YRKESHÖGSKOLAN
NOVIA

Cyber Secure Remote Access to Critical Infrastructure

Hannes Nyåker

Degree Thesis for Bachelor of Engineering

Degree Programme in Electrical Engineering and Automation

Vasa 2020

BACHELOR'S THESIS

Author:	Hannes Nyåker
Degree Programme:	Electrical Engineering and Automation
Specialization:	Information Technology
Supervisors:	Jan Berglund, Novia University of Applied Sciences
	Dan Källroos, Wärtsilä

Title: Cyber Secure Remote Access to Critical Infrastructure

Date: May 2, 2020 Number of pages: 32

Abstract

This thesis was done on behalf of the Mobilisation & Support team within the company Wärtsilä. The goal of this thesis was to find what to implement in Wärtsilä's network architecture for remote access connections to critical infrastructure to fulfill the requirements stated in the IEC 62443-2-4 and IEC 62443-3-3 standards.

Wärtsilä's network architecture was evaluated in order to find out which requirements in the standards were not fulfilled. The process of evaluating the network architecture was done by looking at each requirement stated in the standards and comparing them to the network architecture to find out whether the requirement was fulfilled or not. After the evaluation, a list of unfulfilled requirements was compiled and used to find and evaluate new solutions to implement into the network architecture which would fulfill all requirements in the compiled list.

As a result, two new network architectures were designed and presented which both fulfill the requirements in the IEC 62443-2-4 and IEC 62443-3-3 standards. These two network architectures fulfill the goal of the thesis and ensure a cyber secure remote access connection to critical infrastructure.

Because the thesis contains business secrets, this version is partly censored.

Language: English Key words: Cybersecurity, Remote Access, IEC 62443

EXAMENSARBETE

Författare:	Hannes Nyåker
Utbildning och ort:	El- och automationsteknik, Vasa
Inriktningsalternativ:	Informationsteknik
Handledare:	Jan Berglund, Yrkeshögskolan Novia
	Dan Källroos, Wärtsilä

Titel: Cybersäker fjärråtkomst till kritisk infrastruktur

Datum: 2.5.2020 Sidantal: 32

Abstrakt

Detta examensarbete har gjorts åt avdelningen Mobilisation & Support inom företaget Wärtsilä. Målet med examensarbetet var att ta reda på vad som kunde implementeras i Wärtsiläs nätverksarkitektur vid fjärråtkomst till kritisk infrastruktur för att uppfylla krav som anges i standarderna IEC 62443-2-4 och IEC 62443-3-3.

Wärtsiläs nätverksarkitektur evaluerades för att ta reda på vilka krav angivna i standarderna som inte uppfylldes i nätverksarkitekturen. Denna evalueringsprocess gjordes genom att noga jämföra ett krav i taget mot nätverksarkitekturen för att få svar på om kraven uppfylldes eller inte. Efter denna evaluering sammanställdes alla ouppfyllda krav till en lista. Denna lista användes för att hitta och evaluera nya lösningar som kunde implementeras i nätverksarkitekturen.

Som resultat designades två nya nätverksarkitekturer som båda uppfyllde kraven angivna i standarderna IEC 62443-2-4 och IEC 62443-3-3. Dessa två nätverksarkitekturer uppfyllde målet med examensarbetet och skapar en cybersäker fjärråtkomst till kritisk infrastruktur.

På grund av affärshemligheter är detta examensarbete delvis censurerat.

Språk: engelska Nyckelord: cybersäkerhet, fjärråtkomst, IEC 62443

OPINNÄYTETYÖ

Tekijä:	Hannes Nyåker
Koulutus ja paikkakunta:	Sähkö- ja automaatiotekniikka, Vaasa
Suuntautumisvaihtoehto:	Tietotekniikka
Ohjaajat:	Jan Berglund, Yrkeshögskolan Novia
	Dan Källroos, Wärtsilä

Nimike: Kyberturvallinen etäyhteys kriittiseen infrastruktuuriin

---

Päivämäärä: 2.5.2020 Sivumäärä: 32

Tiivistelmä

Opinnäytetyö on tehty Wärtsilän Mobilisation & Support-osastolle. Opinnäytetyön tavoitteena oli selvittää mitä voisi lisätä Wärtsilän verkkoarkkitehtuuriin, jotta etäyhteys kriittiseen infrastruktuuriin täyttäisi IEC 62443-2-4 ja IEC 62443-3-3 standardien asettamat vaatimukset.

