TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ANTTI KANKAANRANTA

THREAT MITIGATION IN INDUSTRIAL INTERNET: CASE VARIABLE-FREQUENCY DRIVE

Master of Science Thesis

Examiner: Marko Helenius
Examiner and topic approved in the Faculty of Computing and Electrical Engineering Council meeting on the 29th of March 2017

ABSTRACT

Antti Kankaanranta: Threat mitigation in industrial internet: Case variable-frequency drive
Tampere University of Technology
Master of Science, 42 pages
February 2018
Master's Degree Program in Information Technology
Major: Software Engineering
Instructors: Jarmo Harju & Marko Helenius

Keywords: Industrial Internet, Cybersecurity, Variable-Frequency Drive

Industrial Internet devices have faced new threats by attackers with high resources. Thus, the cybersecurity of such devices has to improve. Variable-frequency drives (VFD) were selected as the target devices to study cybersecurity of industrial internet devices and give recommendations of how to improve their cybersecurity.

The current status of cybersecurity of VFDs was studied in the thesis. The study was performed by interviewing product development engineers of a VFD manufacturer. VFD's assets were recognized in the interviews also. Security weaknesses were found during the interviews and potential attacks against those weaknesses were also identified. The attacks were categorized and values were assigned to attack's effectiveness and complexity. The description of attacks included also some hints how the attacks could be performed and why attacker might want to perform the operation. Finally the attack tree were performed based on the attacks.

The thesis presented also mitigation strategies which were found from literature. It was also presented how the strategies suited for the VFD context. There was a study of what mitigation strategies VFD are applying. A prioritisation workshop was organized for prioritising the unapplied mitigation strategies. The prioritisation was necessary because there was the need to perform important strategies first. The attendees of the workshop were product managers, software architect and cybersecurity chief of VFD manufacturer. The prioritisation method used was Weighted Shortest Job First. The method notified business value, time criticality, risk reduction and how much effort the job might take to get done.

The most important mitigation strategy was Access Control. Second important strategy was Logging and Event Management. Third important strategy was User Authentication and Authorization. A possible explanation for the prioritisation might be that there were customer requirements for the strategies. However, the discussion in prioritisation workshop cleared the general view of mitigation strategies. Thus, those strategies got highest points in the business value, time criticality and risk reduction.

TIIVISTELMÄ

Antti Kankaanranta: Teollisen internetin tietoturva: tapaus taajuusmuuttaja
Tampereen teknillinen yliopisto
Diplomityö, 42 sivua
Helmikuu 2018
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Ohjelmistotuotanto
Ohjaajat: Jarmo Harju & Marko Helenius

Avainsanat: Teollinen internet, tietoturva, taajuusmuuttaja

Teollisen internetin laitteiden tietoturvaan on alettu kiinnittää enemmän huomiota vasta viime vuosina. Laitteiden verkottuminen ja uhkaajien taitotason noustessa teollisen internetin laitteet tarvitsevat parempaa tietoturvaa. Työssä tutkitaan taajuusmuuttajan tietoturvan nykytilaa ja ehdotetaan toimenpiteitä tietoturvan parantamiseen.

Työssä taajuusmuuttajan tietoturvan nykytila ja potentiaaliset uhkatekijät kartoitettiin keskustelemalla taajuusmuuttajia valmistavan yrityksen tuotekehityshenkilöstön kanssa. Samalla kävi ilmi taajuusmuuttajan suojaamisen arvoiset voimavarat.

Tietoturvan nykytilaa kartoittaessa havaittiin taajuusmuuttajassa erilaisia tietoturvallisuuden heikkouksia. Heikkouksille löytyi myös erilaisia tapoja hyödyntää niitä hyökkäysten muodossa. Hyökkäykset kategorisoitiin ja pisteytettiin vaikeusasteen ja vaikuttavuuden mukaan. Niistä kuvattiin myös se kuinka niitä olisi mahdollista toteuttaa ja miksi hyökkääjä haluaisi hyökätä taajuusmuuttajaa vastaan hyökkäyksen tavalla. Hyökkäykset koottiin lopulta yhteen ja niistä muodostettiin hyökkäyspuu.

Työssä esiteltiin myös kirjallisuudesta löytyneitä tietoturvauhkien lievennysstrategioita ja mitä ne soveltuvat taajuusmuuttajien kontekstiin. Samalla tutkittiin mitä uhkien lievennysstrategioita taajuusmuuttajassa on jo toteutettuna. Toteuttamattomista strategioista järjestettiin priorisointityöpaja. Priorisoiminen toteutettiin, jotta taajuusmuuttajien turvallisuuden kannalta merkittävimmät strategiat toteutettaisiin ensiksi. Työpajassa oli koolla taajuusmuuttaja valmistajan tuotepäälliköitä, ohjelmistoarkkitehti ja taajuusmuuttajien tietoturvan kehityksestä vastaava päällikkö. Priorisoinnin tukena käytettiin WSJF-priorisointimenetelmää (weighted shortest job first), joka huomioi torjuntastrategian liiketoiminta-arvon, aikakriittisyyden, toteuttamatta jättämisen riskin ja strategian toteuttamisen työläyden.

Työpajassa tärkeimmäksi strategiaksi nousi pääsynhallinta. Toiseksi tärkein strategia oli lokien kerääminen ja tapahtumien hallinta. Kolmanneksi tärkein strategia oli käyttäjän autentikointi ja auktorisointi. Osittain kärkistrategiat selittyvät jo työpajan järjestämishetkellä olevista asiakasvaatimuksista, mutta työpajan ansiosta keskustelu strategioista vahvistui ja kyseiset strategiat saivat siten korkeimmat arvot liiketoiminnan, aikakriittisyyden ja toteuttamatta jättämisen riskin suhteen.

PREFACE

I would like to thank everybody who have helped me with this master's thesis. Thanks to professors Tommi Mikkonen and Jarmo Harju who helped me through the struggling start and halfway of the thesis. Thanks also for the university teacher Marko Helenius, who have gave a lot of feedback and helped me to finish this thesis. In addition, thanks very much for the company which enabled this thesis and my instructor who gave valuable feedback of cybersecurity and variable-frequency drives.

Vantaa, 26.2.2018

Antti Kankaanranta

TABLE OF CONTENTS

TERMS, DEFINITIONS AND ABBREVIATIONS

AC	Alternating Current
AP	Adaptive Programming
CAN	Controller Area Network
HTTP	Hypertext Transfer Protocol
I/O	Input/output
IIC	Industrial Internet Consortium
PC	Personal Computer
PLC	Programmable Logic Control
USB	Universal Serial Bus
VFD	Variable-Frequency Drive
VPN	Virtual Private Network
WSJF	Weighted Shortest Job First

1. INTRODUCTION

Number of networked devices is growing in an increasing pace. Devices which did not have an access to the internet earlier are connected today. This enables better communication between devices, remote controlling of devices and collection of data. Which in turn can increase productivity of devices. However, networking of devices may present threats, for example, a malicious person tries to break devices remotely. Because of this, manufacturers have taken steps to increase cybersecurity how the devices detect, analyze and combat threats.

The purpose of this thesis is to study what threat mitigation techniques and strategies are used to strengthen cybersecurity in Industrial Internet devices. The study is performed as a case study and target of study is Variable-Frequency Drives (VFDs). The study focuses on mitigation strategies, which are found from literature, and the application of these strategies in VFDs. The thesis also gives recommendations on which of the identified strategies should be implemented as a priority in order to keep up with the cybersecurity trends. The strategies are prioritised by Weighted Shortest Job First (WSJF) method.

There are also other devices in industrial networks which might cause security issues to VFD. An old phrase in security says that "security is only as strong as its weakest link." So, it is impossible to secure any system completely against all attackers (Saitta et al. 2005). Industrial networks are often considered to be separate from company's network and separate from the internet as well. Recently this has changed and now firewalls are required in order to bring protection from the outside world. Historically industrial systems have been secured by isolating vulnerable components. Thus, networks have been guarded by locks and guards, not cybersecurity agents. (IIC, 2016)

The rest of the thesis is structured as follows: Chapter two describes VFD. The chapter describes what a VFD is as well as its interfaces and services. In the chapter the relation of the interface and services is mapped. There is also an introduction to VFD configuration and programming.

Chapter three focuses on the cybersecurity of the Industrial Internet. The chapter includes categorization of different threats against industrial devices, description of attack process against industrial internet systems and description of the industrial network from the VFD point of view. In addition, this chapter presents mitigation techniques for the industrial devices against attacks.

Chapter four describes how the case study was performed. The chapter starts by describing different threat modelling practices. First sub-chapter of chapter describes the re-

search approach. After the research approach comes the process description. Process description presents the method how the study was performed and what was needed to take into account in the process. In addition, the chapter describes the method how the threat mitigation strategies were prioritised. The chapter describes prioritisation method Weighted Shortest Job First.

The fifth chapter introduces the results of the performed threat modelling. Assets of VFD are presented as well as a study of which of the mitigation strategies presented in chapter three the VFD is supporting. Attacks discovered against the VFD during the threat modelling process are presented. Finally the chapter gives recommendations how to improve cybersecurity of VFD. The recommendations are organized in a prioritized list.

Finally, the last chapter is a conclusion chapter. It wraps together the research what have been done for the thesis. It also proposes actions for the future

2. VARIABLE-FREQUENCY DRIVE

Variable-frequency drives (VFD) are devices which control the speed and torque of Alternating Current (AC) motors. Because of a VFD, motor runs always in the right speed and torque. The function of VFDs is to enable continuous control of motors. Figure 1 presents an example of VFD product family.

A motor without a VFD is connected straight to a power-distribution network. This kind of usage is called direct on line usage. Thus, it runs at the network's frequency. It means that the motor runs at a nominal speed. If motor is not supposed to run at a full speed, it has to be braked, choked or gears have to be used to control speed of motor. Those practices consume a lot of energy. VFD saves energy by using only necessary amount of electric power to run a motor.

Beside of the energy savings and continuous controlling VFD also advances the accuracy of motor movement. For example, VFD in an elevator enables a smooth start and stop for the ride. Without the VFD, the elevator ride starts with a jump and stops in the same manner.

Figure 1. *Variable-frequency drives (ABB, 2016).*

Running an AC motor is not the only application where VFDs are used. VFD works in opposite direction as well which means that they can transform energy into electricity in a frequency that is suitable for a power-distribution network. Thus, the VFD can work with a generator. Wind power is an example of creating energy and converting it into the right frequency for the power-distribution network. Advanced VFDs can also transform braking energy into electricity. Otherwise energy is transformed into heat. This kind of function is useful for example for cranes.

30-40 percent of newly installed motors have VFD installed with them (Lendermann et al. 2011). Hence, VFDs are taken in to use at steady pace. In addition, VFDs can be taken in to use for older motors, so the amount of VFDs might be larger than 30-40 percent.

VFDs are used in different fields, for example, paper, oil and food industries. Washing machines and similar household devices use VFDs too. However, in this thesis focus is on industrial usage, mechanical engineering and building automation. Thus, the focus of the thesis is on paper mills, steel mills, oil refineries, etc. The industrial VFDs work in the same manner than its smaller variants. The biggest difference is that in industry motors are bigger and there are more of them, so industrial VFDs need to be more reliable because delays might be expensive in the industrial process. In addition, it can be costly to replace or repair industrial purpose VFDs. There are also other devices in the same network with VFD. In industry motors working in cooperation should work in the same pace and should hold the right position. It means that there needs to be communication between VFDs concerning motors and states.

Lifetime of VFDs are long. If devices are used in good conditions, variable-frequency drives' operating time can be as long as decades. Some VFDs from 80’s are still in use. Thus, there is a large base of old VFDs installed because of long lifecycle. Hence, many VFDs are manufactured before no one thought that someone might want to compromise VFDs.

2.1 Configuration of VFD and IEC 61131-3 programming

VFD’s have a lot of configuration items. For example, ABB’s ACS880 has 33 different parameter groups. However, VFD does not need that much parameters configured to run a motor. Large amount of parameters enables precise control of VFD in various situations. ACS880 has a feature called parameter lock. It can lock parameters and prevent users to change them. The lock is protected by four digits password. The lock can be opened from the PC tool and fieldbus. The tools are described in the next subchapter.

