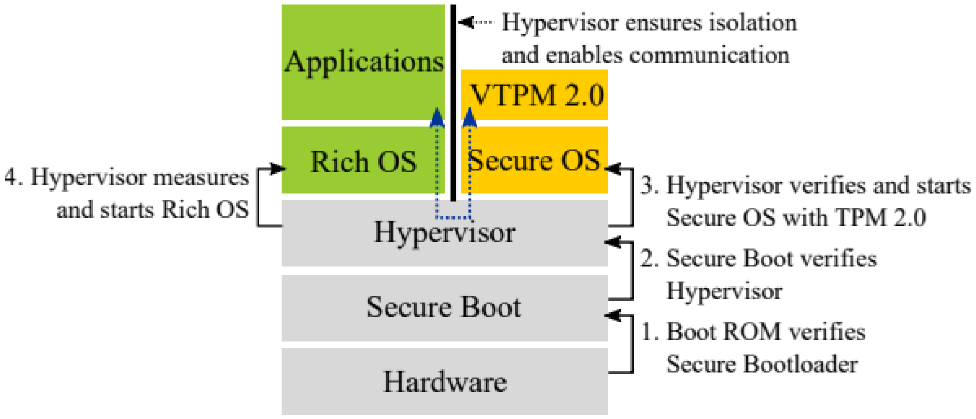

Applications
Hypervisor ensures isolation and enables communication
VTPM 2.0
Rich OS
Secure OS
4. Hypervisor measures and starts Rich OS
3. Hypervisor verifies and starts Secure OS with TPM 2.0
Hypervisor
2. Secure Boot verifies Hypervisor
Secure Boot
1. Boot ROM verifies Secure Bootloader
Hardware

Figure 18. Virtual TPM and its boot sequence (Petri, ym.)

TCG publication about TCG TPM 2.0 Automotive Thin Profile presents conceptual model for Automotive-Rich- and Automotive-This profiles, and present two types of TPMs that could be suitable for automotive vehicle deployments. One approach is to that Head unit or Gateway that communicated directly into public Internet uses rich capabilities (Automotive-Rich) and processing power and other ECUs which has limited processing, networking and application functionalities uses this capability (Automotive-Thin). Figure 19 shows conceptual model of Automotive-Rich and Automotive-Thin approach. (TCG, 2018)

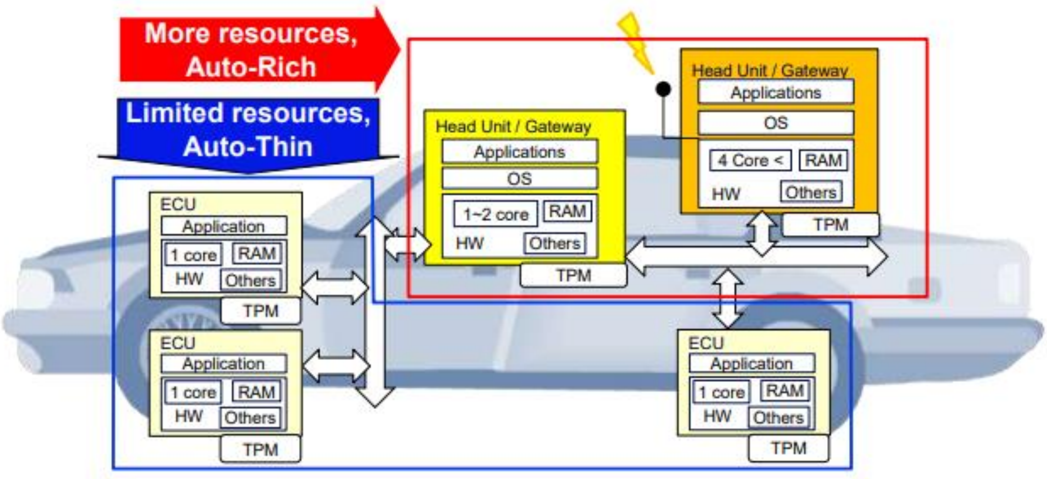


Figure 19. Automotive-Thin and Automotive-Rich conceptual model in a vehicle (TCG, 2018)

8.4.4 CAN devices security controls

CAN (Controlled Area Network) is common bus technology used at vehicles. Protocol does not contain direct support for secure configurations. (Lin & Sangiovanni-Vincentelli, 2012) made a research and proposition of CAN security mechanisms which can prevent cyber-attacks such as reply and masquerade. According this research main challenges of CAN is its limited bandwidth (500kbps) and therefore identifying sender MACs would require splitting MACs into two of multiple different frames. This would degrade communication performance because increasing bus utilization. Another challenge is that CAN is missing global time.

(Lin & Sangiovanni-Vincentelli, 2012) security proposal contains three elements which are described as following:

- **ID table** – each node contains the node ID of the sender and a list of possible receivers.
- **Pair-wise symmetric secret keys** – a pair-wise key Ki,j so called "shared secret" that is used for authentication. Each node pair contains this secret information that is not used by any other node pair. By this way any other node is not able to alter node pair communication.
- **Message counters** – is used to replace missing global time and prevent reply attacks. Each node will maintain the set of counters and each counter corresponds to a message. When using this approach any malicious node messages can be checked the corresponding receiver counter is valid.
  (Lin & Sangiovanni-Vincentelli, 2012)

(Lin & Sangiovanni-Vincentelli, 2012) proposes that this security proposal can be used for retro-fit CAN protocol to protect it from the cyber-attacks such as reply and masquerade. And based on the experimental study results security proposal can achieve high security level without high communication overhead to message latencies and bus load.

8.4.5 Hash-based message authentication code

At 2019 (Yang;Liu;Xu;Wu;& Xu, 2019) made research about Automotive Ethernet security based on Encryption and Authentication Method. At this research they studied AES-128 and HMAC-SHA1 security authentication methods and technologies into vehicle Ethernet systems. These methods efficiently prevents external intrusion and data hopping and improves network security performance of automotive Ethernet that is used at car bus networks.

HMAC is (Hash-based Message Authentication Code) is consists of an internal hash and external hash. HMAC requires hash function and a key K. Figure 20 shows flow diagram of the HMAC algorithm.

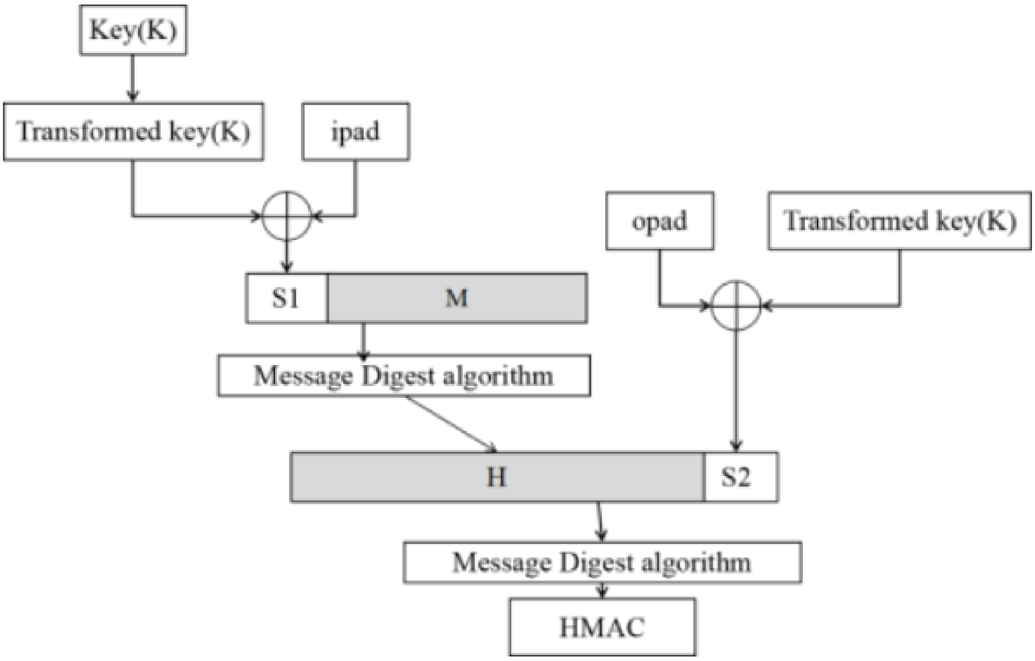


Figure 20. HMAC processing flow chart. (Yang;Liu;Xu;Wu;& Xu, 2019)

According to RFC 2104 HMAC is the tool for calculating message authentication codes by using secret key and cryptographic hash function. HMAC can be used as combination with any type of integrated hash functions. MD5 and SHA-1 are one examples of hash functions. (Krawczyk;Bellare;& Canetti, 1997)

8.4.6 Bluetooth security

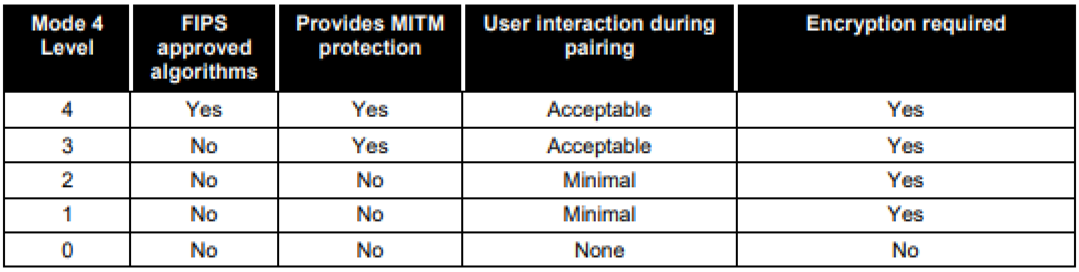
Bluetooth devices security depends very much about used Bluetooth modes and versions. Bluetooth specifications lists several security modes, each version of supports some of these security modes, but not all. Security initialization differs lots of between modes. Some modes have a configurable security level setting which of course affect security of the connections also. (Padgette, ym., 2017)

NIST Special Publication 800-12 lists three different recommendation for Bluetooth security:

- Organization should be using strongest Bluetooth security model that is available for their devices
- Organizations should address Bluetooth wireless technology in their security policies and change the default settings for Bluetooth devices to match the policy
- Organizations should ensure that their Bluetooth users are informed of their security responsibilities with respect to Bluetooth use.
  (Padgette, ym., 2017)

Publication also lists these Bluetooth modes and their capability to prevent cyber security attacks. Following table 2 shows these five levels for mode 4 and their security configuration:

Table 2. Bluetooth devices security configuration options for mode 4



Mode 4 Level	FIPS approved algorithms	Provides MITM protection	User interaction during pairing	Encryption required
4	Yes	Yes	Acceptable	Yes
3	No	Yes	Acceptable	Yes
2	No	No	Minimal	Yes
1	No	No	Minimal	Yes
0	No	No	None	No

(Padgette, ym., 2017)

8.4.7 Wireless LAN security

Wi-Fi is a wireless computer networking technology. Wi-Fi uses 2.4 GHz UHF and 5 GHz SHFISM radio bands. The Wi-Fi Alliance defines a Wi-Fi connection as any "wireless" Local Area Network "(WLAN) product based on Electrical and Electronics Designers (IEEE) 802.11 standards. Wi-Fi connections are more vulnerable than physical Ethernet, because attacker do not need to physical connection into network. (International Journal of Scientific Engineering and Technology Research, 2016)

Wi-Fi connections can be secured by multiple ways. Here is list of common security measures:

- **Change default passwords** – many network devices including wireless access points are pre-configured at the factory for easier access. Changing default passwords makes hackers harder to access devices.
- **Restrict access** – allow only known users to access into network. MAC address filtering is efficient way to allow only legit devices connect into network.
- **Encrypt network data** – wireless networks uses many data encryption protocols such as WPA, WPA2 or WPA3. WPA3 is the newest and strongest encryption protocol available. Other protocols leaves network open for exploits.
- **Protect SSID (Service Set Identifier)** – protect SSID for hiding it, this makes attackers more difficult to find wireless network name.
- **Use Firewall** – host based firewall will add extra layer of protection to the data on computer

(Cyber security & infrastructure security agency, 2020)

8.4.8 IDS/IPS systems

Two most popular approaches for the tools for securing network communication are network firewalls and intrusion detection and intrusion prevention systems. Infosec article which (Yadav, 2020) writes describes very clear how IDP/IPS systems can be used to prevent network based cyber security attacks.

Intrusion detection (ID) is a process for monitoring and identifying unauthorized access or manipulation of systems. Purpose of the ID systems is to gather data from different areas of computer or a network and analyze them to identify security breaches which includes misuse and intrusions. Misuse focus is to identify attacks from the organization and intrusions focus is to identify attacks from outside of the organization. Figure 21 shows basic principle IDS/IPS systems. (Yadav, 2020)

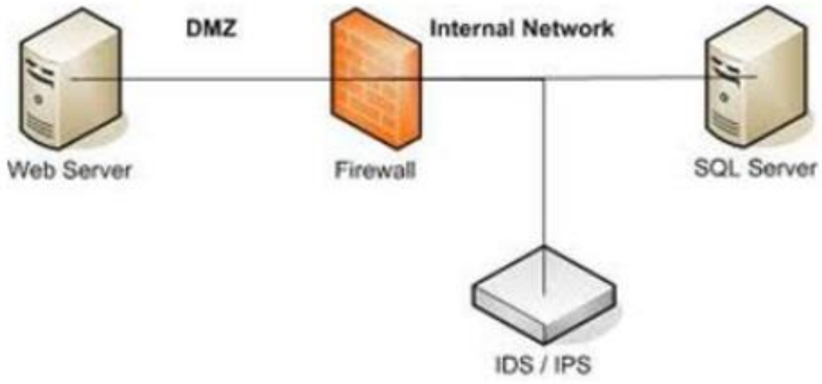


Figure 21. Example of IDS/IDS system connected to the network. (Yadav, 2020)

There are several types of IDS systems available

- **Network intrusion detection system (NIDS)** – is an independent system that identifies intrusion by investigating network traffic and monitors multiple hosts. In a NIDS, sensors are located into network choke points such as DMZ and network borders. Sensors collect all network packages and analyzed their content to find malicious traffic.
- **Host-based intrusion detection system (HIDS)** – in a HIDS agents are installed into HOST systems which recognizes intrusions by analyzing system calls, application logs, file-system modifications such as binaries, password files, capability databases, ACL lists and so on.
- **Perimeter intrusion detection system (PIDS)** – works at the fences of the critical infrastructure and monitors malicious activity. If a system detects intrusion, then it triggers alarm.
- **VM-based intrusion detection system (VMIDS)** – is used to monitor malicious activity at virtual machines side, by using VMIDS is possible to deploy intrusion detection systems into virtual machines.
  (Yadav, 2020)

All IDS/IPS systems uses one of the detections techniques:

- **Statistical anomaly-based IDS** – statistical anomaly detection is based on the known network traffic and uses it as baseline of detection. When statistical analysis detects malicious activity that differs from baseline then it triggers an alarm.
- **Signature-based IDS** – signature based detection is based on preconfigured and predetermined attack patterns as known as signatures. At good protection these signatures must been constantly updated to mitigate threats.
  (Yadav, 2020)

Firewalls and intrusion detection systems relate to network security. Firewall blocks traffic between networks by investigating rules that has been configured and do not give alarms. IDS systems can detect malicious network traffic also at inside network, block malicious activity and alert about it. (Yadav, 2020)

8.4.9 Software updates and patching

Software updates are very critical part of security point of view. New vulnerabilities are discovered all the time in the world around different systems. If software’s are not updated for long time they can considered as vulnerable systems, cyber criminals probably has hundreds and thousands of ways to hack systems. (Kochetkova, 2016)

Because of this for example Windows systems vulnerabilities are known widely and they can be exploited at any vulnerable unpatched system. So at the security point of view highest priority of updates are system updates along with other bug fixes in production systems. (Kochetkova, 2016)

Pathing is the process for fixing security vulnerabilities from the network and endpoints. Patch management is key to ensuring patches are deployed correctly into endpoints and network devices. One of the top drivers for security breaches are unpatched software’s or devices. Leaving critical vulnerabilities unpatched is like leaving your home front door open. (Willis, 2019)

8.4.10 Endpoint security

Software Firewalls

Windows 10 includes security tools which contains multiple tools such as virus & threat protection, account protection, firewall & network protection, app & browser control and more. Windows Defender can be used to block and allow inbound and outbound connections. (Reddy, 2020)

Linux distributions contains iptables firewall which can be used to configure network traffic filtering rules by defining rules at IP, port or protocol level. Network packages can be accepted, rejected or dropped. Firewalld is newer approach for network traffic filtering for Linux, it supports categorizing traffic into different zones. Firewalld makes rule configurations easier to specify services by using the name of the service rather than using ports and protocols. Another good improvement is that it can be used at interactive modification of rules that can tested and previous configuration can be returned easily. (Reddy, 2020)

Antivirus software

Antivirus programs are designed to find out known viruses, worms and other malicious software from the system. It is a good protection for known threats. The effectiveness of antivirus software depends a lot on whether it is up to date. Many antivirus programs rely on a database or library of known viruses which they use to compare programs on the system. If antivirus program finds a malicious program it immediately places it to quarantine area and deletes it from original location. Users can the decide to restore or delete malicious programs from the quarantine area. (The Ohio State University, 2020)

Some antivirus manufacturers uses predictive analysis and artificial intelligence at their products which can be able to detect new malicious programs. These systems focus is to detect malicious programs based on what it does, and do not use traditional database approach to identify known threats. (The Ohio State University, 2020)

Least privileges principles

Idea behind the least privilege’s principle is that any user, program or process should only have minimum necessary privileges to perform it actions. It also referred to as the principle of least authority (POLA) or the principle of minimal privilege (POMP). These privileges can be considered a best practice at information security. (Lord, 2018)

According to Digital Guardians article (Lord, 2018) there are several benefits of the principle of least privilege such as; better security, attack surface minimization, limited malware propagation, better stability and improved audit readiness. Principles of least privilege can be applied to every level of the system. Here are some examples of the principle of least privilege:

- **User Account with Least Privilege** – According to the principle of least privileges, an employee whose task is to enter data into a database only needs the ability to add records to that database. If the malware infects that employee's computer, the malicious attack is limited to making database entries. However, if that employee has administrator privileges, the infection can spread throughout the system.
- **MySQL Accounts with Least Privilege** – MySQL installation follows the principle of least privileges when it uses multiple accounts to perform unique tasks. Ideally, the online form that allows users to sort data should use a MySQL account that has only sorting rights. In this way, an attacker who takes advantage of the format has only gained the power to sort the records. Inversely, if an account is authorized to delete records, an attacker could now wipe the entire database.
- **Using Just in Time Least Privilege** – A user who rarely needs root permissions should work with limited permissions for the rest of the time. To increase traceability, that user can retrieve administrator credentials from the password store as needed. The use of single-use credentials tightens security, which is achieved just in time with the least privilege.
(Lord, 2018)

8.4.11 Hardening

Purpose of hardening is eliminating all possible attack vectors and reduce risks as much as possible. Typically, this can be done by removing all non-essential software programs, interfaces and utilities from the computer operation system. (Sharpened Productions, 2020)

By utilizing hardening practices organizations can rely that devices are secure, and safe from malicious actors. One of the strongest hardening practices is to install security updates and patches into systems as fast as possible to removing vulnerabilities from networks and endpoints. (Willis, 2019)

Protecting endpoints has become the most important task in modern information systems. Nowadays endpoints are key route for entry into network, in the past most data breaches were involved network itself.

8.4.12 Logging and SIEM

Logs are very important part of security is log collection and analysis. Logs are messages that computer systems generates often all sort of software and hardware generated some king of logs. Logs can often contain audit information such as audit records, audit travels and event logs. Logs are not itself the Important part, but analyzing logs is the important part of security. (Watts, 2018)

Security incident and event management (SIEM) goal is to improve security and provide knowledge for system administrators about overall security of the systems. SIEM approach is the real-time analysis and connect systems in order to inform security analysist about current security situation. (Watts, 2018)

8.4.13 Communication protocols

This chapter contains theory of different communication protocols that are related into system security what this thesis covers.