Wärtsilän verkkoarkkitehtuuria on tutkittu, jotta tulisi ilmi mitkä standardien asettamat vaatimukset eivät täyttyneet. Tutkiminen koostui jokaisen vaatimuksen tarkasta vertailusta verkkoarkkitehtuuriin, minkä seurauksena selvisi, jos vaatimukset täyttyivät. Tutkinnan jälkeen kaikki täyttämättä jääneet vaatimukset koottiin listaksi. Tämän listan avulla löydettiin ja evaluoitiin uusia ratkaisuja, joita oli mahdollista lisätä verkkoarkkitehtuuriin.

Tuloksena kaksi uutta verkkoarkkitehtuuria on laadittu. Molemmat täyttävät IEC 62443-2-4- ja IEC 62443-3-3 standardien asettamat vaatimukset. Nämä kaksi verkkoarkkitehtuuria täyttävät oppinäytetyön tavoitteen, ja luovat kyberturvallisen etäyhteyden kriittiseen infrastruktuuriin.

Opinnäytetyö sisältää luottamuksellista tietoa, joka on poistettu julkisesta työstä.

Kieli: englanti Avainsanat: kyberturvallisuus, etäyhteys, IEC 62443

Table of Contents

Figures

Abbreviations

BR	Base Requirement
DMZ	Demilitarized Zone
IACS	Industrial Automation & Control System
IEC	International Electrotechnical Commission
IT	Information Technology
MFA	Multi Factor Authentication
RE	Requirement Enhancement
SL	Security Level
SR	System Requirement
VPN	Virtual Private Network

1 Introduction

This chapter will provide background information about the thesis, define the problem area and give a clear view of the purpose of the thesis. Cybersecurity, standards and critical infrastructure will be briefly explained.

1.1 Background

This thesis was assigned to me by Wärtsilä Finland, Mobilisation & Support team. The team is interested improving their cybersecurity in order to mitigate the risk of falling victim to cyberattacks and to ensure a certain standard is met for all network solutions connected to critical infrastructure, especially when connecting there through remote access (see Chapter 3.3.1).

The critical infrastructure is a section of the network architecture which is also often called a trusted network (see Chapter 3.2.2). In the manufacturing and service industry, Critical infrastructures commonly consist of industrial automation & control systems, shortly IACS.

Cybersecurity, often referred to as computer security or IT-security, is a key term in this thesis. It can be defined as the practice of protecting computers, networks and data from unauthorized users and cyberattacks [1] [2]. The word "cyber" is a prefix that can be applied to words to specify its relation to computers and the internet [3]. Cyberattacks are constantly evolving, therefore cybersecurity is constantly in need of improving in order to withstand the potential threats [4].

A standard refers to a technical document that contains rules, guidelines or definitions. The standard that Wärtsilä has chosen is IEC 62443, also called ISA99, which is specifically developed to help making IACS solutions cyber secure. The IEC 62443 standard is created by the ISA99 committee and utilized by the International Electrotechnical Commission (IEC). The standard consists of multiple parts, although not all are needed for this thesis. The parts used are IEC 62443-2-4: Requirements for IACS service providers, and IEC 62443-3-3: System security requirements and security levels. [5]

1.2 Problem Area

As network architecture grows and becomes more complex, it also increases in the number of vulnerable locations unless proper cybersecurity is applied.

Remote access can be used when someone wants to use a computer without physically being at the computer. Instead, the computer is accessed remotely through another computer via the internet. This is a very useful and flexible solution as you can access computers that are physically far away from you or otherwise inaccessible. However, this practice creates security risks, for example as the remote access connection is carried over untrusted networks.

Because of these potential vulnerabilities, applying the IEC-62443 standard is a secure way of making sure the network architecture achieves a certain level in terms of cybersecurity.

1.3 Purpose

The purpose of this thesis is to design a more cyber secure solution which will add value to the solution and increase customer satisfaction. A secondary purpose is to provide research and advance Wärtsilä's knowledge of the standard to get a better view of how the standard can be applied to Wärtsilä's solutions.

1.4 Goal

The goal of this thesis is to find out what to change or implement in Wärtsilä's network connected to critical infrastructure where IACS are located so that the requirements in the standards IEC 62443-2-4 and IEC 62443-3-3 are fulfilled, then design a new network architecture for Wärtsilä which fulfill the requirements in the standard. The goal is only to create the design, not implement it. Because of Wärtsilä's broad amount of solutions around the world, many of which have specific modifications and configurations in their network architecture, the new design will be created as a generalized design which can then be used as a template.