There is a possibility to program some higher performance VFDs. There are two ways to program them, Adaptive Programming (AP) and other programming methods which are presented at International Electrotechnical Commission (IEC) 61131-3 standard for programmable logic controllers. There are also macros which are set of parameter groups for common use cases like, pump application or fan. AP can be used when set-

ting parameters is not enough but user wants to change parameters when the input changes (ABB, 2016). In addition, IEC 61131-3 programming allows users to create own applications too. IEC programming includes five different programming languages: Ladder Diagram, Instruction List, Function Block Diagram, Structured Text and Sequential Function Chart.

2.2 Interfaces

This sub-chapter describes common interfaces of VFDs. VFDs have input and output interfaces, which are used to control and monitor them. The interfaces are described in the Table 1 below. The VFD's interfaces are fieldbus, Safety option, Memory unit, Drive to Drive link, PC tools, panel, I/O and SD card. The Table presents a short summary of every interface. In addition, the sub-chapter explains wider fieldbus and panel interfaces. Common fieldbus protocol Modbus and Profinet are also presented.

Name	Explanation
Fieldbus	There are different fieldbus option modules available. So VFD can be connected by various protocols. Fieldbus is used to link various field devices to PLC
Safety option	Safety option is an option module, which listens to I/O. Safety options are used to ensure safety of machines. When the safety receives a signal or cannot get signals from the source, it shutdowns the VFD in a controlled way.
Memory unit	Memory unit works as a storage for firmware software, applications and files. Thus, memory unit can be used for loading a new firmware and application.
Drive to Drive link	Implements master/slave architecture connection between VFDs. It is used to link several VFDs together; an example usage case is where motors are coupled together, like via conveyor belt.
PC tools	There are different kind of PC tools for controlling, parameter configuration and creating IEC 61131-3 applications for VFD. Also new firmware can be loaded through a PC tool. PC can be connected to VFD through Ethernet cable.
Panel	Panel works as user interface for the local user. There are also Bluetooth panels available, which allows to configure VFD from the smart phone.
I/O	There are two types of I/O signals, analogue and digital.
SD Card	SD Cards are auxiliary memory, which enables transfering firmware update, user data and user's programs from PC to VFD and vice versa.

Table 1. *VFD Interfaces (ABB – Firmware manual, 2016)*

Fieldbus options offers different protocols for the communication with the PLC and other devices in the industrial network. VFDs support many protocols including, but not limited to, BACnet/Ip, CANopen and Modbus TCP. Wide spread and the de facto protocol of fieldbus communication is Modbus (Knapp 2011, p. 56; Drury 2009, p. 508). The protocol has been developed as early as 1979 and TCP/IP version of Modbus was developed at 1999. Sundell et al. (2012, p. 17) are presenting that many of fieldbus protocols are applying master-slave architecture. Also Modbus is using master-slave mechanisms in communication. Responsibility of configuration and running the system is re-

lying on a master which can be either Supervisory control and data acquisition (SCADA) control system or PLC.

Field devices are working in real-time environment and, thus, those protocols need to be efficient. This means that the protocols do not contain any unnecessary functions. Hence, security features, like authentication and encryption are not supported by protocols. (Knapp 2011, p. 55.)

Modbus works at the seventh layer, which is application layer, of OSI model. The OSI model is presented at the sub-chapter 3.2. Working in the application layer means, that the protocol is not depending on the communications protocols under the application layer. Thus, it can operate in serial networks and also in TCP/IP network. The Modbus protocol uses message broadcasting to send a message to device. The correct device is selected based on a unique address, thus, every device gets a message but only correct one will answer. The security concerns of Modbus protocol are lack of authentication, lack of encryption, broadcasting of messages, programmability and lack of message checksums in Modbus TCP (Knapp 2011, p. 56-60).

Profibus is another protocol supported by VFD. The protocol can be used as asynchronous, synchronic messaging and also over ethernet. The protocol works as a master-slave architecture like Modbus, but the difference is that there can be multiple master nodes. The master has a token which is used to control certain slaves. The master is changed by token sharing. The possible cybersecurity weaknesses of the protocol are lack of authentication, token capturing by malicious person and false token injection. (Knapp 2011, p. 80.)

The panel is connected to VFD through RS-485 connection. The panel has a user interface and user can change VFD's parameter settings through it. There is also an USB interface in the panel. The USB port can be recognized in figure 2 in the bottom of panel. The USB port can be used to connect local PC to VFD. Some versions of the panel allow also a Bluetooth connection. The Bluetooth connection is established by allowing Bluetooth connection from the panel. Hence, the panel generates a four digit pairing number. Thus, the devices with Bluetooth capability can be connected to VFD. The range of Bluetooth depends from the devices class and can vary from 10 to 100 meters (Wright, 2018).

Figure 2. *VFD panel (ABB, 2011)*

2.3 Interfaces and services

Different internal services of VFDs are presented in the Table 2. The Table presents VFDs' services and relation of them to different entry points. The Table shows that PC tools have the widest access to different VFD's services, which makes it the most critical component from a VFD's point of view if attacker wants to download malicious applications or perform other malicious actions against VFD's services. In addition, the Table shows that fieldbus have access to VFD's parameters. Thus, an attacker can also change parameters through it. However, there are parameters which can prevent fieldbus, panel and PC usage of VFD.

service	Fieldbus	Safety option	Memory unit	Drive to drive	PC tools	Panel	I/O	SD Card
Writing parameters	X			X	X	X		
Reading parameters	X	X		X	X	X		
Time services	X			X	X	X		
File system services					X	X		X
Load a new application			X		X			

Load a new firmware			X		X			
Save drive configuration / backup					X	X		
Load a new software license			X		X			
Drive control	X	X		X	X	X	X	
Drive reference	X			X	X	X	X	
Drive monitoring	X	X		X	X	X	X	X

Table 2. *Table about different services and interfaces*

Writing parameters is a service for handling parameters of VFD. The parameters are an important part of VFD's configuration. More about the configuration and parameters is presented at the sub-chapter 2.1. Four interfaces are allowed to write the parameters. Those interfaces are fieldbus, Drive to Drive link, PC tools and panel.

Time services is a service for setting an internal clock of VFD. The clock is used for balance VFD's real-time clock. It is used, for example, in the logging showing current time for the user. The time services are also used for synchronization of Fieldbus communication. Interfaces for accessing to time services are: fieldbus, Drive to Drive link, PC tools and panel.

File system services is a service for accessing VFD's file system. It includes modification of files, removing files and adding new files. Three interfaces have an access to the services: PC tools, panel and SD card. Although, SD card is used only to store data.

Load a new application is a service for loading a new application. Applications are presented in the sub-chapter 2.1. Memory unit and PC tools are allowed to load a new application.

Load a new firmware is a service for updating or changing VFD's firmware. Firmware is a critical part of VFD and only PC tools and Memory unit have an access to load a new firmware.

Save VFD configuration / backup is a service for saving VFD's configuration. Backup can be used to copy parameter set to different VFD. Thus, replacing VFD doesn't take effort of configuration of parameters. Panel and PC tools can be used for backupping VFD.

Load a new software license is a service for loading a new software license. The license allows VFD to upgrade its firmware. Memory unit and PC tools are capable to updating VFD's license.

VFD control is a service to controlling VFD. It includes start and stop of VFD and the motor it runs. Fieldbus, Safety option, Drive to Drive, PC tools, panel and I/O have an access to controlling VFD.

VFD reference is a service to change a reference value of VFD. Reference value determines the speed of motor which is run by VFD. Fieldbus, Drive to Drive, PC tools, panel and I/O have an access to controlling VFD.

VFD monitoring is a service for monitoring VFD functionality. It includes reading VFD reference and notifications which are affecting to usage of VFD. Also data about the load of the motor and its affects of VFD functionality. All the interfaces have an ability to monitoring VFD's functionality.

2.4 Variable-frequency drive as a part of industrial network

Figure 3 presents an example how the industrial network can be built. There are programmable logic controllers (PLC), which are computers designed for working in the industrial environments. Thus, those are robust computers which can operate real-time environment. PLCs are used for controlling industrial automation process like assembly line and robotics. VFDs are connected to PLCs by a fieldbus, for example. There are two kind of VFDs in the Figure 3. The smaller VFDs are located to the right from the local PC at the bottom of Figure. The boxes to the left of the same local PC are larger VFDs, which are called cabinet-build drives.

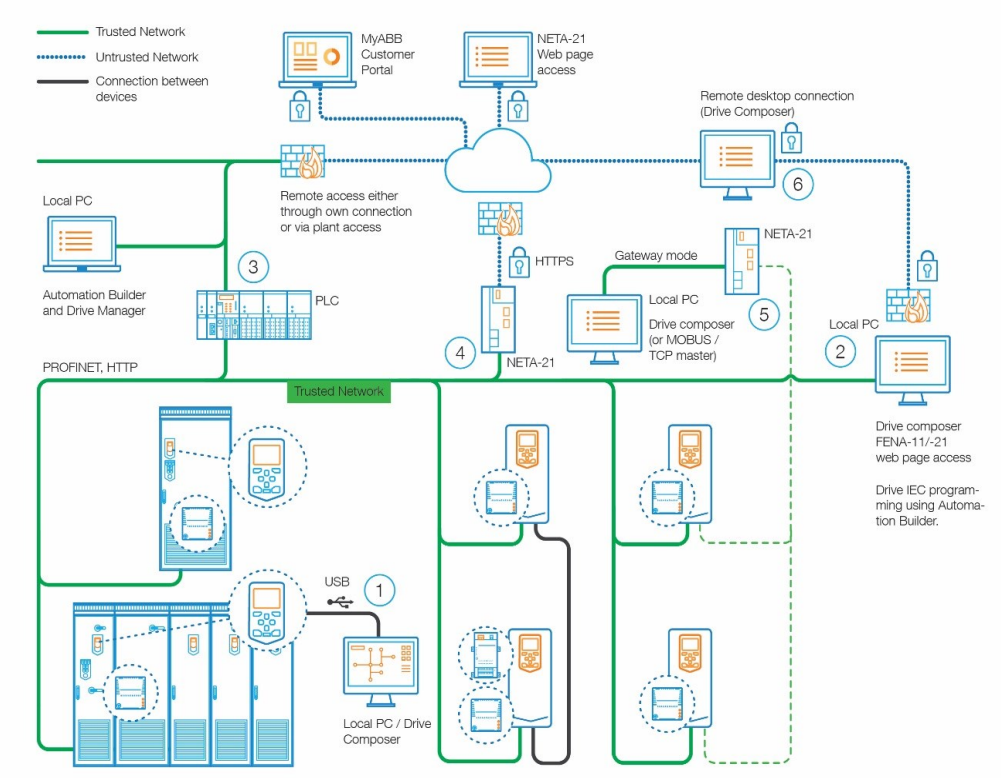

Figure 3. *Industrial network in the VFD point of view (ABB, 2016)*

There can also be a local computer, which has programs to configure VFDs, in the industrial network. The PC programs have an ability to modify and update parameters of VFDs and monitor them. The Table 2 in the sub-chapter 2.3 showed, that PC have a widest access privileges to VFD's services through PC tools, if those are not disabled by configuration parameters.

Figure 3 shows also that there are two VFDs linked together by Drive-to-Drive link, which is a black line in the center of the Figure 3. In the Drive-to-Drive link one device works as a master device and another device works as a slave unit. Another black line in the Figure presents a connection between a panel and a local PC. There is a possibility to connect a local PC to VFD's panel through USB interface and configure the VFD.

Figure 3 presents also that there are firewalls for separating the operational network, where the VFDs are, from the Internet. Messages in the public network are secured by cryptography. There are different solutions, for example, https and virtual private networks (VPN), which are used to secure connections. Although, when there are possibilities to connect to VFDs and other industrial devices from internet, it makes VPNs an attractive target for attackers (Sundell et al. 2012).

