YRKESHÖGSKOLAN
NOVIA

Remote Digital Services

Anders Nordmyr

Degree Thesis

Thesis for a Bachelor of Engineering degree

Electrical Engineering and Automation

Vaasa 2022

DEGREE THESIS

Author:	Anders Nordmyr
Degree Programme and place of study:	Electrical Engineering and Automation, Vaasa
Specialisation:	Automation
Supervisors:	Jan Berglund, Novia University of Applied Sciences Willy Lågas, Wärtsilä

Title: Remote Digital Services

Date: 22.05.2022 Number of pages: 40

Abstract

The Bachelor's thesis was commissioned by the Agreements Proposal Management department within Wärtsilä, Energy Business. This thesis is about Wärtsilä's remote digital services called Operational Support and Expert Insight. These services can be found within Wärtsilä's portfolio of lifecycle solutions.

There was a need for a technical documentation manual at Wärtsilä that explains how these remote digital services work. The research made for this thesis brings up various technologies and subjects. Among these are data collection systems, remote support, connectivity, and anomaly detection systems. The purpose of this thesis was to improve the technical knowledge of these remote services and the benefits they bring in various Wärtsilä Lifecycle Agreements.

The information collected for this thesis was extracted from books, web pages, articles, studies, Wärtsilä's internal material and interviews with experienced Wärtsilä employees. The work was executed by gaining an understanding of the topics the work required and then explaining the technologies needed for these remote solutions.

The result is an internal technical guide about Wärtsilä's remote solutions. The guide is aimed for Wärtsilä employees that want to improve their technical knowledge about these remote services. The goal of this thesis work is to improve the technical knowledge for sales support and to increase sales.

Language: English Key Words: Wärtsilä, remote services, technical knowledge

---

EXAMENSARBETE

Författare:	Anders Nordmyr
Utbildning och ort:	El- och automationsteknik, Vasa
Inriktning:	Automation
Handledare:	Jan Berglund, Yrkeshögskolan Novia
	Willy Lågas, Wärtsilä

Titel: Digitala fjärrtjänster

Datum: 22.05.2022 Sidantal: 40

Abstrakt

Detta examensarbete har gjorts på uppdrag av avdelningen Agreements Proposal Management inom Wärtsilä, Energy Business. Examensarbetet handlar om Wärtsiläs digitala fjärrtjänster som kallas Operational Support och Expert Insight. Dessa fjärrtjänster finns inom Wärtsiläs portfölj av livscykellösningar.

Det fanns ett behov av en teknisk dokumentationsmanual, som förklarar hur dessa digitala fjärrtjänster fungerar. Examensarbetet tar upp flera olika teknologier och ämnen, bland dessa är datainsamlingssystem, fjärrsupport, anslutningsmöjligheter och system för upptäckt av anomalier. Syftet med detta examensarbete var att förbättra den tekniska kunskapen om dessa fjärrtjänster och fördelarna de medför i Wärtsiläs Lifecycle Agreements.

Informationen som samlades in för detta examensarbete har hämtats från böcker inom området, webbsidor, artiklar, studier, Wärtsiläs interna material och intervjuer med erfarna Wärtsilä anställda. Examensarbetet utfördes genom att få en förståelse för de ämnen som arbetet krävde och sedan förklara de teknologier som behövdes för dessa fjärrlösningar.

Resultatet blev en intern teknisk guide om Wärtsiläs fjärrlösningar. Guiden riktar sig till Wärtsiläs anställda som vill förbättra sina tekniska kunskaper om dessa fjärrtjänster. Målet med detta examensarbete var att förbättra försäljarens tekniska kunskaper och att öka försäljningen.

Språk: engelska Nyckelord: Wärtsilä, fjärrtjänster, teknisk kunskap

---

Content

1 Introduction

The thesis work will be about the remote digital services that are offered as a lifecycle solution at Wärtsilä. Wärtsilä lifecycle solutions offer several remote solutions, but this thesis work will be about Wärtsilä's operational support and expert insight services. These remote services can prevent or help to solve problems that may occur to the engines or automation systems at a powerplant. The thesis work was commissioned by the Agreements Proposal Management department within Wärtsilä, Energy Business.