1.5 Disposition

This thesis consists of 8 chapters:

In the first chapter, an overview of the thesis is presented. The background, problem area, goal and purpose of the thesis are explained.

The second chapter provides information about the company Wärtsilä and its current businesses. The Mobilisation & Support team is briefly presented.

Chapter three goes through the basic theory needed to understand the evaluation process and the result presented in this thesis. Network architecture, security zones, components (both common and Wärtsilä-specific) and practices are explained. Lastly, Wärtsilä's current network architecture is presented.

In the fourth chapter, the methods used in the empirical part of the thesis to achieve the result is put forward. The process of evaluating Wärtsilä's current network architecture and new solutions are explained along with the process of designing new network architectures.

The fifth chapter presents the evaluation of Wärtsilä's network architecture. From the results of the evaluation, a list of unfulfilled requirements is compiled and explained.

In the sixth chapter, new solutions are evaluated and compared to the compiled list from the evaluation of Wärtsilä's network architecture. Each solution is presented, showing which requirements it fulfills.

Chapter seven includes the result and an in-depth explanation of it. The chapter aims to complete the goal of the thesis.

The eighth chapter provides my own conclusion about the thesis and the presented result. Ideas of further work which can be done regarding the result and the goal of this thesis are put forward.

2 Wärtsilä

Wärtsilä is a global corporation leading in the marine and energy markets for smart technologies and complete lifecycle solutions through manufacturing and servicing power sources and other equipment. Wärtsilä is split up into two main sections: Marine Business and Energy Business. At the end of 2019 Wärtsilä had 18,795 employees worldwide, 20% of them being in Finland, 42% in the rest of Europe and 38% in the rest of the world. [6]

2.1 History

Wärtsilä was founded in 1834 in Värtsilä, Finland and started out as a sawmill business. In the year 1938 the company signed a license agreement with Friedrich Krupp Germania Werft AG in Germany to start manufacturing diesel engines. During the 1950's, Wärtsilä decided to start manufacturing their very own diesel engines. In 1984 the company becomes the first quoted Finnish company on the London stock exchange. In 2009 Wärtsilä became regarded as one of the top 100 most sustainable corporations globally. Since the beginning, Wärtsilä has grown into a global business in the marine and energy markets, manufacturing and servicing power sources to sites such as power plants or vessels. [7]

2.2 Mobilisation & Support

Mobilisation & Support is a team belonging to the Marine Business and it is on behalf of this team the thesis has been made. The team was created at the start of 2020 and its purpose is to offer mobilization and lifecycle support for digital products. It is part of a department called Digital Product Development. [8]

3 Theory Building

This chapter will go in-depth and explain the terms needed to understand the result of the thesis. First, network architecture along with network security zones, components (both common and Wärtsilä-specific) and practices will be explained. Secondly, Wärtsilä's network architecture will be displayed and explained. Thirdly, the IEC 62443 standards will be further explained and show the reader what they consist of and how to use them as guidelines for building a cyber secure solution.

3.1 Network Architecture

Network architecture is the framework of a computer network. It is a design that includes all components in a network and how they are connected to each other. The design can also consist of different layers or sections. [9] [10] The network architectures shown in this thesis were created using an online open-source diagram software on the website https://www.diagrams.net/.