Figure 3 presents a cloud service also. Manufacturers have started to collect data from VFDs all over the world. Those VFDs are used in different conditions and environments. For example, it can help manufacturers to forecast maintenance need of VFDs.

3. CYBERSECURITY OF INDUSTRIAL INTERNET

Computer security is for protecting valuable things called assets. According to Pfleeger et al. (2015, p. 2), content, i.e. data, is the thing which makes a computer unique and valuable for its user. Data is an asset but there are also more assets in embedded systems than there are in personal computer security. For example, functions which embedded system enables are an asset for the user. Another asset of industrial devices is safety. It is critical that devices work correctly and do not cause danger to its users and other people by working unexpectedly. Thus, some bug in the program code might change device's behavior and the whole system in a critical moment which could even cost lives. Attacker might want to compromise the functionality of the system and produce damages to people or the system. In other words, ensuring safety of the systems and cybersecurity are strongly tied together.

3.1 Terms and definitions of cybersecurity

There are a couple of terms which are essential to cybersecurity and need to be defined. A *security flaw* means a weakness in the system, which a possible attacker can exploit. Attacker's access to a flaw and a capability to exploit the flaw forms a vulnerability. Computer *bug* means a system's unintended or unexpected action based on intended use. Bugs mainly arise from the systems design or errors made by a programmer. *Threat* means a set of circumstances that could cause harm. (Pfleeger et al. 2015) Bugs can cause security flaws.

There are also a couple of terms in the thesis which should be explained to prevent confusion. Thesis' essential term *industrial system* references to the production systems which include devices used for production.

According to Techopedia (2017) and Industrial Internet Consortium (2017) *Industrial Internet* is combination of devices and intelligent data. In this thesis the term Industrial Internet is used in the same manner as organizations' operational network.

3.2 Communication in industrial Internet

Communication has a critical role in industrial networks. Real-time devices must work together and keep the same pace. Thus, communication between devices is in a critical role when complicated functions are concerned. There are different methods how the communication can be established. Operational network may include devices, like field devices, fieldbuses, control computers, etc. Thus, there are different kind of devices

from multiple vendors. Devices communicate with each other by either fieldbus protocols or Ethernet.

The communication between devices can be abstracted, for example, Open Systems Interconnection model (OSI) is a conceptual model for abstracting communication functions. The model is composed of seven layers and each of the layer has its own purpose. For example, Figure 4 shows the path a message has to travel to another device's application layer. Message has to travel through each layer, from Application Layer to the bottom of the model, which is called Physical Layer. Then the message has to continue in Physical Layer to another device's Physical Layer, and from there to Application Layer. What is notable is that in the model's designing phase in the late 1970s, no layer took cybersecurity explicitly into account (Sundell et al. 2012). This is why layers do not have security built in and because of that other layers do not ensure correctness of other layers' messages. Thus, attack might happen in any level of the model and compromise upper levels. For example, if attacker changes destination address of messages then the messages cannot get to Application Layer (Sundell et al. 2012). Thus, software architects and designers should take the OSI model into account and notice that communication happens in all the seven levels in the model. Designers should answer the question which layer or layers need more protection. Adding security features might cause performance costs. (IIC, 2015.) Thus, VFD designers need to take account performance costs for VFD when adding security features to communication. VFDs are real-time machines, hence, the latency cannot be significant.

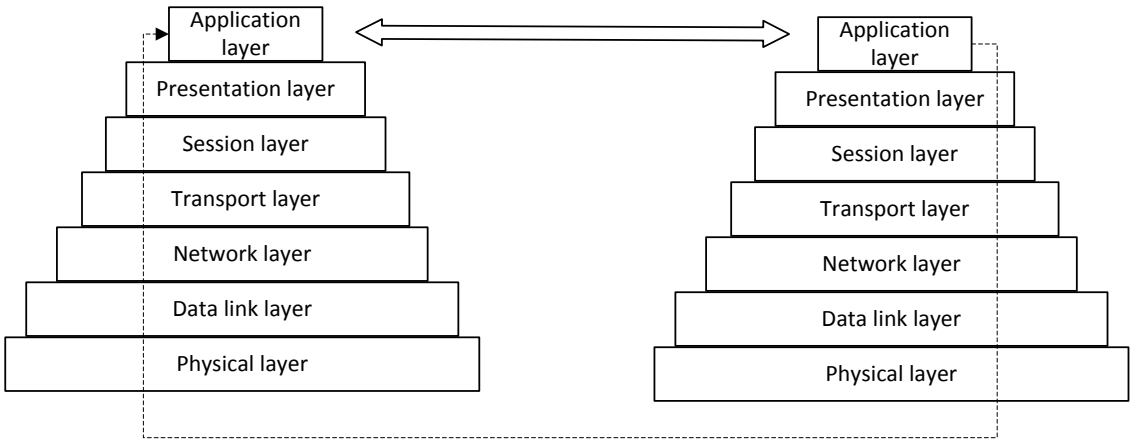

Figure 4. *OSI model*

3.3 Threats to industrial network

The number of security threats against networked devices are increasing. Especially possible attackers got new set of attack tools from an attack tool leak of CIA (MacAskill et al. 2017). An industrial networks' connectivity to the internet enables malicious people to attack remotely against a network and its devices. Although, as Stuxnet case showed, the attacker does not even have to have a remote access to the target system but corrupted USB stick can also spread viruses, for being an example of virus spreading

without networks. More about Stuxnet's attack against an Iranian nuclear power plant is presented in the end of the sub-chapter.

Common threats for machine-to-machine communication are divided into six categories. Those threats apply for the industrial network devices:

1. *Physical attacks* which includes manipulated devices, booting with fraudulent or modified software.
2. *Compromise of credentials* includes attacks against authentication algorithms, tokens, token cloning.
3. *Configuration attacks* includes fraudulent software updates, misconfiguration.
4. *Protocol attacks* includes modification of protocol messages.
5. *Attacks on the core network* includes attacks against routers.
6. *User data and identity privacy attacks* includes stealth of credentials.
   (Cha et al. 2009.)

The list shows that there are various threats for which industrial operators and device manufacturers need to prepare. Manufacturers of VFD can prepare to the points Physical attacks, Compromise of credentials and Protocol attacks. While industrial operators need to protect their factories against attacks on the core network and user data and identity privacy attacks. Defending from the configuration attacks is responsibility of both manufacturer and operator.

Importance of the industrial networks' security has been noted in the Industrial Internet Consortium (IIC) too. IIC have taken cybersecurity into account in their Industrial Network Reference Architecture publication. According to IIC (2015, p. 24), "The enforcement of security policies requires the ability to control various endpoints and their communication involved in an activity in a generic and consistent way to ensure complete end-to-end coverage." IIC presents also four principles how to prevent cyberattacks and prepare for them in a big picture. *Security monitoring* gathers and analyses security-related data continuously as activities are performed. It may take different forms depending on the context of operations and on security events. *Security policy management* manages both automated and human-driven administrative security tasks by documenting their usage and constraints. *Security auditing* "collects, stores and analyses security information related to IIS". *Cryptographic support management* consist of globally interoperable key management, secure credential storage and revocation. (IIC, 2015, p. 24.)

Sundell et al. (2012) recognize two major threats for the field devices of industrial network. Those threats are information leakage and tampering of devices. There are mainly three channels for information leakage. Leakage can happen through an IT leak, human leak or physical leak. Leakages might happen anywhere from device manufacturer's production line to devices' employment place. Tampering of device can happen in two different ways. An attacker can insert spoofed firmware updates or change device parameters through the control PC or device's user interface. There are reasons why an attacker wants to change field devices firmware. An attacker might want to either cause

malfunction to device or improve performance of device. Improved performance of devices brings a threat to device manufacturer in a form of money loss. Less capable devices are priced cheaper than top models. In some cases the hardware and device in cheaper models are the same as in expensive models. In other words, some features are disabled in the cheaper models by the software. (Sundell et al. 2012.) Thus, a device owner may get more features than they have paid for by modifying the device.

A well-known example of an attack against an industrial facility is the Stuxnet case. Stuxnet was an advanced computer worm targeted at nuclear plant of Iran. The facility's network did not have access to the internet. Regardless that there was not access to internet, the virus spread to the system through a contaminated USB memory stick. The code of Stuxnet was written so that it affected only computers, which had a Siemens' Step7 software installed. Step7 is a program for controlling Programmable Logic Controller (PLC) which commands VFDs. VFDs steered motors which controlled centrifuges. First Stuxnet disabled alarms. Then it changed PLC's commands for its own malicious commands. Finally those malicious commands broke approximately 1000 to 2000 centrifuges according to estimates. (Zetter, 2011.)

3.4 Attack process against Industrial system

Before an attacker can perform malicious actions to the system, they need to perform certain steps to break into the system. It is critical to recognize the methods attackers use and how they apply them for implementing functioning mitigation strategies. Infosec Institute proposes seven steps of how successful cyber-attack can be performed:

1. Reconnaissance
2. Scanning
3. Access and Escalation
4. Exfiltration
5. Sustainment
6. Assault
7. Obfuscation (Infosec Institute, 2015.)

Reconnaissance. At first, the attacker identifies the vulnerable targets. Those targets can be persons from all over the target organization including admins or chief executive officer. The attacker needs just a single point of entrance to get started. A common method to gain access is to use different phishing techniques. (Infosec Institute, 2015). Attacker can also gain information from the organization structure and its workforce from the company's website and social media. With deeper knowledge of a target organization it is easier for attacker to launch an attack and gain an access to organization's network.

Scanning. After the attacker has achieved access to organization's network, attacker can start to scan weaknesses. There are different tools available in the internet which can be used to detect weaknesses. This phase of the process might take some time. If the in-

truders are not detected they can spend a long time gathering private data, monitoring communication and mapping the network. (Infosec Institute, 2015.) If the attacker has access to organization's file system, a good practice might be using honey pot defending. The network's admin creates an attractive target for attacker to check. For example, folder with name next year's budget might attract attacker to check. After the attacker enters to the folder, the honey pot program notifies admin that somebody has visited in the folder. Thus, the network admin can investigate if someone is in the network who should not be there.

Access and Escalation. When the weaknesses in the network have been identified, starts the third phase: access and escalation. The phase includes obtaining wider privileges. Thus, attacker can move around more freely in the environment. Attacker's goal is to gain admin privileges. (Infosec Institute, 2015.)

Exfiltration. When an attacker gains admin privileges, attacker "owns" the network. Now the attacker has access to sensitive data. It is called exfiltration phase. An intruder can steal private data with the admin's wider privileges. Attacker can also perform malicious actions, like change or erase files. (Infosec Institute, 2015.)

Sustainment. After the attacker has achieved access with full privileges, starts sustainment phase. It means the attacker stays in the network quietly and monitors the actions of the network. Attacker might install rootkit viruses which make attacker's return to the network and systems easy. Thus, attacker can return as frequently as they want. Because of rootkits or other malicious actions, attacker does not have dependence on a single access point anymore. (Infosec Institute, 2015.)

Assault. Sixth step is assault. Fortunately this step is not taken to use in every attack. In the assault phase attacker modifies target system and attacks against hardware. An attacker might disable hardware entirely as well. In this phase attacker comes visible and stops being invisible. Unfortunately attacker has taken control over the system, so defending the system in this phase might be late. (Infosec Institute, 2015.) Although, best practice might be to run the system down and plug it out from the internet.

Obfuscation. After assault phase comes the last step, obfuscation. Attacker wants to hide their tracks and confuse the victim's examination process of the attack. Log cleaning, misinformation, zombie accounts are tools that attackers are using for hiding their tracks. (Infosec Institute, 2015.)

3.5 Mitigation of threats in the endpoint devices

Previous chapters showed that there are many different types of threats against industrial systems. The chapters described also a process how an attacker performs an attack. Manufacturers can reduce security risks by creating a mitigation strategy. Industrial Internet Consortium has listed methods on how to strengthen the security of devices. Threat mitigations have focused on the industrial networks and their endpoints like, for example, VFDs.