In this chapter I will introduce you to my thesis work. Background information will be presented in section 1.1 and the purpose of the work in section 1.2. Brief information about Wärtsilä will be presented in section 1.3.

1.1 Background

The need for this thesis work was brought up at a meeting between people who work in sales and those who know how these remote solutions are carried out at powerplants. The agenda of the meeting was remote connectivity capabilities for powerplants. At this meeting, it was concluded that there was a need for a technical documentation manual that shares the information about what these remote services are and what type of equipment is required of them.

1.2 Purpose

The purpose of this technical documentation manual was to improve the technical knowledge of the remote services and the benefits they bring to the customer. Remote solutions are becoming more popular every year, especially since the COVID – 19 outbreaks. Therefore, it is crucial to get more knowledge about these solutions.

There was a need to share the technical knowledge on how these solutions work for people working within Wärtsilä. By sharing the knowledge, so can for example salespeople have a better understanding of what they are selling and explain to the customer what these remote solutions can do for them. Those who execute these remote solutions have the knowledge of how they work but there must also be a documentation to those who sell them.

1.3 Short about Wärtsilä

Wärtsilä was established in 1834 and the company first started a business within the lumber industry. The business has changed since then, and the major change was in 1938 when Wärtsilä signed a license agreement with Friedrich Krupp, and this is when the diesel engine era began within Wärtsilä. (Wärtsilä, 2022a)

Wärtsilä has developed its business since 1834 and they are now a global leader within the marine and energy markets. Wärtsilä is an international company and has over 17 000 professional employees operating in 68 countries around the world. The year 2021 was Wärtsilä listed on Nasdaq Helsinki with a total net sale of 4.8 billion EUR. (Wärtsilä, 2022b)

1.3.1 Energy Business

The Energy Business is one of Wärtsilä's business areas and they have delivered a powerplant capacity of up to 76 GW and over 110 energy storage systems worldwide. Wärtsilä Energy strives to reach a 100% renewable energy in the future and want to decrease carbon emission with market-leading technologies. Among these technologies are hybrid solutions, balancing powerplants, energy storage, optimization technology and GEMS energy management platform. Wärtsilä also delivers lifecycle services to these technologies which will improve the efficiency, reliability, and performance of the installations. (Wärtsilä, 2022c)

1.3.2 Marine Business

The Marine Business is another of Wärtsilä's major business areas. Wärtsilä works in many different areas within Marine and their portfolio is extensive. A portfolio that consists of engines, hybrid technology, propulsion systems, lifecycle services and more. Decarbonization and a sustainable future are a key part of Wärtsilä's business, and they are leading the industry with their solutions. (Wärtsilä, 2022c)

1.4 Glossary

Artificial Intelligence - AI

Supervisory Control and Data Acquisition – SCADA

Human Machine Interface – HMI

Host Controller Interface – HCI

Remote Terminal Unit – RTU

Master Terminal Unit - MTU

Programmable Logic Controller – PLC

Local Area Network – LAN

Wide Area Network – WAN

Internet Protocol – IP

Internet Protocol Security – IPsec

Encapsulated Security Payload – ESP

Authentication Header – AH

Security Association - SA

SSH Transfer File Protocol – SFTP

File Transfer Protocol – FTP

Secure Shell – SSH

WOIS – Wärtsilä Operator Interface System

DMZ – Demilitarized Zone

ICS – Industrial Control System

2 Wärtsilä - Remote digital services

Wärtsilä lifecycle solutions offer several different remote services to improve the operation of a powerplant. The services are supported by Expertise Centres and there are several centres that provide operational support, maintenance management and analytics around the world. These solutions use modern technologies like artificial intelligence and advanced analytics. With help of these solutions can operating costs be reduced and problems at the powerplant can be solved remotely. In 2021, Wärtsilä managed to solve remotely 96% of the incoming cases, of which 91% were solved on the same day. **Figure 1** gives an overview of the support possibilities from Expertise Centres to a powerplant. (Wärtsilä, 2022d)