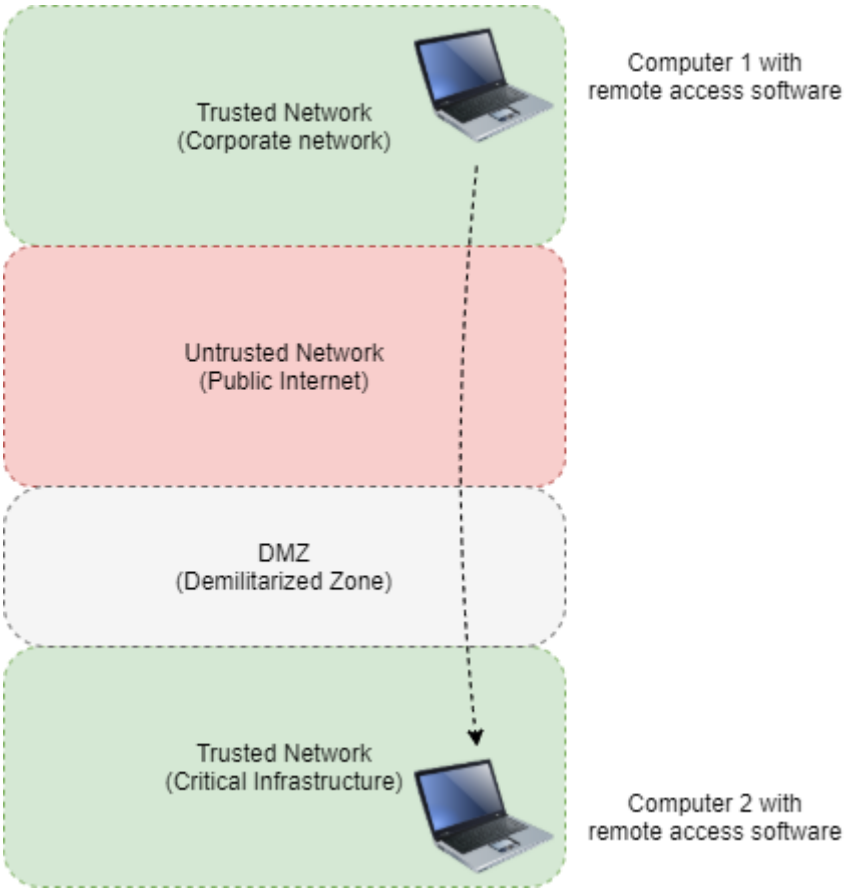

Figure 1. A logical network architecture showing the path of a remote access connection through different sections.

The figure above showcases a very basic network architecture which will be the base of this thesis consisting of four sections: a trusted network, an untrusted network, a demilitarized zone and finally a second trusted network. The figure also consists of two components: computer 1 & 2, both with remote access software installed. The computers do not have to be laptops like in the picture, they could also for example be workstation computers or server computers.

The first network is the corporate network which is trusted (see Chapter 3.2.2). Computer 1 could represent the work computer of an employee with expertise in troubleshooting IACS and therefore has a need of using remote access to connect to different sites in order to troubleshoot from a distance. The corporate network has access to the public internet which is the next network in the architecture.

The public internet is an untrusted network (see Chapter 3.2.1) which the remote access connection must travel through in order to reach its destination, the critical infrastructure. Because the network is regarded as untrusted, it is extremely important that this connection is well protected from cyberthreats.

Before the remote access connection can reach its destination in the figure above, it must go through a demilitarized zone (see Chapter 3.2.3).

The second trusted network in the figure is the critical infrastructure. This is where IACS are located which computer 2 is connected to. When the remote access connection has reached computer 2, the employee can start troubleshooting remotely.

3.2 Network Security Zones

In this chapter, different type of network security zones will be explained. Properties such as degree of trust and representing color for each zone in this thesis will be put forward.

3.2.1 Untrusted Network

An untrusted network is defined as a network which is located outside the security border of a network administrator's own network and is therefore uncontrollable by the network administrator [11]. It is therefore the public internet is generally defined as an untrusted network. Because of its untrusted state, it is critical that proper cybersecurity is applied to the connections going through the public internet in order to prevent other internet users from stealing data. In the architectures shown in this thesis, untrusted networks have been colored red to represent its untrusted state.

3.2.2 Trusted Network

In contrast to an untrusted network, a trusted network is within the security perimeter of a network administrator's own network and is therefore controllable by the network administrator [11]. A trusted network can also be called a private network. In the architectures shown in this thesis, trusted networks have been colored green to represent its trusted state.

3.2.3 DMZ

DMZ is short for demilitarized zone and works as a bridge between an untrusted and trusted network. It is used by trusted networks as a front-line defense, further providing a layer of security. Usually the networks have firewalls set up on the border to this zone, meaning that going from one network to another, two firewalls need to be passed, one to enter the DMZ and another to leave it. A DMZ is less secure than a trusted network and more secure than an untrusted network, therefore it is somewhere in between. Because of this uncertain state of trust, a DMZ have been colored grey in network architectures shown in this thesis. [12] [13]

3.3 Network Components and Practices

This chapter will cover some of the most common components and practices used in network architecture and aims to provide enough information to understand the network architectures presented in this thesis.

3.3.1 Remote Access

Remote access is a practice that enables a computer to gain access and control of another computer via the internet. This allows users to work from a distance without physically being at the location of the accessed computer, for example an office worker working on their office computer from home via their home computer. Remote access is usually done through a software application where you enter the address of the computer you want to connect to, then authenticate yourself in order to establish a connection. [14]

3.3.2 Firewall

A firewall is a crucial and common component in cybersecurity which controls incoming and outgoing network traffic using set security rules. For example, if an unauthorized user tries to connect to a network, the firewall at the border of that network can deny and block the attempted connection in order to protect its network. The management of granting or denying access is done through inspecting the network traffic. The firewall can look at elements such as source IP address, destination IP address and IP protocols and comparing it to its set security rules in order to determine whether to grant or deny access to pass through the firewall. [15]

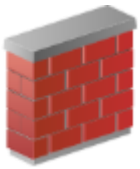

Figure 2. A firewall icon.