Industrial Internet Consortium proposes good practices to mitigate threats against Industrial Internet devices in their Industrial Internet Reference Architecture (2015, p. 50-56):

- Secure Boot Attestation
- Separation of Security Agent
- Endpoint Identity
- Endpoint Attack Response
- Remote Policy Management
- Logging and Event Management
- Application Sandboxing
- Application Whitelisting
- Network Whitelisting
- Endpoint and Configuration Control
- Dynamically Deployed Countermeasures
- Remote and Automated Endpoint Updates
- Policy Orchestration Across Multiple Endpoints
- Peripheral Devices Management
- Endpoint Storage Management
- Access Control

Secure Boot Attestation is a practice which says that device must start from a known secure state and prevent modification of boot sequence. If the boot sequence is modified unexpectedly, boot system should fail. Failure actions should depend on a security policy. Reporting of failure can be implemented by secure agent. (IIC 2015, p. 51.)

Security Agent is a software that monitors the device. For instance, anti-virus programs are security agents. Security agents have various features for keeping device secure. One feature is logging and event monitoring. It means that every violation of permission leaves a trace. Also user login/logout, data access, configuration changes, application execution and communication are archived in a log. (IIC 2015, p. 51.) The S*eparation of Security Agent* is in this context a practice that the security agent is separated from the other processes and other processes cannot influence it. IIC (2015, p. 51) lists four different methods to separate the security agent: Process-based separation, container-based separation, virtualization-based separation and gateway based separation. The security agent works as a separate process in process-based separation. Container-based separation is a practice where the security agent is separated in the own module which might have an own processor and capabilities for secure memory. Virtualization-based separation means that there are own virtualized operating system for the security agent. Gateway-based separation is practice where the cybersecurity functions in the different device than the target device. The device works as a proxy for the network traffic. (IIC, 2015, p. 51.)

Endpoint Identity means that every device in the industrial network should have an own unique identity. IP, MAC and Bluetooth addresses are used to identify devices. Although, those addresses are easy to change and thus, are easy to fake by an attacker. A

better way to identify a device is to have a cryptographic key to ensure genuineness of the credentials. Hardware is needed to prevent leakages of keys as well. Having a unique identifier also eases authentication of devices. (IIC 2015, p. 52.) Thus, this practice might require the burning of a cryptographic key in the hardware.

Endpoint Attack Response is a practice when the device is under an attack, it should defend itself, report the attack and response to attack based on the security policy. Also, devices should recognize when their peer device is compromised and report it to a security management system. (IIC 2015, p. 52.)

Remote Policy Management is a procedure to keep devices' security policy configuration and functions updated. Central security management system should control the devices' security policy and transfer changes to devices. Security agent is used to authenticate and put into action the security policy in the device. (IIC 2015, p. 52.)

Logging and Event Monitoring is a practice for monitoring and recording events in an endpoint. Events like, security violations, user login or logout, data access, configuration update, application execute and communication should leave a mark into logs. (IIC 2015, p. 53.) In addition, it should be noted that attacker might want to prevent being noticed by changing logs, like the attack process' last phase obfuscation mentioned.

Application Sandboxing is a practice where endpoint devices applications have own separated environment. Applications have limited access to the system resources. Thus, the application cannot damage the system. On the other hand, isolating the application from the system resources, might prevent usage of important resources. (Rouse, 2012.)

Application Whitelisting and *Network Whitelisting* are practices where only certain applications or network addresses are allowed. Other connections or applications are terminated. Whitelists are used to allow scripts, binaries, and libraries in the device. Thus, only certified programs are able to run. Programs which are not allowed to run are terminated and it should leave a mark to the log. (IIC 2015, p. 53.)

Endpoint and Configuration Control is a practice to prevent unauthorized changes to endpoints configuration.

Dynamically Deployed Countermeasures means that security management system should have a capability to create new countermeasures to prevent attacking (IIC 2015, p. 53).

Remote and Automated Endpoint Update is for having the most recent security updates in the machine always. Updates must be automated and performed by a trusted security agent via a secured process. Updates of firmware must be authorized beforehand by a security management system to prevent attackers from installing malicious firmware updates. (IIC 2015, p. 53.) The practice might require sign of the update packages to ensuring that the update packages are not tampered.

Policy Orchestration Across Multiple Endpoints is practice to coordinate security policy across multiple devices. It enables secure workflow between devices. (IIC 2015, p. 54.)

Peripheral devices management means an auxiliary device's controlling policy. USB sticks and such constitute as peripheral devices. Peripheral devices should have their own security policy. Violation to security policy, for example when a peripheral device is disconnected, means that the device is compromised. (IIC, 2015.) The practice means that when the new modules are connected, the device should ensure that it is not maliciously tampered module.

Endpoint Storage Management is a practice to secure data of a device. Whitelists can be used to check which applications or users have access to device's data. Storage management includes files integrity monitoring and encryption of data and software also. Data loss should be prevented and policy violations should be alerted. (IIC 2015, p. 54.)

Access Control is a practice for controlling who and what can control device. It is based on a security policy and let only allowed users to use a device. Access Control should alert security management system for unauthorized access attempts. (IIC 2015, p. 54.) It should be thought carefully who have the right to reset the user's password. Resetting the password should not be too easy to prevent an attacker to guess a password reset questions. For example, governor Palin's personal email was stolen by using email's reset functionality and the attacker found answers to reset questions from the internet (Zetter, 08).

In addition, a practice which is not in the mitigation strategy list is *hardening* or system hardening. It is a set of practices to increase device's security. Hardening means that all the programs which are not used, default passwords, unnecessary services and usernames are disabled. Hardening includes removing unnecessary applications, denying file sharing between programs and using encryption where possible. (Techopedia, 2017.) The hardening should be performed when the devices are moved from the testing and development phase to production.

A good practice for ensuring code level security is to have code reviews. Code reviews for whole code might be too costly, thus threat model can guide to make reviews for the parts of software which are ranked most vulnerable (OWASP, 2016). Hence, all the effort for making software more secure is directed towards most vulnerable areas.

Now the mitigation strategies of devices have been dealt. Although, even if a device is secured, threats might rise from the network itself, so the network needs securing too. Next the thesis will proceed to network security

3.6 Threat mitigation in the Industrial network

Device's security also includes communication security. After the mitigations of the previous chapter are performed device is not completely secured. There can be PLC and

PC that control VFDs in the industrial network, and if network is compromised, an attacker can get control over the devices. Thus, it is also important to secure the network. If the network is insecure, there are methods to increase communication security. Industrial Internet Consortium (2015, p. 55) proposes the following practices to mitigate security risks in communication:

- Mutual Authentication Between Endpoints
- Communication Authorization
- Identity Proxy/ Consolidation Point
- User Authentication and Authorization
- Encryption in Communication

Mutual Authentication Between Endpoints ensures that data is not leaked to unknown parties but communication happens between authenticated parties. In the other hand, authentication might be a too costly function for some smaller devices, like sensors. In these cases it is recommended to use lightweight authentication. (IIC 2015, p. 56.) With authentication malicious devices or entities cannot get control over the device without proper credentials.

Communication Authorization should happen after authentication. It means that when the opposite is authenticated, certain resources are allowed for authenticated party based on the opposite's permissions and security policy. (IIC 2015, p. 56.) Best practice is to give user enough resources to perform necessary tasks and hide all unnecessary features and data-accesses.

Identity Proxy / Consolidation Point can be used for old industrial network devices to perform secure gateways. Identity proxy can also be used for old protocols and devices which do not support authentication otherwise. (IIC, 2015.) Thus, proxy servers can add security to the industrial system, if the network traffic are cycled through it. Having an authentication to older devices is not the only advantages of proxy. It can also log activities of the device. Thus, proxy can also collect logs about the network traffic.

In addition to previous practices, which are focused to the communication between devices, *User Authentication and Authorization* is recommended practice also. Based on a combination of user information and access device's information can be formed a unique access profile. (IIC, 2015.) Thus, security policy can define where and when users are allowed to access to devices.

Encryption in Communication is a practice to secure communication from outsiders by encrypting the communication messages (IIC 2017, p. 56).

3.7 Attacker profiling

It is useful to know what kind of people or organizations might threaten VFDs. First step in profiling an attacker is to find the motivation of attackers. Attackers' motivation depends on the usage and location of VFD. Like described in chapter three, VFDs are

used in industrial environments in this thesis, so attacker might want to steal process knowledge or they might want to sabotage the processes somehow, for example.

There are different types of attackers which are listed in Table 3. Even national agencies are believed to sometimes want to harm devices. For example, Stuxnet is believed produced by governments (Zetter, 11).

According to IBM X-Force® Research report (2016), number of cyber-attacks has decreased a little but at the same time attacks have become more sophisticated. More professional attacks may indicate that organized crime has taken growing interest in cybercrime. Organized crime wants to profit from the attacks by, for example, blackmailing companies by threatening them with attacks to their factories and production processes.

	Resources	**Motivation**
Script kiddies	low	fame, “Can I do it”
Organized crime	medium / high	profit by blackmailing or selling information for competitors
Terrorists	medium	terror
National agency	high	attacking against hostile governments, spying

Table 3. *Different attacker types*

4. CASE STUDY

The following chapter describes how the case study was performed. The target of the case study was Variable-Frequency Drive (VFD), which were presented in the chapter 2.

4.1 Research approach

The study started by finding out the initial status of VFD's cybersecurity by discussing with VFD developers and staff of VFD manufacturer. The result of initial status was that not much has not been done for improving cybersecurity of VFDs. In the first study we discovered that there was a feature made for locking the VFD parameters. We also discovered that the cybersecurity had been a constant and important topic in the discussions after the Stuxnet. Another driver for the improving cybersecurity is a networking of devices. It enables a remote attack against VFDs.

After the state of the cybersecurity of VFDs was studied we started the process to improve the cybersecurity. First we studied the different methods for improving cybersecurity. The best method for improving cybersecurity was to find threats by performing threat modelling and mitigate threats. So we started to study threat modelling and ended up performing attack based threat modelling. A threat modeller should think like an attacker in the attack based threat model. Thus, threats are same as attacks. According to Shostack (2014) threat modelling is all about looking security issues in a bigger picture by abstracting the system. Saitta et al (2005) adds that threat modelling should examine all potential risks of the system and not concentrate only on the place where security flaws are predictable. The attack based threat modelling produces attack vectors which can be presented in an attack tree form. The whole threat collecting process is presented at the sub-chapter 4.2

After the threats were discovered we started to consider mitigation strategies against threats. We discovered a list of threat mitigation practices from Industrial Internet Consortium's publication: *Industrial Internet Reference Architecture*. Based on the attacks we arranged a workshop for prioritisation of the mitigation strategies. More discussion about the prioritisation and prioritisation method is presented in the sub-chapter 4.3.