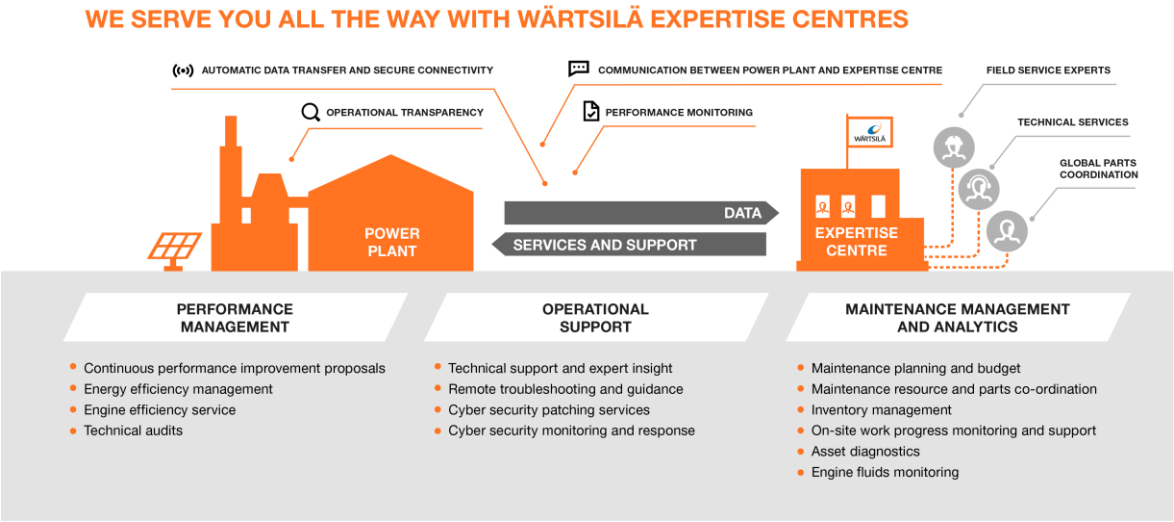

Figure 1. Wärtsilä Expertise Centres (Wärtsilä, 2022e)

2.1.1 Wärtsilä - Operational Support

Operational support can be found in Wärtsilä's lifecycle solution portfolio and is available in lifecycle agreements. This service enables remote support around the clock for the customer. The operational support service offers a way to solve operational issues remotely with help of an expert crew in Expertise Centres. The experts can provide guidance, advice, and recommendations to personnel on the installation site. An expert from the Expertise Centre can support customers with urgent operational issues and can be contacted by phone or email. The expert can be contacted during office hours otherwise an on-call expert will be contacted.

Installations have a dedicated Wärtsilä expert, which means that they have good knowledge of the customers' assets and installation equipment. Other than good knowledge about the installation, experts can also have access to Wärtsilä's data collection system. If the customer has Wärtsilä's data collection system, then the expert can access data from the site such as operating data, alarms, and events. Remote support is available for various assets, these are 4-stroke and 2-stroke engines, GVU systems, LNGPacs and generator systems.

Wärtsilä's data collection system and applicable equipment can enable more opportunities for the expert to troubleshoot issues occurring at the installation. A real-time remote connection can then be established which enables additional tools to collaborate with installation personnel at a powerplant site. Among these are remote monitoring, chat functions and remote tuning capabilities. (Wärtsilä, 2021a)

2.1.2 Wärtsilä - Expert Insight

Expert insight is another solution that is available in lifecycle agreements and is delivered by Wärtsilä Expertise Centres. The service relies on artificial intelligence methods and rule-based asset diagnostics technologies to identify anomalous behaviour in assets operating data. Deviations or anomalies detected by the system will be highlighted and investigated by an expert from Wärtsilä's Expertise Centres. This service is available for 4-stroke and 2-stroke engines and a pilot product for scrubbers. (Wärtsilä, 2021b)

The AI-based detection system is trained to fit the customers' assets. Operational data is gathered from the assets and are analysed with the AI-based detection system. Deviations or anomalies are then found if data deviates from the normal behaviour pattern created by the AI-based system. The rule-based system has been developed for a long time to define how a normal operating condition looks like. If data collected from assets differ from the thresholds created by the rule-based system, an anomaly is found. A combination of these two systems is used in Expert Insight to detect potential failures in time and decrease the possibilities of a major breakdown, which will result in increased reliability, efficiency, and safety. (Wärtsilä internal document, 2022a)