3.3.3 Jump Host

A jump host (also referred to as jump server and bastion host) is a server that provides controlled access between two different security zones. A common practice is to put the jump host inside of a DMZ between the two different security zones. [16]

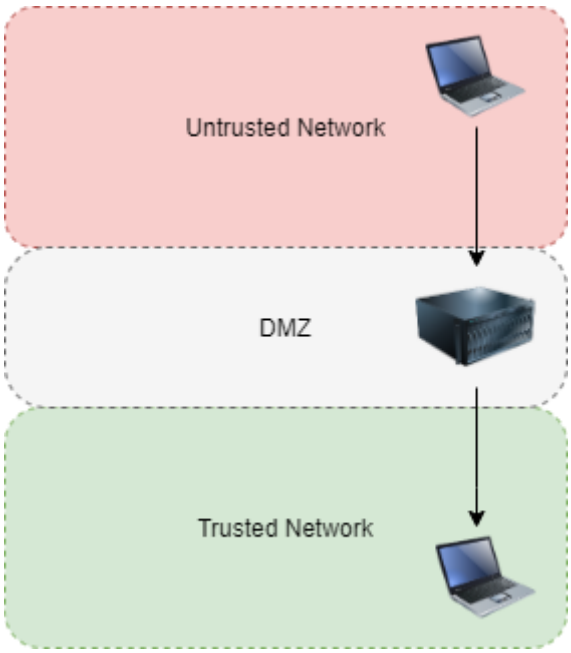

Figure 3. A jump host represented by a server icon inside of a DMZ controlling access between two different security zones.

In the figure above we can see a server icon that represents a jump host inside of the DMZ. For a computer in the untrusted network to establish a connection with a computer in the trusted network, it must go through the jump host. With this method, no connection from an untrusted network is established directly to a trusted network.

3.3.4 MFA

MFA is short for multi factor authentication and is the practice of requesting additional authentication methods on top of a username and password when authenticating users. In this context, a factor refers to a piece of evidence the user can provide to prove their identity. There are three different types of factors: knowledge (e.g. knowing a password), possession (e.g. having a key or access card) and inherence (e.g. fingerprint or face recognition). [17]

For example, a multi factor authentication process could request a user to enter a username, password and an authentication code sent to the user's personal mobile phone. This way the user must prove two different factors: knowledge (knowing the correct username and password) and possession (having the mobile phone related to the user's account).

3.3.5 PAM

PAM is short for privileged access management and is a solution consisting of different technologies that aims to improve the cybersecurity in user and role management environments through restricting privileged access. PAM also aims to improve an organization's control and capability to monitor of which users gain privileged access to where. [18]

3.3.6 VPN

VPN is short for virtual private network and is an extension of a private network. A user can connect to a private network virtually, meaning they do not physically connect to the network through a cable, but instead remotely through the public internet. Normally, the connection is secured using an encrypted layered tunneling protocol. [19]

For example, this solution can be used by an office worker who wants to work on the corporate network from home. With the use of VPN software, the worker can securely connect remotely to the corporate network.

3.4 Wärtsilä-specific Components

3.5 Wärtsilä's Network Architecture

3.6 The IEC 62443 Standard

The IEC 62443 standard is created by the ISA99 committee and utilized by the International Electrotechnical Commission, shortly IEC. It is not a single standard, but rather a series of standards which together cover the whole scope for a cyber secure solution. [5]

The standard is mainly designed for IACS solutions, but as the focus in this thesis is on securing a remote access connection, not all requirements are applicable.