4.2 Threat mitigation process description for variable-frequency drives

Figure 5 illustrates the thesis' threat modelling process for VFD. The process is divided into three phases: initialisation phase, threat modelling phase and updating phase. The

process is based on a discussion with an experienced design manager in a VFD manufacturer company. The discussion gave a foundation of the threats and knowledge where to start searching for more threats. The design manager suggested that I should discuss with the senior developers in charge of the operating system and various internal modules. Literature supports the idea of discussing threats with various developers

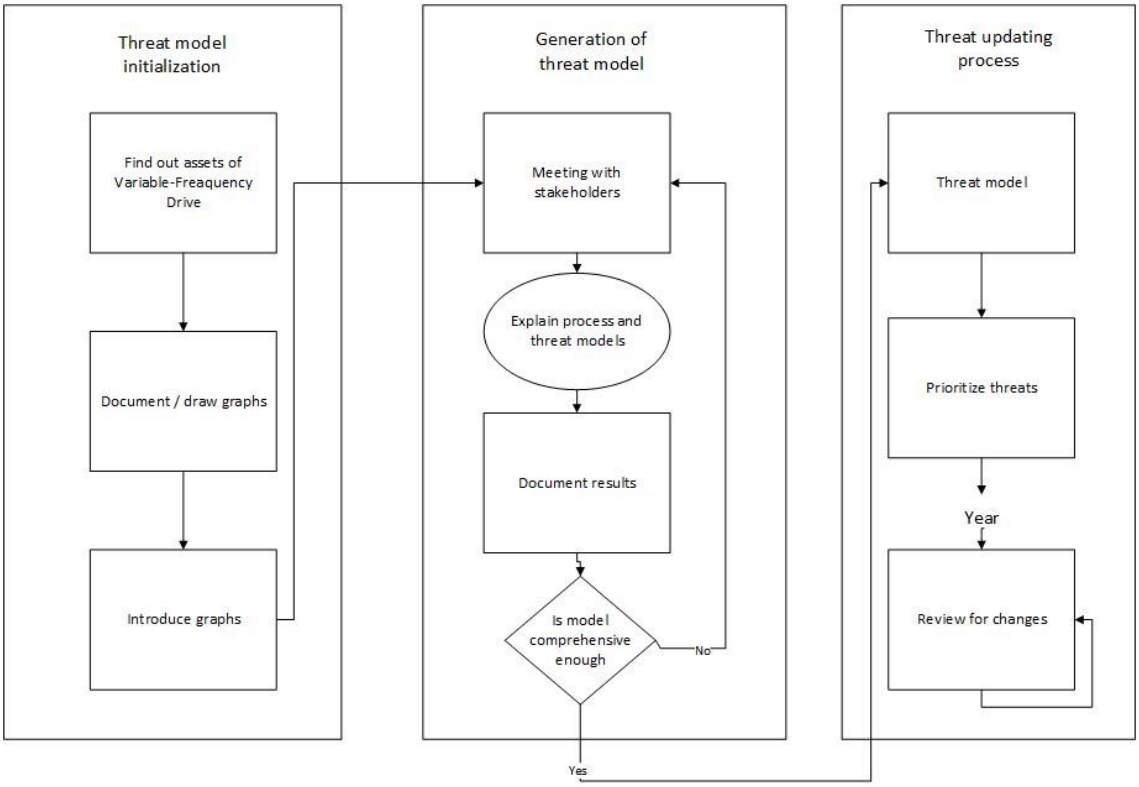

Figure 5. *Threat modelling process*

First phase of the process is to initialize threat modelling for VFD. It consists of finding VFD's assets. This step requires a person with thorough knowledge of devices, their content and usage. In this phase a sketch of an attack tree is created. After the attack tree has been created, it is presented to the design manager who gives feedback on it.

In the second phase of the process, actual threat modelling begins with stakeholder meetings. Stakeholders are selected based on their area of expertise. The meetings are held one-on-one because the format eases explaining the model to the stakeholders. In addition, one-on-one conversation lowers the threshold to propose new ideas; there may be some dominant individuals in a group conversation. It leads to a situation where quiet people are not willing to present their ideas. At the beginning of each meeting the term ‘asset’ is defined and found assets are listed. It is important to properly define the terminology before moving the discussion to other topics. Then follows a discussion concerning the validity of those assets. Also questions of possibly having more assets and whether the already collected threats are valid threats, should be stated at this stage. After that the interfaces are presented and explained to developers. It is critical in these meetings to achieve a common understanding of the assets, the attack tree graph and threats. When the individual interviews are completed, a group interview is held. All the

possible attacks were found in the previous meetings are presented in the meeting and after that the rest of the meeting should be used discussing and analysing the threats and attacks. Benefits of the group interview come from the common understanding of the threats and possible attacks. Thus, stakeholders can expand a scope and increase knowledge of attacks.

When the model is ready, actual threat modelling does not stop there. New threats occur when the technology evolves. This leads to a situation where the threat model should be updated regularly.

4.3 Prioritisation method of VFD mitigation strategies

There are some factors which should be taken into account when prioritizing the mitigation strategies. One prioritization factor is how easy it is to apply these strategies. Does implementing the strategies require some kind of special expertise or can those strategies be implemented easily? For example, authentication could be easy to put into practice but it could demand authentication capability from other devices. Thus, the practice might be easy to implement but it does not give full protection if other devices do not support it. Another point is the question of what strategies fulfil each other. Does the chosen strategy provide support for implementing other strategies? Is it necessary to implement strategies in a certain order?

There are many ways to prioritise mitigation strategies. In this thesis two prioritisation methods were considered. First method was Weighted Shortest Job First (WSJF) method. The second method was to use well known list of attacks to prioritise mitigation strategies. For example, this kind of list is an OWASP's top 10 application security risks.

The newest version of the list is from 2017:

1. Injection
2. Broken authentication or session management
3. Cross-site scripting
4. Broken access control
5. Security misconfiguration
6. Sensitive data-exposure
7. Insufficient attack protection
8. Cross-site request forgery
9. Using components with known vulnerabilities
10. Unprotected APIs (OWASP, 2017)

The OWASP threats list is focused on web applications. Industrial devices differ from web applications by their nature of accessibility and lifecycle. So, top ten attacks are not strictly applicable for prioritization of mitigation strategies. Although, the list can give

hints where to focus development efforts on after basic mitigation strategies are fulfilled.

Another prioritisation method WSJF is a simple function to determine prioritization of software features. It is calculated by the following formula:

$$WSJF = \frac{Business\ Value + Time\ Criticality + Risk\ Reduction}{Job\ Size}$$

Business value in the formula describes how much the threat mitigation practice impacts the customer experience. Is there a penalty of delay or other negative impacts for manufacturer? Time Criticality means importance of timing when the feature is delivered. If a feature is delayed, does it cost the customer some potential business value? Risk Reduction: Does this reduce risks or does neglecting it affect in a negative way. Job Size means how much implementation takes time. Value of Job Size comes from comparing different features. For example, story points are good indicators of feature's size (Scaled agile framework, 2017).

WSJF is more suitable for prioritisation in this case than OWASP's top 10 list. The prioritisation with WSJF needs a wide group of specialists, so the results of prioritisation is relevant for VFD manufacturers.

The chosen method WSJF needed a broad view for development of VFDs and knowledge from many stakeholders to be more effective. Thus, we needed to organize a workshop for prioritising the mitigation strategies. The workshop's invitations were sent by email and the location was VFD manufacturer's meeting room. The invitation mail included short description of WSJF method and list of mitigation strategies to be prioritised. The stakeholders were selected from different units and area of expertise. There were product managers from different usage fields of VFD, developers and architect. Because of a broad expertise of attendees we had the best view of future development of VFDs and future customer requirements.

The workshop was structured as follows: First we agreed prioritisation method, which was Weighted Shortest Job First (WSJF) method. The method was already familiar for stakeholders so we did not have to spend a lot of time for understanding the prioritisation method. The method uses Fibonacci series for giving priorities to targets. Thus, we agreed in the workshop to use same kind of numbers than there are in Fibonacci series: 1,2,3,5,8,13,20,30,40 where 40 was highest priority in the Business Value, Time Criticality, Risk Reduction fields whereas 1 was fastest job to perform and 40 most difficult to perform in the Job Size field. The numbers were selected because those were included in the method. The values are relative to each other and the values does not represent any single unit, like a day or a week. First there should be selected a smallest job and other items are compared to it and prioritised. The Fibonacci series is good option in the

prioritisation of largest numbers because the numbers are further apart, hence, it is easier to give values for jobs between numbers 13 and 21 than deciding between numbers 13 and 14 (Brown, 2015). The possible results of the formula are between 0.075 and 120.

After the method was presented to all of the attendees, we had a short conversation about the mitigation strategies. What those practices were, how those affect to security and were there requirements for some features already.

When everything was clear, we started voting. We all had cards where was Fibonacci numbers. Then we voted by showing the card at the same time, so that no one would copy others' voting numbers, and that we would get a propriety view of everyone. The voting went without confusions. Some of the mitigation strategies lead to discussion about the implementation and need of the feature in some specific cases.

We had reserved an hour to meeting but the beginning of the workshop took so much time that we had only time to have a long discussion about the Business Value of every item. The two factors: Time Criticality and Risk Reduction we went through without deeper discussions. After the Risk Reduction the time was up and values of Job Sizes were missing. We agreed that everyone will give their estimates of Job Sizes by email. At the end we had only two answers of Job Size by email. The Job Size values are average of the two answers.

5. RESULTS

This chapter presents the results from the case study. The results are presented in the same order that the findings were found during the threat mitigation process. Hence, first the assets of VFD are presented. Availability of interfaces are discussed after the assets sub-chapter. The attacks against VFD are presented in sub-chapter 5.3. After it the results of the study of VFD's mitigation strategies are presented. After the mitigation strategies the not applied mitigation strategies are arranged by the results of workshop. Finally discussion ends the chapter.

5.1 Assets

Threat modelling started by finding what is needed to protect, i.e., which are the assets of the VFD. The recognised assets are presented in the Table 4

Name	Explanation
VFD works like expected	VFD works in full capacity and the way it is configured
Intellectual Property	VFD does not leak information to competitors. This also includes manufacturers' intellectual property.
Safety	Related to the asset of the "VFD works like expected" but emphasizes VFD's functionality in the failure cases and cases where harm can happen to humans.
Legislation	Trading agreements do not allow to export VFDs to countries which might use them in military purposes, like in process to enrich uranium for nuclear weapons.

Table 4. *Assets of VFDs*

The study recognized four assets concerning the VFD. The main asset is that VFD works like expected. It means that VFD is configured properly by instructions of a manufacturer. In addition, VFD obeys commands which it gets from the user. Thus, the asset is strongly related to the safety asset. Safety asset means that VFD should not cause any damage to humans. For example, if repairer is performing maintenance inside a machine, machine cannot start unexpectedly.

Legislation can be an asset also. Selling VFDs that have a capability to enrich uranium to countries which might have an interest to develop nuclear weapons is restricted by trading agreements. For example, United States have set restrictions of potential military-use items exporting to North Korea (Noland, 2004).

Intellectual property asset means that VFD does not leak any information to outsiders. The asset includes also intellectual property of a manufacturer. For example, how VFD's torque control is designed is an intellectual property which VFD manufacturers want to keep secret.

5.2 Availability of interfaces

Availability is in critical role when malicious persons are trying to achieve their goal of compromising VFD. The best defence method has been for a long time isolating production environment from the organization's information network and from the internet. Because that situation is changing, and users can have a remote access to production environment from organizations' network, attackers might be capable of attacking remotely against VFDs. Isolating VFD and industrial network makes attacking against them more difficult. On the other hand, computer worms can spread to the industrial network though they are isolated. For example, the Stuxnet worm spread to the isolated environment.

A considerable thing in availability is whether the attack needs physical access to a device or can attacks be generated remotely. For example, if an attacker wants to just stop VFD and motors, there are many different interfaces, which allow to stop motor or disturb its functionality. For example, modification of encoder I/O signal can modify control of the VFD except, this requires physical access to cables between motor and VFD. However, if the attacker can achieve a physical access to devices, there have been security weaknesses in the organization access control.

5.3 Attack tree

An attack tree is a form to present attack vectors. The attack tree is presented in the Figure 6. The attack tree is based on discussions with stakeholders and their perceptions about weaknesses of VFD and potential attacks which might threaten VFD. There are connections between different elements in the attack tree. However, in this thesis it was difficult to present how the attacks proceed because the attacks were possible to be performed through multiple different interfaces. Thus, the interfaces box is abstracted to include all the interfaces.