IPsec

IPsec is group of communication protocols that are used together to established encrypted connection between devices. Its purpose is to keep data secure that travels thru public networks. IPsec is commonly used by VPN connections. (Cloudflare, 2020)

Many of VPN connections uses IPsec protocol suite to encrypt communication between devices. Not all VPN connection use IPsec, another approach is to use TLS/SSL encrypted VNP connection this operated at different level at OSI model layer. (Cloudflare, 2020)

VPN can used to different modes, IPsec tunnel mode and IPsec transportation mode. IPsec tunnel mode is used between two dedicated routes, both of the routers are acting one end of virtual “tunnel” through a network. At IPsec tunnel mode, original IP header which contains final destination is encrypted, at addition to package payload. For telling router where package is heading IPsec adds a new IP header. After this at end of the tunnel another router decrypt the IP header and delivers packages into final destination. (Cloudflare, 2020)

In IPsec transportation mode, each package payload is encrypted, but original IP header is not encrypted. After this intermediary router are able to see the final destination of each package. (Cloudflare, 2020)

SSL, TLS and HTTPS

SSL (Secure Sockets Layer) is a standard technology for keeping an internet connection secure and safeguards sensitive data that is transmitted between two systems. It prevents malicious users for accessing data at any way. SSL uses encryption algorithms for scrambling data in transit. (DigiCert, 2020)

TLS (Transport Layer Security) is improved version of SSL. It works pretty similar way as SSL, using encryption to protect the transfer of information and data. For guarantee the authenticity and integrity of all messages transferred thru network, SSL and TLS protocols also contains authentication process using message authentication codes (MAC). (DigiCert, 2020)

Websites uses HTTPS (Hyper Text Transfer Protocol Secure) for securing connection with SSL certificate. This ensures that malicious user cannot have eavesdrop or alter data transmitted between browser and server. Figure 22 shows differences between HTTP and HTTPS communication. (Tip Top Security, 2017)

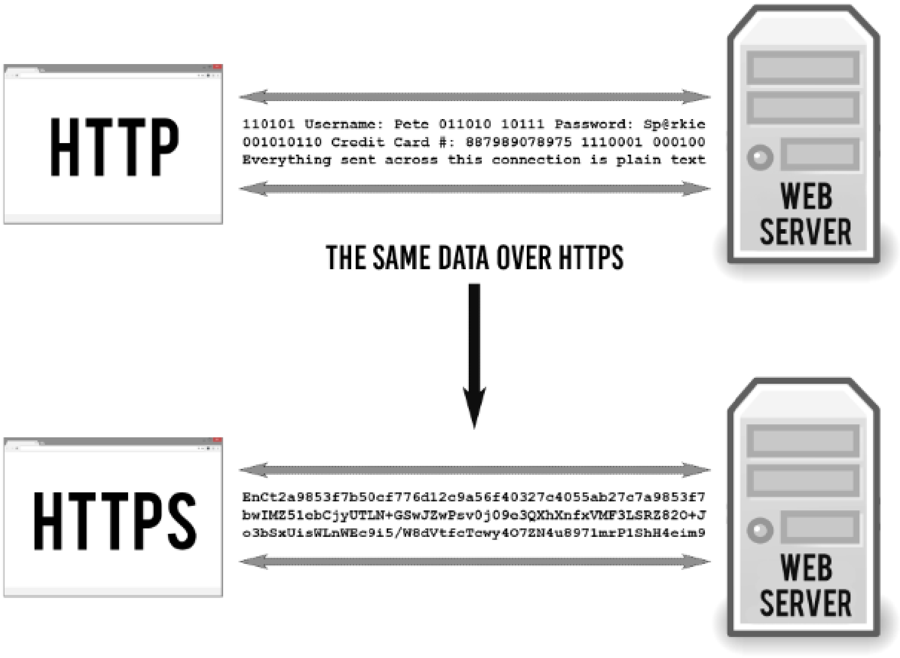

HTTP
110101 Username: Pete 011010 10111 Password: Sp@rkie
001010110 Credit Card #: 887989078975 1110001 000100
Everything sent across this connection is plain text
WEB SERVER
THE SAME DATA OVER HTTPS
HTTPS
EnCt2a9853f7b50cf776d12c9a56f40327c4055ab27c7a9853f7
bwIMZ51cbCjyUTLN+GSwJZwPsv0j09c3QXhXnfxVMF3LSRZ820+J
o3bSxUisWLnWEc9i5/W8dVtfcTcwy4O7ZN4u8971mrP1ShH4cim9
WEB SERVER

Figure 22. Data transmission difference between HTTP and HTTPS (Tip Top Security, 2017)

DTLS

DTLS (Datagram Transport Layer Security) is a protocol based on TLS it is capable of securing the datagram transport (UDP). UDP datagram suits well for securing communication between applications and services that rely delay-sensitive communication. (F5, 2020)

Protocol ensures secure connection between client and server, it can be used to prevent eavesdropping, unauthorized access or message tampering. However, this protocol has also vulnerabilities at 2012, when vulnerability called Heartbleed was discovered. This vulnerability effects widely TLS and DTLS protocols, but this is fixed now at OpenSSL version 1.0.1g. (Cristina, 2020)

SSH

SSH (Secure Shell) is a software package that enables secure communication method for system administrators and file transfers over insecure networks. It is very widely used at every data center and every large enterprise. (SSH Communications Security, Inc, 2020)

Protocol uses encryption to ensure secure connection between server and client. User authentication, commands, outputs and file transfers are encrypted to protect against network attacks. Figure 23 shows basic steps between client and server at SSH connections. (SSH Communications Security, Inc, 2020)

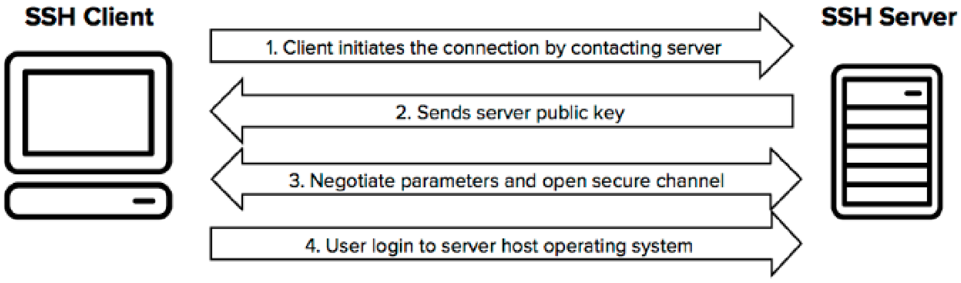

SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

Figure 23. Steps of SSH connection between client and server (SSH Communications Security, Inc, 2020)

SFTP

SFTP (Secure File Transfer Protocol) is a secure file transfer protocol. It runs top of SSH protocol. SFTP protocol has protection against password sniffing and man-in-the-middle attacks, it protects data integrity using encryption and cryptographic hash functions and authenticates client and server. (SSH Communications Security, Inc, 2020)

9. Processing of results

This chapter processes the main results of the thesis.

9.1 Theme interview analysis

Theme interview was conducted at may 2020. Researcher interviewed 9 persons from different positions at Ponsse and Epec. This section discusses the results of the thematic interviews one theme at a time. Summary of the results from the theme interviews can be found at appedix 1.

The interviews revealed that the desire to develop information security can be found in both organizations, the importance of information security has been identified and it is desired to start investing in it. In some products, the level of security is in good shape, but the need for improvement was identified. Several assets to be protected were identified, in mobile work machines Machine safety is very important and must not be compromised due to a cyber-attack. Security methods have been made in previous products, but never in Automotive Ethernet-related products.

The purpose of the interviews was also to find out the knowledge of the experts regarding product development and maintenance processes. In product development, good practices in terms of information security were identified, such as static code analysis and equipment hardening. However, there were differences in these practices between companies. The development of this section was particularly hoped for.

When asked about the cyber security standards or cybersecurity models interviewed, knowledge and know-how was limited. Only one of the organizations had the intentions to implement the information security management standard ISO 27001 and standardize operations to comply with it.

9.2 Literature review results

As a summary of available cyber security standard. These is not specified standard for non-road vehicles such as forest machines. Even these standards contain lots of valuable information that can be used to implement best parts of these standards to create secure non-road vehicles control system and create own model for Ponsse's and Epec's needs for control system side.

At the side of the ICS security researcher investigated two suitable security framework ISA/IEC 62443 standard and NIST 800-82 Guide to Industrial Control System (ICS) security. Both of these frameworks contains lots of information about securing ICS systems and are closest ones when thinking about securing mobile connected machines.

During the literature review researcher found CEN ISO/TR 22100-4:2020:fi report which is a guideline for machine manufacturers. It describes security relations into machine safety and provides information and guidance to take account cyber threats during control systems development. It instructs machine builders to conduct risk assessments during product development, recognizing cyber threats and risks, and taking these threats into account when developing security-critical systems.

When thinking about cyber security management and developing secure products it is quite important to have all processes inside the organization good shape and order. For achieving this goal, a comprehensive cyber security management system should be in place. Researcher investigated NIST Cyber Security Framework and ISO/IEC 27001 that would be very good guideline for management of cyber security at organizations. Management plays very important role for every organization and with good management and their decisions to invest in security is the only way create safer products to customers.

Also, if we think overall situation about machine manufacturing, behind the scenes there is always development and maintenance processes that should be secured also. ISA/IEC 62443-4-1 standard for Secure product development lifecycle and NIST Secure Development Framework (SSDF) were found to be useful and interesting at this point.

During the literature review researched used guide a lot of time to investigate different cyber security threats and risks which are possible by mirroring the Control Platform architecture. Security control were also investigated for eliminate these threats. Multiple threats, attacks trees were also analyzed to get knowledge of threats severity and likelihood.