Installations with the expert insight solution have a dedicated Wärtsilä expert that daily monitors the anomalies generated by the system. If issues occur, then the expert will provide support to the customer with advice and recommendations. The expert insight service includes a collaboration application where real-time communication between the Wärtsilä expert and installation personnel can take place. This collaboration application can be securely accessed on an internet-connected browser. (Wärtsilä, 2021b)

3 Supervisory Control and Data Acquisition system

Supervisory Control and Data Acquisition system abbreviated SCADA system can provide a monitor and control solutions to a site. This system can collect data from various kinds of sources and apply control functions. Devices or processes can then be monitored and controlled remotely from a computer. SCADA systems are popular in industrial applications and can be found almost everywhere today. (DPS Telecom, 08.08.2011)

A SCADA system simplifies the operator's work by enabling monitoring and control functions from one central computer. The facilities that need to be supervised can be either remote or too big to monitor without a supervising system. That is why it is beneficial for the operator to not have to visit all of them and be able to monitor or control the processes from a single monitor. Alarms and measurements of equipment can be monitored, and the processes can be controlled by for example adjusting the set point on controllers to open or close switches and valves. (Boyer, 2004, pp. 9-10)

The main purpose to use a SCADA system is to automate processes. These processes can be for example dangerous for a human to perform or hard to control without a SCADA system. These systems are implemented in industries where automation can increase efficiency. The efficiency can be increased when all measured values can be shown on a single monitor instead of having to walk around the whole plant to check on all equipment.

The structure of a SCADA system may vary depending on the purpose of implementing the system. SCADA systems can have different functions but there are four core functions, these are data acquisition, networked data communication, data presentation and control. These functions also need four basic components performing them, these are field devices, RTUs or PLCs, MTUs, and communications network. (DPS Telecom, 08.08.2011)

3.1 SCADA components

3.1.1 Field devices

Field devices are typically sensors and actuators, these devices make it possible for the SCADA system to interact with the processes (WhatIs, 2021). A SCADA system can supervise anything from a few field devices up to several 100, so there is no specific limit. There are several different types of sensors and actuators, depending on what you want to measure or control. (DPS Telecom, 08.08.2011)

Sensors can measure physical units and convert them to data. The data can then be further processed by a machine or human. Sensors can measure many things, such as temperature, pressure, light and flow. (Electronics Hub, 02.04.2021) Sensors monitor processes in a SCADA system.

Actuators can move something and make the monitored processes mechanism operate. Actuators receive control signals from the SCADA system and operate accordingly. (WhatIs, 2021) There are different kinds of actuators, such as motors, pumps, switches, and valves (Tatum, 20.03.2022).

3.1.2 Master Terminal Unit and Remote Terminal Unit

A master terminal unit is abbreviated MTU and can also be called host computer or server. Today are MTUs based on a computer and with help of remote terminal units abbreviated RTU, monitor and control functions can be applied. These monitoring and control functions can be automated which means that it does not necessarily need an input from an operator to act but there can also be functions that need an input from an operator. Automated functions are programmed to do a specific task. MTUs can ask for inputs from RTUs and then act according to the data received from them.

RTUs is connected to the field devices and scans all the sensor and actuators that it is connected to it. There can be multiple RTUs in a SCADA system and be located far away from the MTUs. A connection is needed between MTUs and RTUs to be able to monitor and control the processes. MTUs are connected to RTUs like RTUs scans field devices, MTUs scan RTUs.

The MTU is a device that can collect all data, send commands, send information to other systems and interface with the operator. Information needs to be sent to a RTU from an MTU, for RTUs to be able to do something. This is also called master-slave communication where MTU is master and RTU is slave. So RTUs collect the data and saves it in its internal memory until the MTU ask for it. The RTU then transmits the data to the MTU for further progression. The same applies to control instructions, the MTU sends commands and the RTU responds with controlling the applicable actuators. (Boyer, 2004, pp. 11-14; 89; 107)

3.1.3 Programmable Logic Controller

Programmable logic controller abbreviated PLC is mostly used in industrial control systems and works like a small computer. A control system can have different functions and the PLCs can execute these functions with logic programming. The main task is to automate processes and efficiently perform them. PLCs are often known for their robustness and versatileness.