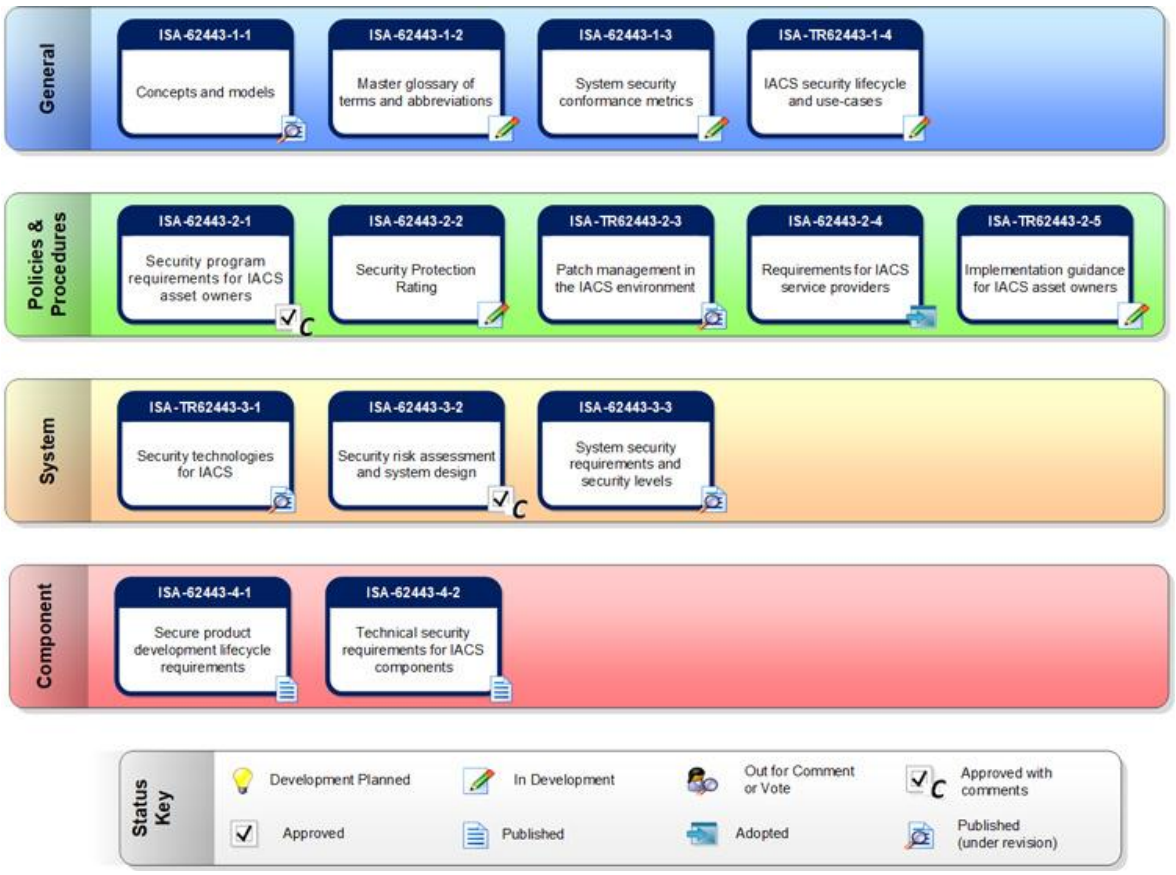

Figure 4. Diagram depicting all standards in the series and their sub-groups. [5]

As previously mentioned, the standards used in this thesis are IEC 62443-2-4 and IEC 62443-3-3 which both can be seen in the diagram above. These two standards have been chosen as they are the most relevant ones for this issue and were specifically requested by Wärtsilä to be looked at for this thesis.

3.6.1 Security Levels

IEC 62443-3-3 is titled "System security requirements and security levels" and consist of requirements to achieve different security levels (SL). The levels represent the overall quality of cybersecurity for the solution, a higher SL means a more secure solution. Different SLs can be achieved at different parts or zones of the solution, meaning that the achieved SL does not necessarily need to be the same everywhere in a solution. [20]

Achieving SL 1 would essentially mean that the solution is well protected against mistakes within the own work force. Having achieved SL 2 would in turn mean the solution is well protected against lowly resourced hackers with low motivation. SL 3 ensures the solution

is well protected against a group of hackers with sophisticated means, high motivation and knowledge about the targeted solution. [21]

3.6.2 Structure of the IEC 62443 Standard Requirements

There are two types of requirements in the IEC standards: base requirements and requirement enhancements. Base Requirements (BR) are the core requirements of the standard and together they make the base of the whole standard. Some BRs may have Requirement Enhancements (RE) on top of them, which are extensions of the BR with additional requirements that need to be met in order to reach a higher Security Level. It is worth noting however that a BR may have zero to many different REs and in some cases fulfilling a BR is enough to reach a high Security Level in that specific area. [20]

4 Methodology

In this chapter, details of the methods chosen to the empirical part of this thesis are provided. The chapter will also explain the process of evaluating Wärtsilä's network architecture followed by designing a new network architecture.