After theme interviews and literature review, the researcher investigate various models secure development models that would be utilized to take cybersecurity into account at product development phase. This work appendix 7 contains basic principle of secure development lifecycle model that describes things that should take account during development phase.

9.3 Risk and thread assessment results

At august 2020, researcher stated to investigated Control Platform architecture it's threats and risks, investigated suitable IVN security controls and conducted a risk analysis of potential threats of Control Platform. During this phase lots of architectural drawing were done and Control platforms network architecture were arranged into different security zones after this security control proposals were done to help threat assessment analyzing.

After summer every risk and threat were introduced for Control Platform work group. Risks and threads were classified by following instructions at NIST's 800-30 Guide for Conducting Risk Assessment. All risks were classified according to occurrence and impacts, after classification researcher created risk and threat matrix to group threats and risks to different levels: highest, mediocre and low.

The formed risk and threat matrix can be found from appendix 5. After risk matrix were conducted researcher estimated cyber security risks impact relation to machine safety risks with cooperation at product safety engineer. The following subsections discuss describes the impact of listed cyber threats on the security of the target system.

9.3.1 Attackers motivation to attack on mobile machines

According to J. Desjardins publication at 2018 in Visual Capitalist web pages "*Why Hackers Hack: Motivites Behing Cyberattacks".* Hackers had many different motives figure 24 shows main motives of attacks and patterns.

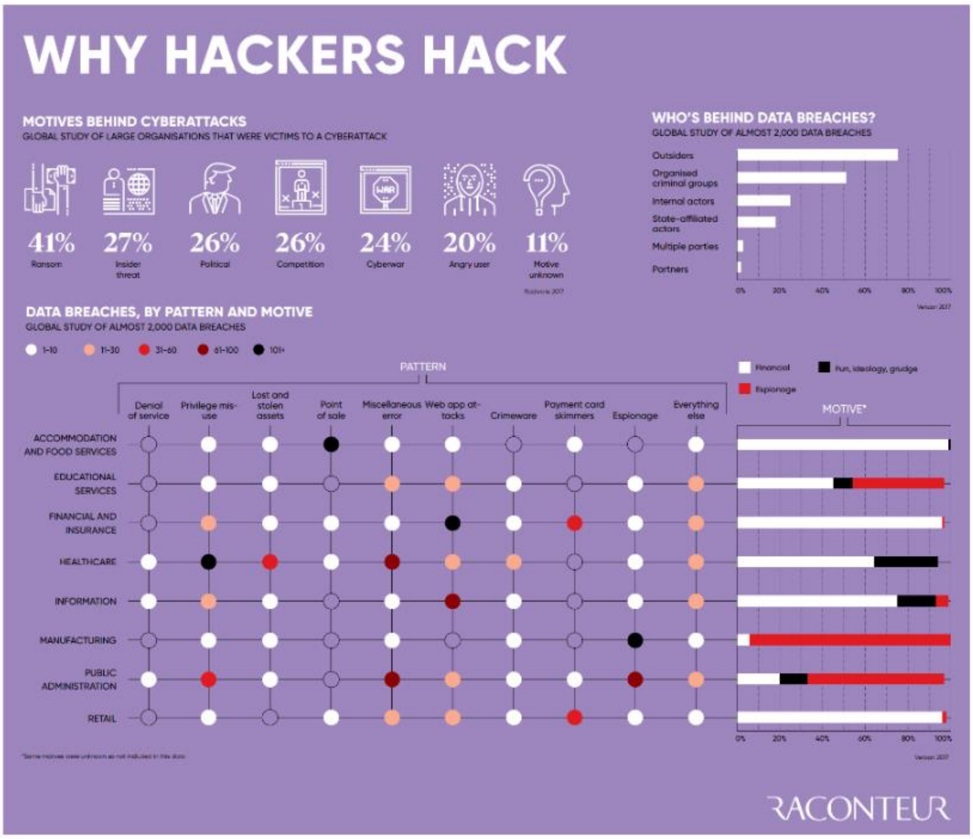


Figure 24. Why attackers perform attacks (Desjardins, 2018)

If we think highly automated connected machines such as forest machines. They are naturally pretty safe from cyber-attacks that are coming from public network, but nowadays digitization and connectivity into back-end office systems or cloud solutions brings this threat factors into reality. Attackers could have multiple motives to attack forest machines. Generally, first motive of attackers is money or course and we could think that all available insecure systems would be easy targets to attackers gain some money for example using ransomware attacks for blackmailing machine owner. Forest machines are tools for machine entrepreneurs and their money income is depending the availability of machine, if systems breakdown in case of cyber-attacks, entrepreneurs would not be able to create products such as cutting wood and therefore this instantly leads money loss of entrepreneur. Also, at these situation entrepreneurs would need assistance from machine manufacturer such as Ponsse or Epec to reinstall current control systems components, and this will lead money loss of machine manufacturer because of maintenance effort to help customers.

Another aspect and motive of attackers would be for example different activists or activists' groups that would like to prevent machine to fell and cut forest. Activists could try to attack against individual machine of machine fleet by using different methods such as, remote connection options WLAN, Bluetooth, or denial-of-service attacks by using public internet where machine is connected into.

Thirds possible motive of attacker would be for example espionage attacks performed by competitors of Ponsse and Epec, according to picture 26% of attacks are performed competitors or hackers that competitors has paid money to perform attacks. Competitive is hard nowadays when companies tries to gain market-share of total markets. Espionage is common not maybe in Finland, but other countries this could be very common situation and competitors follow each other's products, technological developments and seek to benefit from this information themselves.

The fourth motivation for the attack could be intentional harm, for example by tampering with the machine's output data and thereby lead to erroneous output data that is noticed either in the machine manufacturer's systems or, in the worst case, at the sawmill to which the timber is delivered. This can lead to situations where forest machines can be banned and again in these cases the fee lies with the machine manufacturer.

Attackers motives are different, and we can just imagine different motivates of attackers. But reality is that we cannot know all motives and we be aware the there are lots of different actors that could do harm to Ponsse's and Epec's systems so better option is to prepare and take cyber security issues in the table and create feasible counter measures to prevent these threats and risks.

9.3.2 Safety related cyber security risks

Biggest safety issues occur if attacker gains access into Control Platform primary network and can communicate with devices that are controlling ex. machine hydraulics. Ways of getting access into primary network would be ex. social engineering or phishing attack via machine operator and then infecting machine with malicious software and continue attack SSH credential theft or exploiting SW vulnerabilities. After gaining access into primary network attacker could send malicious control messages between core unit and gateway units could lead to serious dangers for example crane could move, harvester head could open or close. Sudden movements of the machine can cause dangerous situations to machine operator or outside properties ex. buildings. Attacker could reply machine control messages, alter control system communication performing man-in-the-middle attack or cheat control system devices by impersonating another device by performing spoofing attack.

Second aspect of safety issues can occur if control system components availability decreases for example situations of denial-of-service attacks. Control Platform architecture contains many connection interfaces such as Ethernet, CAN, GPS, WLAN, Bluetooth, 3G/LTE. Mainly all of these connection interfaces has own vulnerabilities relating to denial-of-service attacks these attacks are pretty straightforward to implement and under heavy load this could slow down control system devices communication or lead to crashes and because of this situation these can be considered at safety risks.

It is common for operational technology solutions that software patches and critical security updates are not patched often, lifecycle of these products are quite long and over a time system security goes down when new vulnerabilities are discovered. Attacker could exploit these known vulnerabilities ex. scanning machine network and find OS vulnerabilities and possibly get access into systems and at worst case scenario get access into primary network.

Control Platform formed by centralized control system architecture, where central embedded device contains all intelligence for moving machine via gateway slave units. Architecture biggest problem at security point of view is all connectivity interfaces inside Core unit, most vulnerable interfaces are WLAN-, BT- and 3G/LTE-interfaces. For example, adding extra secure switch of firewall to protect primary network functions will not help if attacker gets access into core unit by exploiting vulnerabilities of these interfaces. Modern automotive industry solutions have been taken this into account, by moving all vulnerable interfaces away from vehicle control system side by adding firewalls and secure switches to gain safer network topology and segmentation.

Another aspect of security vs safety at future is control system devices at secondary network such as lidar and other radar or camera solutions. These technologies will be used to sense machine surrounding and use their data and inputs to control machine in the future. At future also GPS attacks could harm machine location data availability or integrity, this may lead issues where machine thinks that it is some specific location at map, but location data is not available, or data is altered. These threats should be considered thru when level of automation and autonomous machines are developed. In the future, as the level of automation of control systems increases and possibly also to ensure the remote operation of machines, the information security of the 3G / LTE network connection must also be considered.

9.3.3 Data security related cyber security risks

The Control platform project will produce a unified new generation centralized control system for the Ponsse's and Epec's needs. In mobile work machines, data protection is important. In general, the data traveling on the bus and devices does not contain, for example, personal data or other confidential information. In work machines, moving data is usually related to machine control data, such as various actuator control commands.

The data generated by the machines is usually transferred by various external data transfer devices such as a mobile phone or a USB stick. Data is also transferred to cloud services via 3G and LTE networks. Output data is important, and its accuracy must be able to be preserved during data transfers. Machine entrepreneur gets payment from forest company according to machine production data. Therefore, data protection must be implemented in the machine's internal information system and data transfer into external information systems.

Most of the threats and risks described in the risk matrix (appendix 5.) have a negative impact on the integrity and confidentiality of machine production data, if no security controls were implemented in the Control Platform.

9.3.4 Human to machine related cyber security risks

The actions of the machine user will have a major impact on information security if security controls are not implemented in the Control Platform. In the control system, the machine operator has an OptiPC computer. OptiPC is a Windows based computer that is connected to the internet. The machine operator can be used to assist in attacking the target system, for example by sending the user a fishing email with malware attached, or the machine user can get lost on the Internet to a malicious site from which malware can spread to the machine. And more common scenario is that machine operator attaches USB into system that contains malicious software and that way infect machine.