PLC is an input and output system which is then controlled by logic programming. Data is received from the inputs, and these are commonly digital or analog signals. Digital inputs can be switches which are either on or off. Analog inputs can be sensors and for example measure temperature, pressure and more. The programmed logic will determine how the output signal is set. Typically, an output signal will then control an application for example lights, motors and more.

PLCs are programmed to execute functions and the program is uploaded to the PLCs central processing unit (CPU). The program is written on a computer using a PLC programming software. The program monitors all inputs and if a condition in the code is met, an output will be set.

There are 5 standard programming languages, and these are defined in the IEC 61131-3 standard. Ladder logic is one of them and it is a graphical coding language and mostly used when programming an PLC. (polycase, 10.09.2021)

3.1.4 Communications network

Communication is a crucial component in a SCADA system, without it nothing works. The communication referred in a SCADA system, it is a movement of data from one place to another. To establish this a connection between the devices must exist. (Boyer, 2004, p. 53)

The SCADA architecture can typically consist of five hierarchical levels from level 0 to 4. These are field level, direct control, plant supervisory, production control and production scheduling. **Figure 2** illustrates the hierarchical architecture levels of a SCADA system.

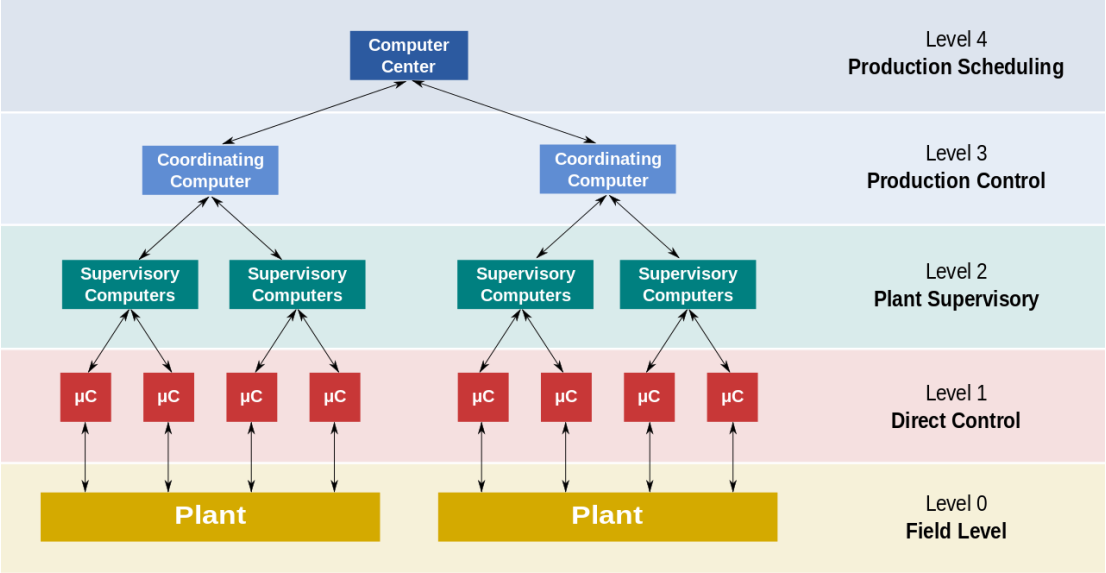

Figure 2. Architecture (Wikipedia, a)

Field Level (Level 0): The bottom level consists of field devices and these devices are technical equipment. Field devices can be sensors or actuators, sensors can be used to measure physical measurements and actuators can be used to move or control something.

Direct Control (Level 1): The direct control level consists of controllers that can read the sensors and control the actuators. These controllers can be PLCs and RTUs.

Plant Supervisory (Level 2): The plant supervisory level consists of supervisory computers. The computer collects all data provided by the controllers and can send commands to the controllers to execute something.

Production Control (Level 3): The production control level consists of coordinating computers that supervise level 2. These computers can provide reports, alerts and other regionwide functions to level 4.