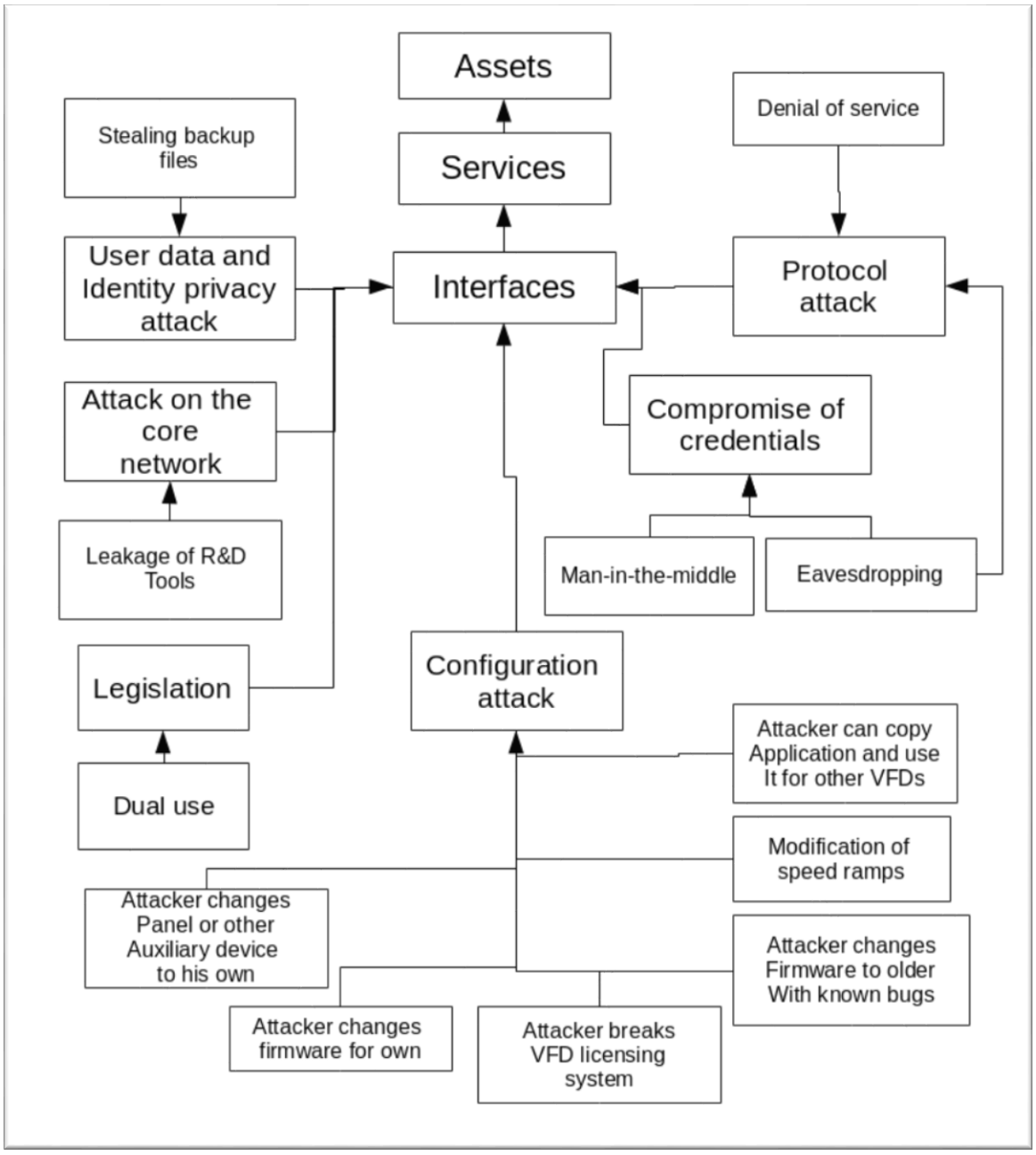

Figure 6. *Attack tree*

First level of the attack tree is assets, which were presented in the sub-chapter 5.1. Below the assets level is a services level. VFD's services and their interface access are presented in the sub-chapter 2.3. There are VFD's interfaces represented below the services box. Lowest boxes of the tree describe attacks against VFD. The attacks are presented later and every attack has its own dedicated table for describing it.

The services and interfaces row describes what kind of setup enables attacks. For example, if an attacker wants to stop VFD, they can use any interface which has a capability to prevent VFD running in order to launch an attack. More sophisticated attacks, for example, logic bombs need a certain route, like modification of firmware or controlling local PC.

Content of assets, services and interfaces boxes of the Figure 6 are expanded in the Figures 7, 8 and 9. The Figure which included all the attacks, interfaces, services and assets was too wide to presented as in one figure, thus the attack tree is simplified by abstracting Interfaces, services and assets. The assets are listed in the Figure 7. The Figure 8 presents services which were listed in the sub-chapter 2.3. VFD's interfaces, which were listed in the sub-chapter 2.2, is presented in the Figure 9.

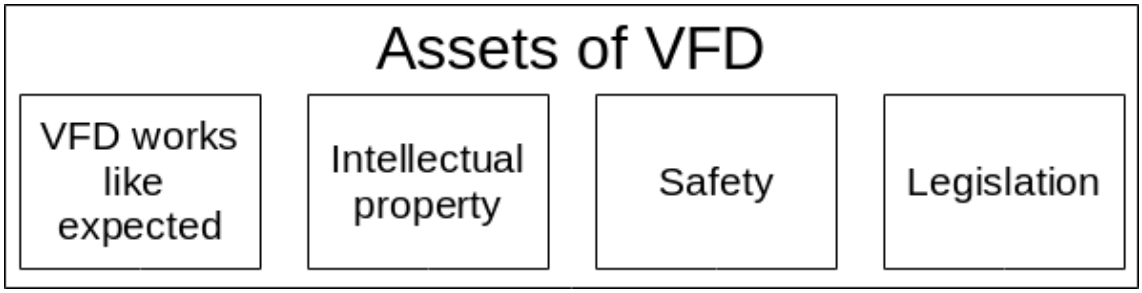

Figure 7. *Assets of VFD*

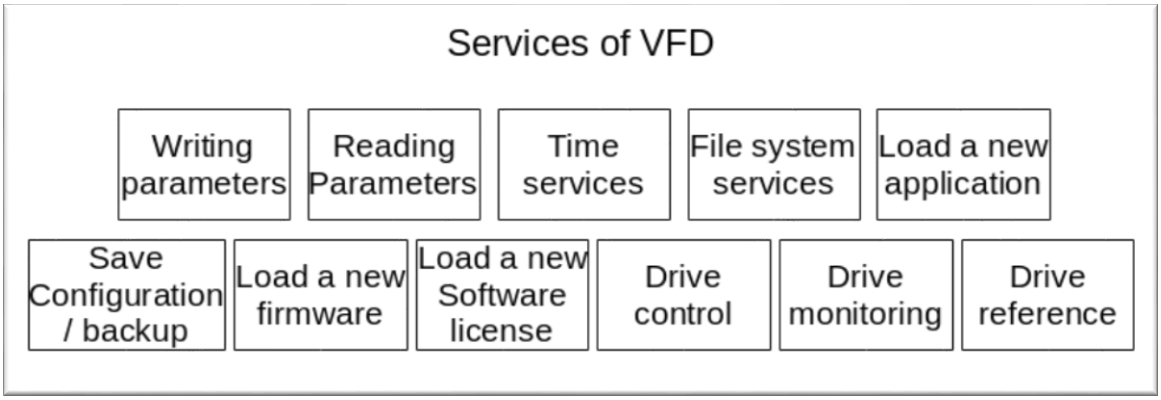

Figure 8. *Services of VFD*

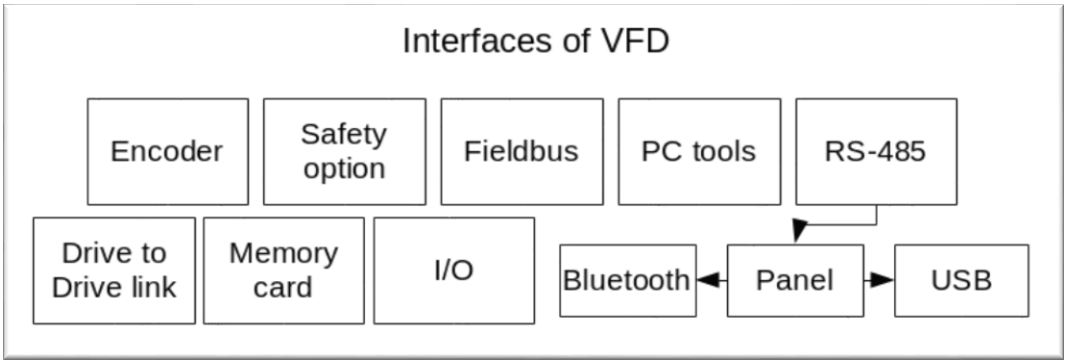

Figure 9. *Interfaces of VFD*

5.4 Attacks

Attacks which were found in the discussions with the stakeholders are presented in the tables below. The list is not all-inclusive but it presents all of the attack vectors this group of subject-matter experts identified during one round of threat modelling. The list should be updated constantly when new threats are found, if manufacturers want to keep their VFDs secure.

The found attacks are listed in the Table 5. The Table have different fields describing attacks. Fields are: Category, What, Why, How, Difficulty and Severity. Table's row what is the attack's name. Table's row why answers the question why attacker might want to attack in the described manner for the certain component. It describes also what an attacker can possible benefit from the attack. Table's row how describes how the attack might be performed. It describes also what attacker needs to take into account while attacking. Table's row difficulty gives an estimate how difficult the attack is to perform. Table's row severity is estimation how effective succeed attack might be. Number three is broadest impact and number one is lowest impact. Some of the rows are left to blank because those rows might need the knowledge of different kind of experts which were not available while the attacks were discussed and invented.

The category row maps attacks to the categories which are presented in the chapter 3.3. The categories are: *Physical attacks*, *Compromise of credentials*, *Configuration attacks*, *Protocol attacks*, *Attacks on the core network*, *User data and identity privacy attacks*. Categories are used to detect which parts of the system are more vulnerable than other parts

Category	**Compromise of credentials**
What	Eavesdropping
Why	Competitor might get data about machine utilization and the production processes. Also attacker can take control of VFD if message protocol is easy to study.
How	Attacker gains an access to a network and listens VFD's messages.
Difficulty	1. Messages are not encrypted so listening is easy. Most difficult factor in the attack is to gain an access to the network.
Severity	3

Category	**Compromise of credentials**
What	Man-in-the-middle
Why	Attacker wants to compromise a VFD or devices which are depending on VFD. Attacker can also take control of VFD.
How	Attacker have investigated the VFD's messaging protocol and places a computer into middle

	of communication link of VFD and device which is controlling VFD. Thus, attacker can either prevent messages from VFD to controller and opposite. Attacker can also send fake messages to both of devices and create confusion and malfunction to operator.
Difficulty	2. Messages are not encrypted so listening of messages is not difficult. Most difficult factor in the attack is to gain an access to the network.
Severity	3. Depending on the quality of credentials.

Category	**Configuration attack**
What	Modification of speed ramps
Why	Attacker wants to damage devices which are run by VFD.
How	There are parameters for setting speed ramps and limits. Manipulating them can remove speed ramps.
Difficulty	1. If parameters are not locked, it is easy to delete speed ramps by fieldbus or PC tools.
Severity	2.