Various security controls should be implemented to avoid these threads or block them out, such as up-to-date antivirus software, Windows security updates & patches and non-administrator user accounts. Correct security controls are the best way to stop these threads. It is also very important to inform the machine users such as machine operator and machine maintenance personnel about the various security threats and how they spread into computer systems.

9.4 Cyber security management models investigation results

According to the article of Cyber Experts, processes, practices and technologies are needed when security organizations critical infrastructure from cyber-attacks. Companies should understand essence of the different cyber security frameworks for enhancing security of the company. (Mutune, 2020)

Field of cyber security contains lots of different frameworks and guidelines. When thinking about cybersecurity management system (CSMS) or information security management system (ISMS) two most used frameworks are ISO 27001 and NIST Cyber Security Framework. Best option to improve cyber security at research point of view is to start following these guidelines and frameworks. This can be done to implement practices that NIST Cyber Security framework offers. NIST framework forms from five major aspects: Identify, Protect, Detect, Respond and Recover (as seen at figure 25).

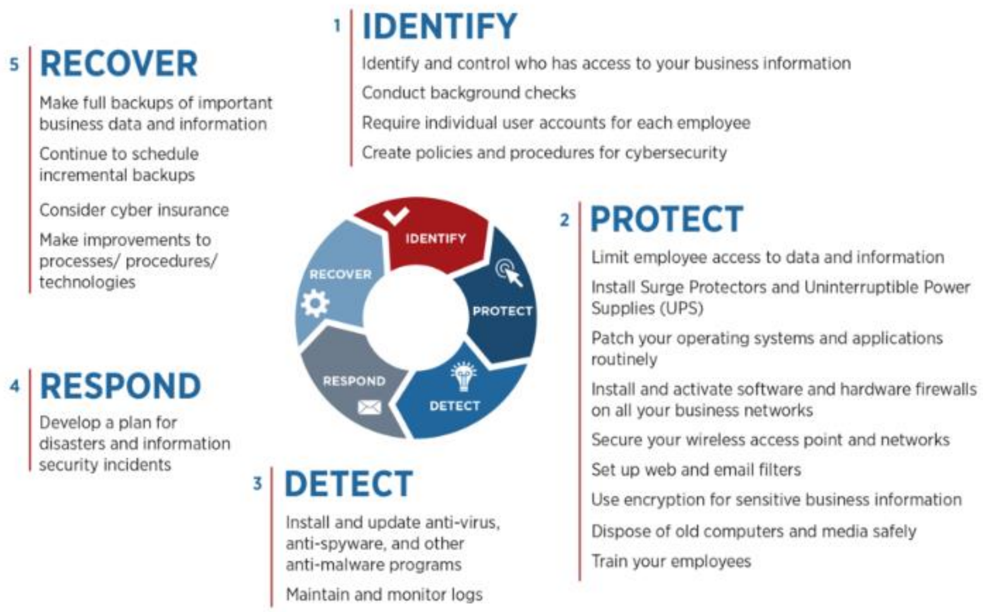

1 IDENTIFY
Identify and control who has access to your business information
Conduct background checks
Require individual user accounts for each employee
Create policies and procedures for cybersecurity
2 PROTECT
Limit employee access to data and information
Install Surge Protectors and Uninterruptible Power Supplies (UPS)
Patch your operating systems and applications routinely
Install and activate software and hardware firewalls on all your business networks
Secure your wireless access point and networks
Set up web and email filters
Use encryption for sensitive business information
Dispose of old computers and media safely
Train your employees
3 DETECT
Install and update anti-virus, anti-spyware, and other anti-malware programs
Maintain and monitor logs
4 RESPOND
Develop a plan for disasters and information security incidents
5 RECOVER
Make full backups of important business data and information
Continue to schedule incremental backups
Consider cyber insurance
Make improvements to processes/ procedures/ technologies
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Figure 25. NIST Cyber Security Framework (National Institute of Standards and Technology, 2018)

NIST Cyber Security Framework is designed to reduce risks, it gives wide range of view of organizations capability to improve cyber security risk management. Framework also reflects multiple industrial standards, guidelines and frameworks such as ISO 27001 information security management standard, ISA/IEC 62443 standard for security of industrial automation and control systems and more. NIST Framework collects information from different standards and guidelines and brings it a one single package of information.

Another approach is to introduce security management standards such as ISO 27001. It is widely used standard all over the globe, many organizations use it as a backbone for implementing standard way to manage cyber security at organization level. Standard describes requirements for information security management system such as: protect organization employees and customers information’s, efficient risk management, compliance archiving and protect company’s brand image (as seen at figure 26).

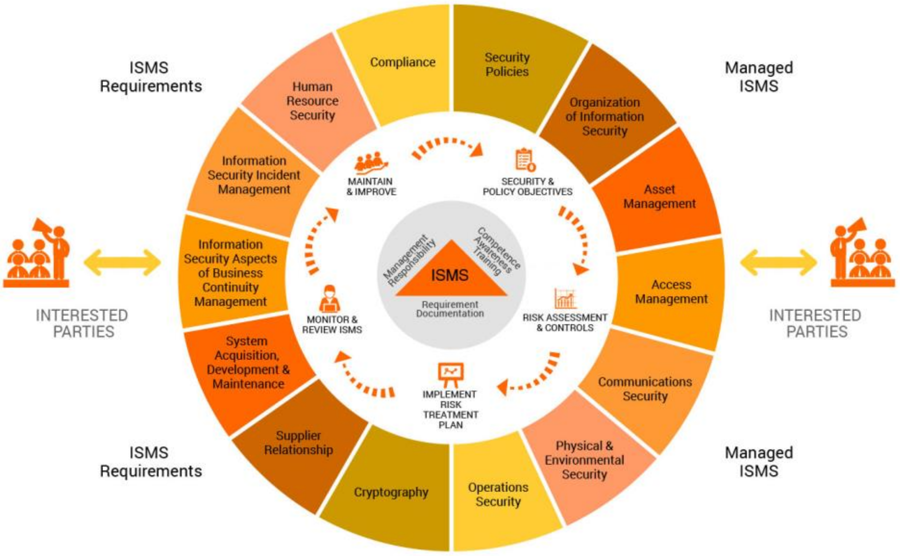

ISMS Requirements
Compliance
Security Policies
Managed ISMS
Human Resource Security
Organization of Information Security
Information Security Incident Management
MAINTAIN & IMPROVE
SECURITY & POLICY OBJECTIVES
Asset Management
Information Security Aspects of Business Continuity Management
Management Responsibility
Competence Awareness Training
ISMS
Requirement Documentation
Access Management
INTERESTED PARTIES
MONITOR & REVIEW ISMS
RISK ASSESSMENT & CONTROLS
INTERESTED PARTIES
System Acquisition, Development & Maintenance
IMPLEMENT RISK TREATMENT PLAN
Communications Security
Supplier Relationship
Physical & Environmental Security
ISMS Requirements
Managed ISMS
Cryptography
Operations Security

Figure 26. ISO 27001 organizations information security management (SBSoft, 2020)

ISO 27001 follows a risk-based process that requires companies to take action to detect security threats affecting their information systems. ISO 27001 standard recommends various security controls to address and identify threats. ISO 27001 lists total 114 controls which are categorized into 14 different categories. (Mutune, 2020)

10. Thesis results

This chapter reviews the models that were investigated during the study and opens up their applicability to the target industry. Models are very important when discussing about cyber security management. Many different processes are needed for comprehensive cybersecurity management. It is not enough to make secure products from a purely cyber security perspective. In cyber security management, the activities of an organization must also be considered as a whole, because modern threats also threaten the organization from the inside and outside.

10.1 Defence in depth model and processes around it

This chapter answers this thesis research question one, which were "How control systems of mobile machines and their In-Vehicle Network communication should be constructed in order to make it safe from a cyber security point of view? "

Today's world is changing all the time, more and more devices for the Internet and device collection as data is utilized in a variety of applications such as output data reporting, proactive maintenance, remote measurement, remote control, and many other purposes. Connectivity to the outside world from a device or machine exposes the machine to cyber attacks. Many manufacturers have not taken this issue due to the fact that no connections were originally needed in the products, devices or machines.

Information systems consist of overlapping and parallel subsystems, such as hardware, networks, access points, operating systems, software, and libraries and components. Various vulnerabilities in these partitions open up opportunities for hackers to use these vulnerabilities to attack your system. Therefore, the protection of information systems must be considered as a whole, in which the selected security controls form a whole and bring a layered thinking to the protection of the system. Layered data security is called the Defense-in-depth model.

In the security of information systems, the first thing to identify is the assets to be protected, which in mobile work machines is the data produced by the work machine, as well as the people who use the work machine. In the event of a cyber attack, the work machine must not endanger human life in any way. There are three things you need to be able to ensure in securing communication between information systems and these are; data confidentiality, data availability and data integrity.

When developing information security, it must also be taken into account that the protection of one information system may not be enough. Often an information system consists of several systems, for example from the point of view of mobile connected machines, the machine data can be transferred to the back-end systems in the cloud service, from where it is stored in a database, and through this the data can also move to other external systems. Information systems will eventually be used by many different parties in their own operations, which is why information security must be thought of holistically, this holistic thinking is referred to as the chain of trust.

In addition to the external threats to the system, the comprehensive development of information security also includes internal threats, which can be, for example data leaks and phishing of information from the company's internal systems. Consider, for example, a situation where a company's product development leaks encryption keys for communication in use in an information system in production, or system admin passwords. This information leakage is not only a problem for the company, but it also endangers the company’s customers who use the information system. For this reason, the company's internal processes and operations must also be strongly managed, consistent and secure in terms of information security at all stages of the process.

The last and very important thing to consider is that once the desired level of security of the systems has been achieved and the appropriate security measures have been implemented, the level of security needs to be constantly monitored and developed to maintain the desired level of security. Much of the security vulnerabilities are due to the fact that critical security updates to the systems have not been deployed to the systems and thus allow for various cyber attacks. Maintaining and developing information security is an eternal path that must be traveled so that threats and risks do not arise and the level of security can be maintained.

Appendix 9 of this thesis contains a description of the defense-in-depth model created in this work. The model seeks to describe aspects of holistic cybersecurity management that should be considered in product development activities at Ponsse and Epec.