In this thesis, a qualitative method has been used to achieve the result because only one specific network architecture was looked at, which is Wärtsilä's own network architecture. This thesis explains how to cyber secure that specific network architecture when using remote access, not a broad selection of different network architectures.

The process to achieve a new network architecture design, which fulfills the requirements stated in the IEC 62443 standard, was to evaluate Wärtsilä's current network architecture. This was done by looking at the standard and comparing it to the architecture. The requirements stated in the standards were looked at one by one in order to determine whether the current network architecture fulfilled it or not. When this process was done, a list of unfulfilled requirements was compiled. The compiled list was then used to find out what type of solutions to search for that could be implemented in the new design. Once a solution was found it got implemented in a new design of the network architecture which could then be evaluated to see if all requirements are met.

Because IEC-62443 part 3-3 has four different Security Levels you can achieve, this whole process would need to be done four times. The first time would achieve SL 1 and would be the longest process as it covers all the base requirements. To achieve SL 2, 3 and 4, only requirement enhancements would need to be looked at.

During the process of comparing requirements from the standard to the network architecture, some requirements were especially tricky to answer whether they were fulfilled or not and therefore assistance from experts within the field was needed. Meetings were arranged where specific questions regarding components in Wärtsilä's network architecture were put forward and answered.

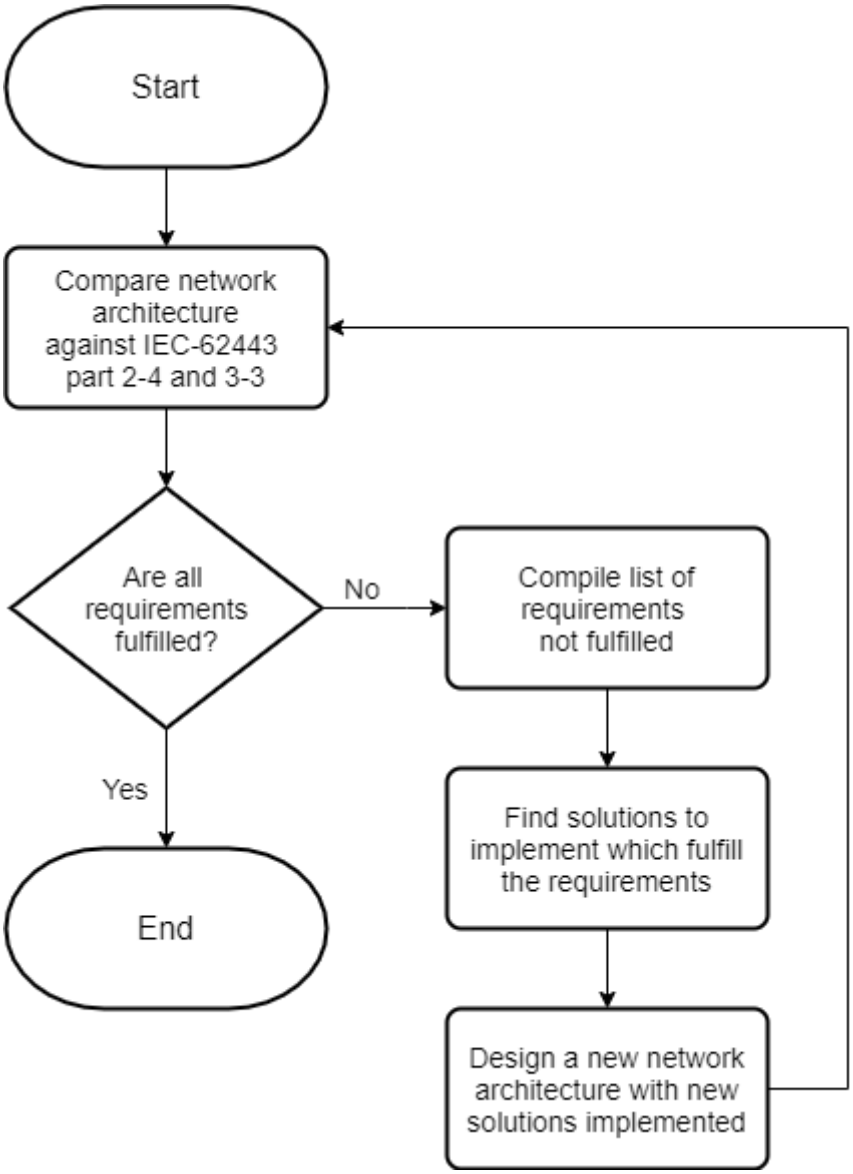

Figure 5. Flowchart depicting each step needed to achieve the desired results.