Category	**Configuration attack**
What	Attacker changes firmware for his/her own.
Why	Attacker can launch attack at the worst moment and cause damage. Attacker can also use this to collect information about competitor.
How	-
Difficulty	3. Attacker should have a lot of knowledge about VFD's internal processes. For example, target VFD consist of three parts and the parts need a correct license key to work together. Getting the license keys might be difficult.
Severity	3

Category	**Configuration attack**
What	Attacker changes firmware to older version with known bugs
Why	Attacker can damage the process
How	Attacker changes firmware version to older which has the known bugs and utilizes bugs to harm process of target user.
Difficulty	3
Severity	1

Category	Configuration attack
What	Attacker breaks VFD licensing system
Why	Attacker wants more features or higher power output.
How	Attacker breaks into VFD licensing system and copies the higher level license to cheaper units to get more features.
Difficulty	2
Severity	1

Category	Configuration attack
What	Attacker changes panel or other auxiliary device for his own.
Why	Attacker wants to have a control over a device. For example, panel is easy to change and it has wide service access. Thus, attacker can use panel to collect information about the usage of VFD.
How	Attacker must reverse engineer an auxiliary device's firmware and study the protocol which is used to communicate with VFD.
Difficulty	2. There is a parameter value for disabling panel or fieldbus control. Thus, properly configured VFD can be protected against attacks.
Severity	3

Category	Configuration attacks
What	Attacker can copy a VFD application and use it for other VFDs
Why	VFD's applications are allowed only paying customers.
How	The applications are distributed by flash sticks. An attacker copies flash stick to computer memory and creates a new stick from copy.
Difficulty	2
Severity	2

Category	Protocol attack
What	Denial of service
Why	Paralyzing a production process.
How	Attacker sends a constant flood of messages to VFD trying to paralyze it.
Difficulty	1. Attacker needs an access to the industrial network where VFD is located. Denial of ser-

	vice tools for PC are available in the internet, so the biggest difficulty comes from getting an access to network
Severity	2

Category	**Attacks on the core network**
What	Leakage of R&D tools
Why	R&D tools have capability to read and write to every memory slot of the VFD if the feature is not disabled from the parameters.
How	Attacker bribe manufacture's R&D workers to get the program or try to steal repairer's PC.
Difficulty	2
Severity	3

Category	**User data and identity privacy attack**
What	Stealing the backup files
Why	Backups store VFD parameters. For example, attacker might want to calculate production volume or map the organizations process to copy it.
How	Attacker might get backups from careless distribution of the backups.
Difficulty	1
Severity	2

Category	**Legislation**
What	Dual-use
Why	Exporting VFDs, which can be used for military use purposes, like enriching uranium, to some countries is denied by international trading agreements.
How	Attacker needs a correct license to enable VFD's dual-use feature. The correct license can be stolen from VFD which supports frequency of dual-use.
Difficulty	2
Severity	2

Table 5. *Attacks against VFD*

5.5 Description of mitigation strategies in VFD context

This sub-chapter describes the mitigation strategies and how those strategies can be applied into the VFD.

Separation of security agent is a practice in VFD context where a single module called security agent is separated from other code. It means that the security agent is hardened and there is not an easy way for an attacker to disable security agent or disturb it. This practice can be produced by creating a new container-based separation and older VFDs can be protected by gateway based separation. Although, Gateway-based separation have a weakness if the attacker have an access to the device. Hence, attacker can bypass the security agent by just connecting straight to VFD through panel or other interface.

Endpoint Identity is a strategy where VFD recognizes other devices in the network. The strategy is essential for authorization. VFD's communication process is a master-slave method, which gives full control to master. Thus, it is critical to know who is a master. IP, MAC and Bluetooth addresses can be used for the identifiers but those can be spoofed.

Remote Policy Management could be, in a VFD context, a central program or a cloud service which updates VFD's security agent to deal with new threats when new threats occur. Although, the identification of cloud service or a central program must be secured by authentication and messages are needed to be encrypted because if a malicious person can perform man-in-the-middle attack, that person can inject malicious code to VFD.

Logging and Event Management is a strategy to store data about user actions, parameter change, configuration change and new IEC 61131-3 programs. By logging it is easy to track what went wrong and later investigate attack path if attacks happen. It can also help VFD developers in debugging computer bugs. With endpoint identity practice can be tracked where the attacker accessed to the VFD.

Application Sandboxing can mean that if users have an opportunity to create own applications, its functionality is limited to a sandbox. VFD can be programmed by IEC 61131-3 programming languages and application sandboxing can limit certain functionality of the languages.

Endpoint and Configuration Control to prevent unauthorized change to the endpoints. This practice was fulfilled by the parameter lock. It prevents an unauthorized person, which is a person who are not allowed to access to the system, to change the parameters of VFD.

Dynamically Deployed Countermeasures means that VFD can alert security system that it is under attack and create new counter measures against attacks.

Remote and Automated Endpoint Update is a strategy for updating operating system and programs of VFD remotely.

Peripheral Devices Management. VFD have external options like panel and different option modules like safety module. The strategy means that the option modules must be authenticated with the VFD. The strategy prevents a usage of a modified panel. Thus, for implementing this strategy peripheral devices need to have a signature which should be verified from a VFD every time when a device is plugged in.

Endpoint Storage Management means taking care of the integrity and encryption of data. In the VFD's context it can mean encrypting file system, encrypting IEC 61131-3 applications, encryption of backups.

Access Control in VFD means that only authorized users are allowed to use it. The access control can be performed by password, for example. There are a couple of access control practices taken in use at VFD. User lock prevents unauthorized users to change the passwords. There are also parameters which can exclude connection types like fieldbus and Bluetooth connections and those parameters can also disable some PC tools which are used for debugging.

Mutual Authentication between Endpoints means that VFD can recognise other parties in the network and authenticates with them. This is practically setting authentication protocols and credentials for authentication. It might be a good practice to implement this feature in the security agent.

Communication Authorization means in VFD context that only recognized parties can communicate with VFD. When the opposite is recognized, VFD can provide certain resources which are allowed to the opposite.

Identity Proxy/ Consolidation point practice can be taken in use if the VFDs are spread in the different locations, for example, VFDs which are not in the same network. Thus, the communication between VFD's which does not support the encryption of messages can have encryption, if the proxy is responsible of sending the communication messages. The proxy can implement higher cybersecurity standards in communication than VFD. With the practice security-gateway can be produced (IIC 2015, p. 56).

User Authentication and Authorization is a practice where user is identified. Depending on user access level user can either change parameters get access to other VFD's services.

Encryption Communication is a practice where messages between VFD and other communication parties are encrypted. Without encryption the attackers can produce eavesdropping attack easily and study what kind of communication happens between VFD and other industrial Internet devices. On the other hand, encrypting and decrypting might be a costly process for the field devices calculating power. Those devices might

not have efficient processors to encrypt and decrypt messages and work in the real-time at the same moment.

5.6 Applying mitigation strategies for VFDs

The sub-chapters 3.5 and 3.6 described different threat mitigation strategies that could be applied to industrial network devices, such as VFDs. The sub-chapter 5.5 described what those strategies mean in VFD's context. This chapter maps which mitigation strategies are already applied in the VFDs. Based on this review it is later possible to suggest new strategies to be worth of considering what it comes to increasing the security of VFDs.

The Table 6 presents which mitigation strategies are being used in VFDs, both to the device itself and its network communication. The Table consists of mitigation strategies presented in sub-chapter 3.5 and 3.6.

Mitigation strategy:	**Yes**	**No**
Secure Boot	X	
Separation of Security Agent		X
Endpoint Identity	X	
Remote Policy Management		X
Logging and Event Management		X
Application Sandboxing		X
Application Whitelisting		X
Endpoint and Configuration Control	X	
Dynamically Deployed Countermeasures		X
Remote and Automated Endpoint Update	X	
Peripheral Devices Management		X
Endpoint Storage Management		X
Access Control		X
Mutual Authentication Between Endpoints		X
Communication Authorization		X
Identity Proxy/ Consolidation point		X
User Authentication and Authorization		X
Encryption Communication		X

Table 6. *Applied mitigation strategies of VFDs*

As the Table 6 shows, there are a couple of strategies being applied. The applied strategies were *Secure Boot*, *Endpoint Identity* and *Remote and Automated Endpoint Update*. Although, the secure boot strategy is applied, it could be enhanced to give better protection by burning crypto key to the hardware. Varghese and Bose (2014) suggest that making boot more secure can be accomplished by burning bootloader firmware image into embedded controller. Thus, encryption key is embedded to the hardware and cannot

be changed. This enables secure boot and can get rid of hardware tampering. Hence, pre bootloader can be secured also.

Access control requirement was partly satisfied by user lock. User lock locked the VFD's parameters from change by password. In addition, Bluetooth connection can be denied, writing to file system can be denied and running the adaptive programming programs can denied too.

The Table 6 shows also that the assumption of the introduction that security of VFD has count upon isolation of the environment is true. Therefore more mitigation strategies are not taken in use. Some of the strategies are not directly applied for the VFD or need support for other devices of industrial Internet. For example, Identity Proxy / Consolidation Point is probably an easiest strategy to add security to communication between VFDs and other devices of industrial Internet. Although, identity proxy does not remove a weaknesses of an actual device. Thus, an attacker who can get physical access to device can cause harm in the same manner than earlier.

The messages of VFD are sent with no encryption and VFD does not identify the receiver. Messages over internet are encrypted in turn. Thus, attacker can more easily attack against communication of industrial network. In addition, sub-chapter 2.2 discussed that common industrial protocols, which VFDs are using, do not support authentication. Hence, it gives an easier ground for attacker to perform malicious actions. Unencrypted and not authenticated devices removes attack phase 3 from the attack process of sub-chapter 3.4. Attacker does not need to get privileges, if attacker can get access to network.

5.7 Prioritized mitigation list

The result of performed mitigation strategy prioritisation meeting is presented in the Table 7. Mitigation strategies: Security Agent and Separation of Security agent were left out of the prioritisation because the mitigation strategies were unclear in the meeting so those practices were left without values. In the prioritisation workshop were also a discussion that the practice Separation of Security Agent needs an implementation of a Security Agent practice first. Thus, those strategies are inseparable.

The scale of values start from a value 0,286 and ends to value 11,125. The scale of voting numbers were in Fibonacchi series but in the workshop some attendees wanted to increase importance of some features, thus, there are numbers 21 and 34 in some fields.

Mitigation:	Business Value	Time Criticality	Risk Reduction	Job Size	Value
Security Agent	-	-	-	-	-
Separation of Security Agent	-	-	-	-	-
Endpoint Identity	13	5	5	5	4,6
Logging and Event Management	13	20	20	5	10,6

Application Sandboxing	3	5	5	13	2
Application Whitelisting	2	5	5	8	0,875
Dynamically Deployed Countermeasures	1	5	5	21	0,286
Peripheral Devices Management	13	5	13	13	2,385
Endpoint Storage Management	8	5	5	8	2,25
Access Control	21	34	34	8	11,125
Mutual Authentication between Endpoints	13	13	5	13	2,385
Communication Authorization	21	5	5	8	3,875
Identity Proxy/ Consolidation Point	8	5	20	5	6,6
User Authentication and Authorization	21	40	40	13	7,769
Encryption Communication	8	5	5	8	2,25

Table 7. *Prioritised mitigation strategies*

The access control turn out to be a priority number one based on values of the Table 7. The practice got 11,125 points from the WSJF formula. Next significant feature was a Logging and Event Management with the points 10,6. Third practice to implemented was User Authentication and Authorization. The User Authentication and Authorization was requested by some customers, thus, Time Criticality and Business Value were high for the feature. There were also requirements for the Access Control so it got high values too.

The strategy which got lowest points was Dynamically Deployed Countermeasures. Second lowest value was for Application Whitelisting. Dynamically Deployed Countermeasures were seen as a little confusing practice and attendees of prioritisation workshop did not recognize as much business value for it than in other practices. Notable is that Application Whitelisting and Application Sandboxing got low points in business value also. Thus, the practices which are most likely to focus internal operations of VFD are not seen as important as cybersecurity features which are related to networking. The results can be explained by the expertise of the workshop attendees. The product managers listen customer requirements and customers have more focus on the whole network security. Then the focus is not as much in the internal security of VFD than it might be with the developers of operating system of VFD.

5.8 Discussion

The thesis got started from a requirement that business unit of a large manufacturer must perform a threat modelling for its product. The business unit's product is VFD so the thesis started with the goal to perform a threat modelling for VFD. Basics of threat modelling were found from Olli Penttilä's master thesis, which focused threat modelling in maritime container terminal automation systems (Penttilä, 2016).

After the attacks were collected, the thoughts about the threat modelling changed. The initial goal was to increase security of VFDs but the collected attacks did not answer to the need. Thus, answer to need was to apply mitigation strategies. The found attacks

were useful for selecting mitigation strategies to the thesis. The attacks gave a hint which mitigation strategies were relevant against the know attacks.

During the attack collecting phase it was noticed that it is difficult to give a certain numbers for attack's severity or difficulty to prioritise them. Initial idea of the categories was to categorize attacks if those can be performed remotely or do attacks need a physical access to device. Thus, many of found attacks were difficult to categorize because of there were many ways to perform them. The idea of categories were discarded because many of the attacks could be performed remotely through different devices and using protocols or with physical access to device. Hence, categorizing attacks to remote and physical access attacks did not have any value.