10.2 In-vehicle-network security model

This chapter answers this thesis research question two, which were “*What are possible attack vectors/interfaces and what security controls should implemented to secure IVN?*“

Cyber security is the comprehensive identification of threats and risks and the response to them through various security controls. The Control Platform system project that is the subject of this study includes a wide variety of connections and interfaces to internal system functions as well as external actors. This section describes the key threats and proposed security controls.

During the study, the researcher identified cyber threats and risks associated with these interfaces and modes of communication. Threats and risks were reviewed by the project team, for each threat and the risk was ranked according to the probability and severity of the threat, after which the threats and risks were formed into a matrix identifying the worst threats, moderate threats and least threat threats. This threat matrix can be found in Appendix 5 of this work.

The most important threat attack interface was the OptiPC in the system, which acts as the machine operator's interface to the machine control system. Most high-severity and high-probability cyber threats are possible through the OptiPC system. These cyber threats to the system are made possible, for example, by various social engineering attacks such as, email phishing, visits to malicious websites, malicious programs via USB.

If the OptiPC in the system were infected through these attack vectors and malicious software entered the system, it would allow for various additional threats depending on the user level used in the operating system. For example, if the system were used with administrator privileges, it would allow the attacker every opportunity to infiltrate the system. In the worst case, the data used by the entire system could be destroyed or could be stolen. The data produced by the machine control system is not in itself comparable to, for example, personal information systems, but the data is valuable to the owner of the machine because the owner of the machine receives a salary according to the output of the machine. Any change in the data could result in the machine being banned by the ordering forestry company.

If an attacker were allowed to execute code on the system, it would also allow intrusion into the Core unit in the machine control system, which manages the functions of the entire machine. This could be done, for example, by determining the encryption keys used by the system to communicate and thus the system would be able to communicate with the Core unit. Attacks from now on, however, require the attacker to know the system, thus the attack would be tricky without a holistic knowledge of communication. Because of this the encryption keys of the encryption used for communication or system credentials should be stored in a safe place, a place that cannot reverse engineered.

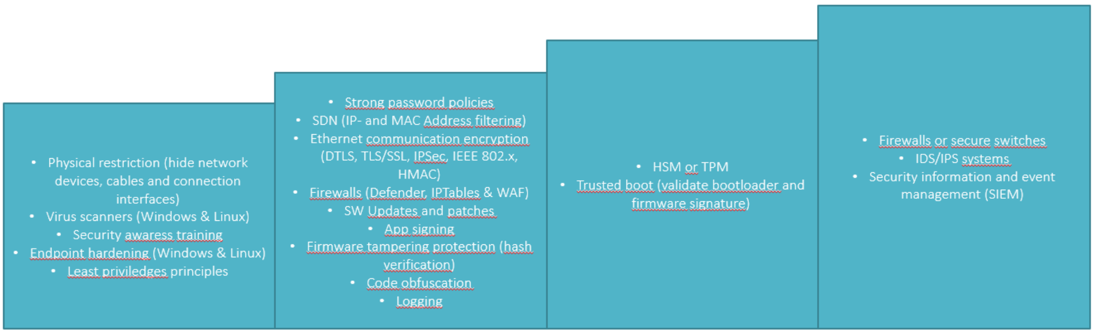
One of the large scale threats was that if an attacker took control of the system, it would allow the system to be used to attack, for example machine control system could be part of the botnet. The machine could thus be used, for example, in a distributed denial-of-service attack, or it could be used to penetration attacks.

Another major problem in the Control Platform acrhitecture is that Core unit contains multiple connectivity interfaces such as WLAN, Bluetooth and 3G/LTE. These communication interfaces should be removed from the Core unit and place them safer place such as behind firewall or secure switch to totally extract them out from machine primary control network.

These attacks can be quite easily to prevent by using multiple security controls. ISA/IEC 62443 standard introduces and defines different SL-levels. According to ISA/IEC 62443 these levels can be thought as following protection levels:

- **SL1 – Protection against casual or coincidental violation**
- **SL2 – Protection against intentional violation using simple means**
- **SL3 – Protection against intentional violation using sophisticated means**
- **SL4 – Protection against intentional violation using sophisticated means with extended resources**

By this way it is easy to create comprehensive model and approach for layered security. Researcher created following step by step models of security controls that could be used to protect Control platform architecture. Figure 27 shows the proposed security control for Control Platform project.



- Physical restriction (hide network devices, cables and connection interfaces)
- Virus scanners (Windows & Linux)
- Security awaress training
- Endpoint hardening (Windows & Linux)
- Least priviledges principles

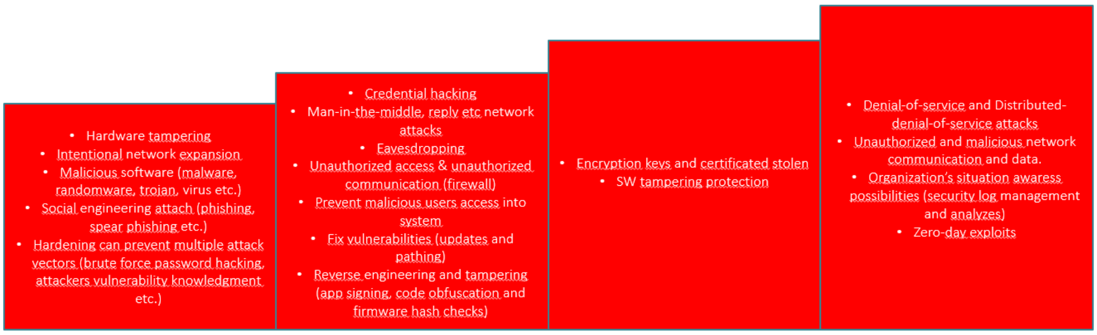
- Strong password policies
- SDN (IP- and MAC Address filtering)
- Ethernet communication encryption (DTLS, TLS/SSL, IPSec, IEEE 802.x, HMAC)
- Firewalls (Defender, IPTables & WAF)
- SW Updates and patches
- App signing
- Firmware tampering protection (hash verification)
- Code obfuscation
- Logging

- HSM or TPM
- Trusted boot (validate bootloader and firmware signature)

- Firewalls or secure switches
- IDS/IPS systems
- Security information and event management (SIEM)

Figure 27. Proposed security controls for Control Platform project

Figure 27, respectively, shows the cyber-attacks that can be prevented for using security controls that are proposed in Figure 28.



- Hardware tampering
- Intentional network expansion
- Malicious software (malware, randomware, trojan, virus etc.)
- Social engineering attach (phishing, spear phishing etc.)
- Hardening can prevent multiple attack vectors (brute force password hacking, attackers vulnerability knowledgment etc.)

- Credential hacking
- Man-in-the-middle, reply etc network attacks
- Eavesdropping
- Unauthorized access & unauthorized communication (firewall)
- Prevent malicious users access into system
- Fix vulnerabilities (updates and pathing)
- Reverse engineering and tampering (app signing, code obfuscation and firmware hash checks)

- Encryption keys and certificated stolen
- SW tampering protection

- Denial-of-service and Distributed-denial-of-service attacks
- Unauthorized and malicious network communication and data.
- Organization's situation awaress possibilities (security log management and analyzes)
- Zero-day exploits

Figure 28. Attacks that can be prevented using proposed security controls.

A proposal for a communication protocol can be found in Appendix 6 of the study. The proposal includes communication protocols within the machine's Ethernet network and also for external V2X communication.

10.3 Cyber security models of research and development

This chapter answers this thesis research question three, which were "*What is a good cyber security model that can will be used at development and maintenance of control systems for mobile machines?* "

Models for Cyber security management

Organizations are rapidly developing security in their products to prevent cyber security threats, mainly these products are secured to prevent outside cyber-attacks. Cyber security management is entity management, it must be remembered that the activities of the organization also have an impact on cybersecurity. The risks within the organization should be identified and the safety of the products made through it should be ensured during whole application lifecycle. Think of a situation where the product has been made completely secure, but the computer used in product development leaks, for example, encryption keys cyber security through an attack on hackers. In this case, hackers can take advantage of the leaked keys and use them to attack the company's products.

Active information security development is a complex activity, it is necessary to develop the security of the organization's internal processes, product security, security related to product development and maintenance activities, and security from the customer's point of view. Therefore, it is well justified to introduce models to improve information and cyber security, such as the NIST Cyber Security Framework or ISO 27001 information security management system standard. Implementing holistic models may seem tedious at first, but rewards in the longer run. Information security is being developed around the world in different ways, and therefore it is not worth starting to create your own model, because there are already good models for improving information and cybersecurity.

One important starting point for operational development is the support of the organization's management. The importance of cyber threats in today's products cannot be underestimated and ignored. Operations must be actively developed in the direction of information security, development always requires operating models that are followed. The development of information security is no exception here either, but requires a determined, conscious management approach.

The NIST cyber security framework or ISO 27000 informaton security standards provides a good infrastructure for managing cyber security in an organization. Appendix 8 of this work provides a description and researcher's view of the first steps to purposeful security development. The model is based on the sub-areas according to the NIST Cyber Security Framework, the model also covers the sub-areas of the ISO 27001 standard, as there are references to them in the NIST Framework.

Product related security standards and guidelines

The purpose of the standards and guidelines is to guide operations in a standard manner. With regard to cyber safety and product safety, the researcher will explore many different standards that could be utilized in the development of a control system for mobile connected work machines. No directly applicable standard or guideline was found for work machines, however, the following standards and guidelines are well utilized in the development of cyber-safe control system products:

- **NIST 800-82 Guide to Industrial Control Systems (ICS)** – this document provides guidance for securing industrial control systems (ICS), it also includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control systems like programmable logic controllers (PLC). This documentation contains overview of ICS and its typical system topologies, identifies common threat and vulnerabilities of the systems and describes recommendations of security countermeasures which can used to mitigate risks and threats.
- **NIST Special publications** – contains lots of different guidelines of how for example secure wireless local area networks (WLANs), guides to Bluetooth security, cryptography related guidelines etc.
- **ISA/IEC 62443-4-2 Technical security requirements for IACS components** – describes the technical requirements for securing the individual components of an ICS network.