5 Evaluation of Wärtsilä's Network Architecture

5.1 Notes From Meetings

5.2 Requirements Check for IEC 62443 Part 2-4 and 3-3

6 Evaluation of New Solutions

7 Result

8 Conclusion

The goal of this thesis was to find what to implement in Wärtsilä's network architecture for remote access connections to fulfill requirements according to the IEC 62443-2-4 and IEC 62443-3-3 standards, which has been completed and presented in the previous chapter. It is worth noting that the focus has been on cyber-securing remote access and therefore this network architecture does not ensure that specific components such as IACS fulfill the standards. Only two standards in the IEC 62443 series has been looked at in this thesis. In order to cyber-secure the whole solution on different layers, all the standards in the series should be looked at.

The result is one of many and there are other solutions to fulfilling the requirements in the standards which could be evaluated.

9 References

[1] "Lexico," Oxford, 2020. [Online]. Available: https://www.lexico.com/definition/cybersecurity. [Accessed 27.4.2020].

[2] "Kaspersky," Kaspersky, 2020. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed 27.4.2020].

[3] "Lexico," Oxford, 2020. [Online]. Available: https://www.lexico.com/en/definition/cyber. [Accessed 27.4.2020].

[4] P. W. Singer and A. Friedman, Cybersecurity: What Everyone Needs to Know, Oxford University Press, 2014.

[5] ISA, "ISA99, Industrial Automation and Control Systems Security," 2020. [Online]. Available: https://www.isa.org/isa99/. [Accessed 21.2.2020].

[6] Wärtsilä, "This is Wärtsilä," 2020. [Online]. Available: https://www.wartsila.com/about. [Accessed 21.2.2020].

[7] Wärtsilä, "The History of Wärtsilä," 2020. [Online]. Available: https://www.wartsila.com/about/history. [Accessed 28.4.2020].

[8] Wärtsilä Internal, 2020. [Online]. [Accessed 2020].

[9] Techopedia, "Network Architecture," 2017. [Online]. Available: https://www.techopedia.com/definition/8549/network-architecture. [Accessed 2.3.2020].

[10] J. V. Luisi, "Pragmatic Enterprise Architecture," Elsevier Inc., 2014.

[11] A. Shekhar, "Types Of Networks: Trusted, Untrusted, And Unknown Networks," 2017. [Online]. Available: https://fossbytes.com/types-of-networks-trusted-untrusted-and-unknown-networks/. [Accessed 2.3.2020].

[12] S. Young, "Designing a DMZ," 2001. [Online]. Available: https://www.sans.org/reading-room/whitepapers/firewalls/designing-dmz-950. [Accessed 28.4.2020].

[13] Cisco, "About Security Zones," [Online]. Available: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ag1463340.html. [Accessed 28.4.2020].

[14] Citrix, "What is Remote Access?," 2020. [Online]. Available: https://www.citrix.com/glossary/what-is-remote-access.html. [Accessed 28.4.2020].

[15] W. Noonan and I. Dubrawsky, “Firewall Fundamentals,” Pearson Education, 2006.

[16] A. Kili, “How to Access a Remote Server Using a Jump Host,” 2018. [Online]. Available: https://www.tecmint.com/access-linux-server-using-a-jump-host/. [Accessed 29.4.2020].

[17] F. Aloul, S. Zahidi and W. El-Hajj, “Multi Factor Authentication Using Mobile Phones,” 2009. [Online]. Available: https://pdfs.semanticscholar.org/2599/ad2d3b40a47b7d7816b28f2791d4edb95109.pdf. [Accessed 29.4.2020].

[18] Microsoft, “Privileged Access Management for Active Directory Domain Services,” 2017. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services. [Accessed 29.4.2020].

[19] World Meteorological Organization, “Guide to Virtual Private Networks via the Internet between WMO Information System Centres,” 2016. [Online]. Available: https://library.wmo.int/doc_num.php?explnum_id=5221. [Accessed 29.4.2020].

[20] International Electrotechnical Commission, “IEC 62443-3-3: System security requirements and security levels,” 2013.

[21] D. W. Goble, “Applying the Global Automation Standard IEC 62443 to protect against cyber threats,” 2019. [Online]. Available: https://www.designlights.org/default/assets/File/SHM%202019/Building%20Cyber%20Oveview%20R3.pdf. [Accessed 28.4.2020].

[22] International Electrotechnical Commission, “IEC 62443-2-4: Security program requirements for IACS service providers,” 2015.