The thesis got a newer form when the Industrial Internet Consortium's Reference Architecture publication was found. There were taken into account the cybersecurity of Industrial Internet device and mitigation strategies for threats. The publication created a base of enhancing cybersecurity of VFDs. Thus, the thesis can be criticized for relying too much for the one publication. Although, the mitigation strategies of Reference Architecture are reasonable and source is trusted though source is not the easy to understand. The presented mitigation strategies are basic strategies which are good to be implemented before more advanced practices. For example, cryptography is mandatory practice in the web applications. Hence, the message encrypting might be better implement before the buffer overflows of operating system. If the messages are not encrypted an attacker does not have to study operating system vulnerabilities but an attacker can take control of VFD only by studying networking protocols and using them against VFD.

The number of found attacks in the thesis was enough for the thesis scope, but for the developing more secure VFDs it might be good idea for implementing the mitigation strategies and after the implementation to take a look which attacks are still valid. Then it is a good time to perform threat modelling again with deeper knowledge of VFD. A subsequent threat modelling exercise might guide to implement more advanced practices.

Software developers from a VFD manufacturer were interviewed in the attack collecting phase. Thus, the view of threats is a quite succinct. Wider view of threats might be achieved by interviewing cybersecurity specialists. Although, cybersecurity experts are not likely to have as good knowledge of VFD as developers of VFD but they might have a deeper knowledge of industrial network and the protocols. Also the security is as strong as the weakest link of the chain, it is also recommended to have a threat modelling for the full network where VFDs are operating for gaining a better protection.

The thesis prioritization method Weighted Shortest Job First (WSJF) can be criticized from the emphasis of Job Size. Even though if the Business Value, Time Criticality and Risk Reduction have a high values, partitioning by high value of Job Size directs working towards jobs with smaller divisors. Hence, the smallest job is more likely to be a most important job.

The result of prioritization can be criticized about the Job Size. There were only two answers considering the values of them and the values were received by email. Thus, the deeper discussion of job sizes were missing. Hence, we can argue that the Job Size does not describe the situation. On the other hand, the prioritisation of Job Size would be more realistic if there have been developers in the prioritisation workshop. The attendees of workshop were only business people, so the insights focused more on the business value of different strategies. On the other hand, values of Job Size cannot be as accurate as values in Business Value, Time Criticality and Risk Reduction because of Job Size cannot be accurate if the practice has not divided into tasks. The size of tasks can be estimated and then the Job Size can be estimated based on the mitigation strategy's tasks sizes.

Perhaps the most difficult issue in the prioritisation workshop was to achieve a common understanding of different mitigation strategies and what those strategies meant in the VFD context. Thus, some of practices might have been a little unclear in the prioritisation workshop. Better preparations for workshop would give better results but the workshop was needed to arrange under short notice time because of attendees were busy and there were confusion in the meeting invitations.

It is important to notice that mitigation strategies which are presented in the thesis are just a beginning and the strategies will not give a full protection against attackers. More likely the strategies gives basic protection for VFDs and, thus, might lead attackers to attack against VFD through other devices in the organization network. In addition, it has to be notified that there are devices which use old protocols in the same networks with VFDs, hence, transition to use newer more secure protocols might take a longer time depending on the other devices in the network and support of those devices.

Another important aspect in the implementation is that target devices are working in real-time, thus, those do not have possibility to perform expensive calculations. Also resources of the VFDs are limited, hence, it might be difficult to implement most sophisticated features. The life cycle of VFD's are long, thus, it is impossible to forecast what kind of threats VFDs can face in the future. Hence, practices which ease to updating the VFD's cybersecurity remotely is important.

Results of the thesis were what was expected. There has not been done much in protecting VFD's against cyberattacks. The protection against attackers have been dealt with by the guards and locks this far. Thus, the thesis gives a good recommendations about where to focus development efforts next. However, manufacturers are not probably going to improve cybersecurity of their devices if clients does not require the cybersecurity features. However, having a good cybersecurity might give a competitive advantages against competitors.

6. CONCLUSION

The thesis focused on the cybersecurity of industrial Internet devices. The study was performed as a case study and the target device was variable-frequency drive (VFD). So far industrial devices have been protected by guards and locks. Those protection methods are not enough when the devices are connected to internet. Thus, manufacturers of devices like VFD need to take cybersecurity into account.

VFD is a device which is used to steer AC motors. So, VFDs can be used in different applications like running assembly belt, pumps, and elevators. Some VFDs in the industrial network have options to access in cloud services on the internet.

The thesis introduced cybersecurity in the industrial Internet. There was also presented a classification of threats. The cybersecurity included descriptions of threat mitigation strategies for devices and communication in the industrial Internet. In addition, the thesis showed that there are different parties who might have an interest in attacking VFDs.

The thesis describes the process of how the cybersecurity of VFDs was studied and how the thesis ended up to the results. The prioritisation method was Weighted Shortest Job First (WSJF). WSJF was chosen for prioritisation because of its familiarity for stakeholders and its capability to collect wide views of priorities from different stakeholders. The study included also collection of attacks against VFD. The thesis presented VFD's assets, which are: VFD works like expected, intellectual property, safety and legislation.

Availability of interfaces was discussed and VFD's assets were presented also in the thesis. The study of threat mitigation strategies and application of them in VFDs was performed. Thus, the not applied strategies were prioritised in the stakeholder meeting by giving WSJF value for each of them.

Man-in-the-Middle attack and other attacks related to communication between devices were found during the study. However, the attacks were not in the focus of this thesis but adding better protection for VFDs. In the study we noticed that there was a protection for VFD's parameters by enabling password protected parameter locking. In addition, there was a few threat mitigation strategies already applied. The strategies were: *Secure Boot*, *Endpoint and Configuration Control* and *Remote and Automated Endpoint Update*.

There was a workshop for prioritising not applied mitigation strategies. The workshop's attendees were VFD manufacturer's staff with position ranking from product managers to software architect. The result of workshop was a prioritised threat mitigation list. The

list guides how the manufacturers can improve cybersecurity of their devices and which strategies have been seen more important to increase cybersecurity than others.

The top three mitigation strategies in the prioritised list were Access Control, Logging and Event Management and User Authentication and Authorization. These strategies were selected as the most important ones because using the WSJF technique gave highest scores for them. These three strategies got highest points especially in the business value. It was so because majority of people in the prioritisation workshop were business people. Thus, the mitigation strategies were prioritised mainly in the business point of view. There was an indication that customers want certain features, thus, the features got the most points in the prioritisation method.

The thesis proposes, as the next step, to implement the mitigation strategies first and after the practices are implemented the next step can be a subsequent threat modelling of the VFD. Thus, the later threat modelling would give a hint where to focus cybersecurity enhancement efforts next.

REFERENCES

ABB Drives. Technical Guide – Cybersecurity for ABB drives. 2016. Referenced: 17.10.2016. Available: https://library.e.abb.com/public/e71305ed2cd747b3b65a2becaf9a58bd/EN_Cybersecurity_guide_A_A4.pdf

ABB industrial drives Firmware manual – ACS880 primary control program. 2016. Referenced: 27.10.2016. Available: https://library.e.abb.com/public/851179d8a3314c9192e1a7f51b7e8620/EN_ACS880_FW_manual_P_A4.pdf

ABB industrial drives Application guide – Adaptive programming. 2016. Referenced: 5.10.2017. Available: https://library.e.abb.com/public/1d854eb683f0438cba1774f7c1e3178c/EN_AdaptiveProgramming_AG_C_A4.pdf

ABB - All-compatible ABB drives: Designed to optimize every kilowatt and maximize output. 4.4.2011. Referenced: 8.2.2018 Available: http://www.abb.com/cawp/seitp202/69e3d67432de968fc125786300486731.aspx

Brown, Keith. 16.12.2015. Just Launched! - Better Feature Prioritization Using the Fibonacci Series. Referenced: 8.10.2017. Available: https://blog.aha.io/feature-prioritization-fibonacci-sequence/

I. Cha, Y. Shah, A. U. Schmidt, A. Leicher and M. V. Meyerstein, "Trust in M2M communication," in IEEE Vehicular Technology Magazine, vol. 4, no. 3, pp. 69-75, Sept. 2009.

Drury, B. 2009, The Control Techniques Drives and Controls Handbook, Second Edition: Power and energy series 57, 2nd edn, Institution Of Engineering & Technology (Iet), GB.

Pfleeger, Charles P. Pfleeger, Sand Shari Lawrence. Margulies Jonathan. 2015. Security in Computing (5rd ed.). Prentice Hall. pp. 850.

IBM X-Force® Research, 2016 Cyber Security Intelligence Index. Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations. Referenced: 12.12.2016 available: https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF

Industrial internet consortium. 04.06.2015. Industrial Internet Reference Architecture. Version 1.7. Referenced: 20.4.2017. Available: https://www.iiconsortium.org/IIRA-1-7-ajs.pdf

Infosec institute. 11.6.2015. The Seven Steps of a Successful Cyber Attack. Referenced: 26.1.2017. Available: http://resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack/

Lendermann, Heinz. Moghaddam, Reza. Tammi, Ari. Motoring ahead.ABB Review 1|11. Available: https://library.e.abb.com/public/0941e2550dc01000c1257854003b153a/ABB%20Review%201-2011_72dpi.pdf

MacAskill Ewen, Thielman Sam, Oltermann Sam. Wikileaks publishes 'biggest ever leak of secret CIA documents'. 7.3.2017. Guardian. Available: https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance

Noland, Marcus. 27.4.2004. The Legal Framework of US-North Korea Trade Relations. JoongAng Ilbo. Referenced: 7.10.2017. Available: https://piie.com/commentary/op-eds/legal-framework-us-north-korea-trade-relations

Penttilä, Olli-Jussi Johannes. 9.3.2016. Cyber Threats in Maritime Container Terminal Automation Systems. Master of Science thesis, Tampere University of Technology. pp.101.

Rouse, Margaret. 11.2012. Definition application sandboxing. Referenced: 5.1.2018. Available: http://searchmobilecomputing.techtarget.com/definition/application-sandboxing

Saitta, Paul. Larcom, Brenda. Eddington, Michael. Trike v.1 Methodology Document [Draft]. 13.7.2005. Referenced: 9.9.2016. Available: http://octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf

Scaled agile framework. WSJF (Weighted Shortest Job First). Referenced: 15.5.2017. Available: http://www.scaledagileframework.com/wsjf/

Shostack, A. 2008. Experiences Threat Modelling at Microsoft. Referenced: 16.9.2016. Available: http://www.homeport.org/~adam/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf

Shostack, Adam. 2014 'Threat Modeling: Designing for Security', 1st edn, US, John Wiley & Sons Ltd, 2014).

Sundell, Magnus. Kuivalainen, Janne. Mäkelä, Juhani. Gervais, Arthur. Orava, Jouko. Hyppönen, Mikko. 23.10.2012. White paper on Industrial Automation Security in

Fieldbus and Field Device Level. Available: https://www.vacon.com/imagevaultfiles/id_3695/cf_2/vacon-white-paper-on-industrial-automation-securit.pdf

A. Varghese and A. K. Bose, "Threat modelling of industrial controllers: A firmware security perspective," 2014 International Conference on Anti-Counterfeiting, Security and Identification (ASID), Macao, 2014, pp. 1-4.

Wright, Joshua. Dispelling Common Bluetooth Misconceptions. Referenced: 8.2.2018 Available: https://www.sans.edu/cyber-research/security-laboratory/article/bluetooth

Techopedia. Hardening. Referenced: 15.5.2017. Available: https://www.techopedia.com/definition/24833/hardening

Techopedia. Industrial Internet. Referenced: 15.5.2017. Available: https://www.techopedia.com/definition/30044/industrial-internet

Zetter, Kim. How Digital Detectives deciphered stuxnet, the most menacing malware in history. 07.11.2011. Wired. Referenced: 24.10.2016 Available: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zetter, Kim. Palin E-mail Hacker Says It Was Easy. 18.09.2008. Wired. Referenced: 23.9.2017. Available: https://www.wired.com/2008/09/palin-e-mail-ha/