The study reviewed various standards and guidelines for product safety in industrial automation systems. For mobile machinery, no applicable standard was found that would be directly applicable to the study area, but the above standards and guidelines are a good starting point for the development of product safety. Industrial automation systems as well as distributed control systems have very many in common with the control systems of mobile work machines.

The researcher also tried to get his hands on the ISA / SAE DIS 21434 standard, which deals with cyber safety of road vehicles. However, this standard is still under development and is likely to be released by the end of 2020.

Secure development lifecycle for Research and Development

Secure development lifecycle is a process that standardizes development lifecycle and gathers best practices tools and processes that should be used across products and applications. When thinking about products and their cyber security often normal development lifecycle is not enough because new steps may be needed to create secure products into customer's needs.

In this research field of study focuses at machinery side and because of functional safety requirements are very important requirement that should be considered when designing and implementing safe and secure products. Cyber risk assessment and risks reflection into functional safe is crucial to taken in account.

According to report CEN ISO/TR 22100-4:2020:fi Safety of machinery —Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects, machine manufacturers are obligated to perform risk analysis for cyber threats. Because of this aspect cyber risks assessment should be made to identify cyber threats and risks and their relation info machine safety.

Risk assessment is efficient way for organizations to identify cyber risks and selecting correct security control for avoiding, preventing and lowering risks. After identifying risks, it is also very important to ensure that selected security controls will prevent cyber-attacks and for this security assessment is another efficient way to get assurance about security level before rolling products into field.

After identifying these two new aspects that were not taken account by target organizations before this study. Researcher decided to create a proposition for securing development lifecycle of Control Platform project, this SDL proposition can be seen from Appendix 7.

Secure development cycle model describes all key factors and steps that should be taken account when developing embedded control system at Ponsse and Epec. At security point of view multiple new development steps are needed from requirements implementation to product release and steps between these stages of development.

There are lots of information about literature and different publication about SDL and its phases. During this research following interesting standards and guidelines for this purpose was investigated:

- **ISA/IEC 62443-4-1 Secure product development lifecycle requirements** – this part of the standard ISA/IEC 62443 describes a process and requirements for the Secure Development Lifecycle (SDL) of products at control systems and industrial automation.
- **NIST Secure Development Framework (SSDF)** – documentation provides secure development practices including business owners, software developers, project managers, and cyber security professionals.

Secure development lifecycle (SDL) solves multiple problems, lack of standard approach for securing product causes problems. First problem is vulnerabilities in the products, fixing vulnerabilities at the products afterwards takes lots of time and effort due to this, the developer will not be able to create new code. Second problem is that developers tent to repeat same mistakes. Third thing is that problems are found after releasing.

Finally, without a safety standard, customers have no assurance about the safety of a particular product. One product you are considering buying can be one good or terrible in terms of safety. Without SDL, there is no product security parity throughout the company. And without the usual process, some product teams completely ignore security.

Summary of models

Standards are absolutely necessary to guide operations, cyber security processes should by no means be developed from scratch, as compliance with already established standards is laborious and time-consuming in itself. Utilizing ready-made models is a very sensible approach to a company's product development operations.

The researcher proposes three mutually supportive approaches to the development and implementation of comprehensive cybersecurity in the company. The first step is to introduce the secure development lifecycle process (SDL) for Ponsse and Epec, the appropriate SDL process must be followed during the life cycle of each product. Second step is to secure Ponsse's and Epec's products by proactively development of ICS products security by utilizing suitable standards into product security development. The third and final important step is to actively start developing a cyber security management system (CSMS) for comprehensive enterprise information security and cybersecurity management.

11. Conclusions

The aim of the work was to study the cyber security of the Control Platform machine control system being developed by Ponsse and Epec. Finding out how a machine control system should be built to make it secure from a cyber security perspective. The second goal of the work was to study Automotive Ethernet-based control system intrusions from the automotive industry as well as other industries, to identify cyber threats and security controls related to these solutions. The third goal of the work was to find out what models could be used in Ponsse's and Epec's product development to develop cyber security.

The work achieved all the goals set for it, and as a result of the work, Ponsse and Epec can further develop cyber security in product development and at the Group level. The work identified how the system under development should be protected, identified the main threats related to the Control Platform architecture, clarified security controls and their levels, and found alternative models for developing the security of a comprehensive organization.

The feedback from the organization of the results of the work has been good. The work fully meets the need and is very useful. The organization has identified areas for development and based on the results of this work, it is very good to proceed to further develop the organization's information security at product level and also organizational level.

For the Control Platform project related to product development, the work has so far been based on a review of architectural solutions and the next development is to define the desired level of security and to start implementing security controls related to the security of the system. The models studied for the organization's information security management provide a good opportunity for Ponsse and Epec to review their own information security-related processes and further develop them as needed.

12. Afterwords

The researcher would like to thank the clients for this very interesting topic and wide-ranging research questions. The work provided a very wide range of experience and learning about cybersecurity for the researcher. In addition, conducting research through participation in a project team provided the researcher and the project team with knowledge and an idea of cybersecurity and its challenges today.

The assistance of the project team helped the researcher to understand the nature, limitations, target environment and visions of the future of the machine control system, without which the results of the research could have been incomplete. In addition, the existence of the project team drove the researcher to schedule the research, achieve the goals, answer the challenging questions, and otherwise promote this export through the work.

References

Cybersecurity Help. (2020). *Latest zero-days*. Retrieved from Zero-day.cz: https://www.zero-day.cz

Angermeire, D. (2020, 3). *ISA/SAE 21434 - a field report*. Retrieved from YSEC Knowledge Base: https://www.security-analyst.org/iso-sae-21434-a-field-report/

Apampatzis, A. (2019, 09 10). *What is the ISA/IEC 62443 Framework?* Retrieved from The State of Security: https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/

C Miller, C. V. (2013). *Adventures in automotive networks and control units.*

Center for Internet Security. (2020). *Cybersecurity Spotlight – Defense in Depth (DiD)*. Retrieved from https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/

Cloudflare. (2020). *What is IPsec? | How IPsec VPNs work*. Retrieved 2020, from https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

Cloudware. (2020). *What is a Denial-of-Service (DoS) Attack?* Retrieved from Cloudware: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Cristina, J. (2020). *DTLS security over UDP*. Retrieved from https://www.teldat.com/blog/en/dtls-security-udp-tls-heartbleed/

Cyber security & infrastructure security agency. (2020, May 8). *Securing Wireless Networks*. Retrieved from https://us-cert.cisa.gov/ncas/tips/ST05-003

Cynet. (2020). *Unauthorized Access: 5 Best Practices to Avoid the Next Data Breach.* Retrieved from Network attacks: https://www.cynet.com/network-attacks/unauthorized-access-5-best-practices-to-avoid-the-next-data-breach/

Desjardins, J. (2018, January 3). *Why Hackers Hack: Motives Behind Cyberattacks*. Retrieved from Visual capitalists: https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/

DigiCert. (2020). *What is SSL, TLS and HTTPS?* Retrieved from https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https

environment, Y. S. (2020, 07 30). *Global Forest Atlas*. Retrieved from Logging: https://globalforestatlas.yale.edu/forest-use-logging/logging

Escrypt. (2020). *How to secure automotive Ethernet with a firewall solution*. Retrieved from https://www.escrypt.com/en/Ethernet-webinar

F5. (2020). *Datagram Transport Layer Security (DTLS)*. Retrieved from https://www.f5.com/services/resources/glossary/datagram-transport-layer-security-dtls

Firch, J. (2020, September 26). *Common Types Of Network Security Vulnerabilities In 2020*. Retrieved from PurpleSec: https://purplesec.us/services/

F-Secure. (2020). *Denial of Service (DoS)*. Retrieved from F-Secure articles: https://www.f-secure.com/v-descs/articles/denial-of-service.shtml

Gasdia-Cochrane, M. (2015, December 21). *New to the Mining Industry? Make Sure You Know the Most Common Types of Mining Equipment*. Retrieved from ThermoFisher Scientific: https://www.thermofisher.com/blog/mining/new-to-the-mining-industry-make-sure-you-know-the-most-common-types-of-mining-equipment/

Gershwin, A. (2019, July 5). *The Layered Cybersecurity Model for Small & Medium Business Protection*. Retrieved from Data Driven Investor: https://medium.com/datadriveninvestor/layered-cyber-security-model-for-small-medium-business-protection-64b293133de4

Hirsjärvi, S., & Hurme, H. (2018). *Tutkimushaastattelu.* Gaudeamus.

Informa Markets. (2017). *Cyber risk and the impact on health and safety*. Retrieved from Barbour safe in our knowledge: https://www.barbour-ehs.com/cyber-risk-impact-health-safety/

Infradata Inc. (2019, 10 22). *What is OT Security?* Retrieved from Infradata web pages: https://www.infradata.com/resources/what-is-ot-security/

International Journal of Scientific Engineering and Technology Research. (2016, October). A Practical Wireless Attack on the Connected Car and Security Protocol. Retrieved from http://ijsetr.com/uploads/142653IJSETR12072-1312.pdf

ISO. (2020, 5 31). *ISO/IEC 27001 Information security management*. Retrieved from ISO webpages: https://www.iso.org/isoiec-27001-information-security.html

ISO. (2020). *Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects.* Helsinki: Finnish standards association SFS.

Jung, R., & Shukla, S. (2020). *Experience and Lessons Learned from Firewall and Intrusion Detection System Development for Automotive Ethernet.* Munich: Automotive Ethernet Congress.

KaranC. (2020, January 10). *30 Types of Navigation Equipment and Resources Used Onboard Modern Ships*. Retrieved from Marine insight: https://www.marineinsight.com/marine-navigation/30-types-of-navigational-equipment-and-resources-used-onboard-modern-ships/

Kaspersky. (2020). *What Is a Replay Attack?* Retrieved from Kaspersky resource center: https://www.kaspersky.com/resource-center/definitions/replay-attack

Kochetkova, K. (2016, October 24). *Software updates are critical, so automate them*. Retrieved from Software updates are critical, so automate them

Krawczyk, H., Bellare, M., & Canetti, R. (1997). *RFC2104 HMAC: Keyed-Hashing for Message Authentication.* Retrieved from https://tools.ietf.org/html/rfc2104#section-2

Lang, M. (2019). *Secure Automotive Ethernet - Balancing Security and Safety in Time-Sensitivice Systems.* Karlskrona: Blekinge Institute of Technology.

Lin, C.-W., & Sangiovanni-Vincentelli, A. (2012). *Cyber-Security for the Controller Area Network.* Berkeley: University of California. Retrieved from https://escholarship.org/content/qt5422g038/qt5422g038_noSplash_f8c542841c55634ea7b98bb06ff39d1b.pdf

Lord, N. (2018, September 12). *What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance*. Retrieved from Digital Guardian websites: https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

Maritime Industry Foundation. (2020). *Equipment manufacturers*. Retrieved from The Maritime Industry Knowledge Centre: https://www.maritimeinfo.org/en/Maritime-Directory/equipment-manufacturers

Meriliitto - Sjöfartsforbundet RY. (2020). *Maritime industries*. Retrieved from Meriliitto - Sjöfartsforbundet RY Suomen merellisten intressipiirien yhteistyöfoorumi: http://www.meriliitto.fi/?page_id=183

Mohanty, S. (2018, March 8). *5 Important Software Vulnerabilities*. Retrieved from Security Zone: https://dzone.com/articles/5-important-software-vulnerability-and-attacks-tha

Mutune, G. (2020). *23 Top Cybersecurity Frameworks*. Retrieved from Cyber Experts: https://cyberexperts.com/cybersecurity-frameworks/

N. Fabritius, R. J. (2017). Ethernet Security. ESCRYPT GmbH.

National Institute of Standards and Technology. (2018, May 3). *MEP Centers Aid Manufacturers on Cybersecurity*. Retrieved from National Institute of Standards and Technology web pages: https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity

New-Tech Europe. (2020). NXP Announces Safe and Secure Automotive Ethernet Switch for Time Sensitive Networking (TSN). Retrieved from https://www.new-techeurope.com/2020/01/07/nxp-announces-safe-and-secure-automotive-ethernet-switch-for-time-sensitive-networking-tsn/

Norton. (2020). *What is man-in-the-middle attack?* Retrieved 2020, from Norton Security Center: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Orange, S. (2020, 07 30). *Cut-to-length vs. whole tree logging*. Retrieved from Forest Restoration Implementation: http://forestrestorationworkshop.org/wp-content/uploads/cut-to-length-vs-whole-tree-logging.pdf

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2017). *Guide to BluetoothSecurity.* Gaithersburg: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

Paloalto. (2020). *What Is Network Segmentation?* Retrieved 2020, from Cloud Security: https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

Penttilä, O. (2016). *Cyber threats in maritime container terminal automation systems.* Tampere: Tampereen teknillinen yliopisto.

Petri, R., Springer, M., Zelle, D., McDonald, I., Fuchs, A., & Krauß, C. (n.d.). Evaluation of Lightweight TPMs for Automotive. Darmstadt, Germany. Retrieved from http://ftp.pwg.org/pub/pwg/liaison/escar/tpm_paper_2016_0513_final.pdf

Ponsse. (2020). *Ponsse Scorpion*. Retrieved from Ponsse harvesting products: https://www.ponsse.com/fi/tuotteet/harvesterit/tuote/-/p/scorpion#/

Ponsse Oyj. (2020). *In the beginning there was a logging site, a frame saw and Einari. Now, Ponsse makes the best forest machines in the world.* Retrieved from Ponsse web pages: https://www.ponsse.com/en/web/guest/company/ponsse#/

Raitis, T. (2018, June 14). *Our factory*. Retrieved from Epec web pages: https://epec.fi/our-factory/

Reddy, P. (2020, April 23). *Is Windows Defender a Firewall? Not Exactly*. Retrieved from Medium website: https://medium.com/lotus-fruit/is-windows-defender-a-firewall-not-exactly-72a598ac1b78

Reichl, C. (2020). *World Mining Data.* Vienna: Federel Ministry of Agriculture, Regions and Tourism. Retrieved from https://www.world-mining-data.info/wmd/downloads/PDF/WMD2020.pdf

Risk Based Security. (2020). *VulnDB*. Retrieved from VulnDB Cyber risk analytics: https://vulndb.cyberriskanalytics.com/#statistics

Roepke, R., Thraem, T., Wagener, J., & Wiesmaier, A. (n.d.). *A Survey on Protocols securing the Internet of Things: DTLS, IPSec and IEEE 802.11i.*

Saaranen-Kauppinen, A., & Puusniekka, A. (2006). *valiMOTV - Menetelmäopetuksen tietovaranto teemahaastattelu*. Retrieved from KvaliMOTv: https://www.fsd.tuni.fi/menetelmaopetus

Safety first for automated driving. (2019). Daimler.

Sandvik. (2020). *IN-THE-HOLE LONGHOLE DRILL RIGS*. Retrieved from Sandvik products: https://www.rocktechnology.sandvik/en/products/underground-drill-rigs-and-bolters/in-the-hole-longhole-drills

SBSoft. (2020). *ISO 27001:2013 – Information Security Management Policy*. Retrieved from ISO 27001- ISMP: https://sbsoft.com/iso-270012013-information-security-management-policy/

Schmittner, C. (2019, August 9). *Automotive Cybersecurity Standards - Relation and Overview*. Retrieved from Springer link: https://link.springer.com/chapter/10.1007%2F978-3-030-26250-1_12

ScienceDirect. (2020). *Eavesdropping Attack*. Retrieved from ScienceDirect Journals and books: https://www.sciencedirect.com/topics/computer-science/eavesdropping-attack

SFS. (2020, 5 31). *Standardit ja julkaisut - SFS-EN ISO 13849-1*. Retrieved from SFS Standardien verkkokauppa: https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/1/410492.html.stx

SFS. (2020, 5 31). *Standardit ja julkaisut - SFS-EN ISO 13849-2*. Retrieved from SFS Standardien verkkokauppa: https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/1/244252.html.stx

Sharpened Productions. (2020). *System Hardening*. Retrieved from https://techterms.com/definition/systemhardening

SSH Communications Security, Inc. (2020). *SFTP – SSH Secure File Transfer Protocol*. Retrieved from https://www.ssh.com/ssh/sftp/

SSH Communications Security, Inc. (2020). *SSH (Secure Shell)*. Retrieved from https://www.ssh.com/ssh/

Stouffer, K., Pillitteri, V., Adrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security.* May: National Institute of Standards and Technology.

Symanovich, S. (2017, July 31). *What Is a Data Breach and How Do I Handle One?* Retrieved from Data Breaches: https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html

TCG. (2018). *TCG TPM 2.0 Automotive Thin Profile.* TCG. Retrieved from https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf

Technology, N. I. (2012). Guide for Conducting Risk Assessment. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Technology, N. I. (2020, September 23). *New to Framework*. Retrieved from CyberSecurity Framework: https://www.nist.gov/cyberframework/new-framework

TechTarget. (2020). *Hardware vulnerability*. Retrieved 2020, from WhatIs.com: https://whatis.techtarget.com/definition/hardware-vulnerability

The Ohio State University. (2020). *Cybersecyrity - AntiVirus*. Retrieved 2020, from The Ohio State University webpages: https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus

Tip Top Security. (2017, Semtember 10). *How Does HTTPS Work? RSA Encryption Explained*. Retrieved from https://tiptopsecurity.com/how-does-https-work-rsa-encryption-explained/

Traficom, K. . (2020). *Pilvipalveluien turvallisuuden arviointikriteeristö.* Liikenne- ja viestintävirasto.

Triassic Solutions. (2018, December 5). *Security Reguirement for Embedded Systems*. Retrieved from Triassic Solutions: http://triassicsolutions.com/blog/security-requirements-for-embedded-systems/

United Nations Conference UNCTAD. (2019). Review of maritime transport. Retrieved from https://unctad.org/system/files/official-document/rmt2019_en.pdf

Walkowski, D. (2019, July 9). *What is the CIA Triad?* Retrieved from F5 Labs: https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Valtionvarainministeriö. (2006). *Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen - hallittu prosessi.* Helsinki: Valtionvarainministeriö.

Valtionvarainministeriö. (2017). *Tietoturvapoikkeamatilanteiden hallinta.* Helsinki: Valtionvarainministeriö.

Watts, S. (2018, January 16). *SIEM vs Log Management: What's the difference?* Retrieved from The Business of IT Blog: https://www.bmc.com/blogs/siem-vs-log-management-whats-the-difference/

Vector. (2020). Cyber Security Mechanisms for Connected Vehicles. Munich, Germany. Retrieved from https://www.infineon.com/dgdl/Infineon-ISPN-Use-Case-Cyber-security-mechanisms-for-connected-vehicles-ABR-v02_18-EN.pdf?fileId=5546d462647e95a60164889affd74a5e

Veracode. (2020). *SPOOFING ATTACK: IP, DNS & ARP.* Retrieved from AppSec Knowledge Base: https://www.veracode.com/security/spoofing-attack

What is Mining? (2020, 07 30). Retrieved from Geologyin: http://www.geologyin.com/2014/03/what-is-mining.html

Willis, V. (2019, October 24). *Endpoint Hardening - Why It is Essential for Cyber Security*. Retrieved from https://blog.automox.com/endpoint-hardening

Yadav, A. (2020, August 4). *Network Design: Firewall, IDS/IPS*. Retrieved from Infosec: https://resources.infosecinstitute.com/network-design-firewall-idsips/

Yang, H., Liu, M.-Z., Xu, Y.-H., Wu, Y.-J., & Xu, Y.-N. (2019, February). *Research of Automotive Ethernet Security Based on*. Retrieved from https://pdfs.semanticscholar.org/2768/fac52a80f25f0b927ec522b89257769e9078.pdf

Appendices