Production Scheduling (Level 4): The production scheduling level consists of business systems that can manage the processes. (WhatIs, 2021)

3.2 SCADA functions

3.2.1 Data Acquisition

A SCADA system can monitor many sensors often up to hundreds or thousands of them and a data acquisition function can be found in SCADA systems. Historical or/and real-time data can be viewed on a monitor. (DPS Telecom, 08.08.2011) The data acquisition system gathers data from sensors which then can be stored and used for manipulation on a computer. The measured physical phenomena can be for example pressure, voltage, and temperature.

Dynamically and statically measurements can be made, and this will often require a powerful computer, so low and high-speed sampling can be collected. Sensors often measure units in analog format and need to be converted to digital format to be able to utilize the measured values on a computer. Data acquisition systems then process all signals and a software on the computer can analyse the signals. The idea of how a data acquisition works can be visualized in **Figure 3**.

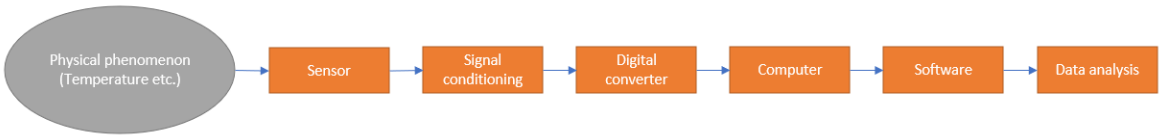

Figure 3. Data collection process (Nordmyr, 2022a)

Several different devices can be used in a data acquisition system, and it is crucial that all devices can work together. These devices can be for example computers, software, databases and more. (electronics notes, n.d.)

3.2.2 Data communication

Data communication is used to transport all data collected from various sensors to a central location, where all data can be monitored. There are different forms of network communications, but one commonly used today is to send data through ethernet and IP over SONET. Synchronous Optical Network is abbreviated as SONET and is a communication protocol that can transfer data using an optical fibre cable (GeeksforGeeks, 22.09.2021). Data should not be sent over an open LAN/WAN because sensitive data may be exposed to the internet.

Data is encoded in protocols and are used for the communication of data and are based on rules and guidelines (techopedia, 24.04.2020). RTUs provide an interface for the sensors and actuators because these devices cannot transform their signal to a protocol format. When the data from the sensors and actuators is converted to a protocol format it is transferred to a SCADA master. The SCADA master will then send control commands in return and the appropriate actuator will receive electrical signals from the RTU. (DPS Telecom, 08.08.2011)

3.2.3 Presentation of data

Data can be presented on a computer and is called a Human Machine Interface (HMI) or Host Computer Interface (HCI). HMI system can often provide a graphical interface, and it should be easier for an operator to understand the process (Boyer, 2004, pp. 163-164). All data can be monitored from one place, and this gives the operator a full view of the processes monitored.

There can be numerous of different functions depending on how advanced the setup is. Typically, all sensors can be monitored, and alarms will be triggered if the sensors receive a value outside the normal operating range. SCADA system can show real-time data gathered from the supervised processes and stored data viewed as a historical trend. (DPS Telecom, 08.08.2011)

3.2.4 Control of devices

In a SCADA system control functions can be applicated. These functions can either be manual or fully automated. (DPS Telecom, 08.08.2011) Control actions from the SCADA system is mostly performed by RTUs or PLCs (DPS Telecom, n.d.).

3.5 Wärtsilä Operator Interface System

Wärtsilä's HMI or SCADA system is called Wärtsilä Operator Interface System and is abbreviated as WOIS or sWOIS. The system is divided into two names since there is an old and newer version of the system. The new version is called sWOIS meanwhile the old version is called WOIS. The new version is a server-based interface system that runs in a virtualized environment and is an improvement of the old WOIS system. (Wärtsilä internal document, 2022b) The sWOIS system can be applied on a powerplant and enables control and monitor functions to the powerplant. **Figure 4** gives an overview of the six key modules that sWOIS can deliver. The plant operation and device integration module are by default included by delivery of the sWOIS system. The rest of the modules are optional and available if needed.

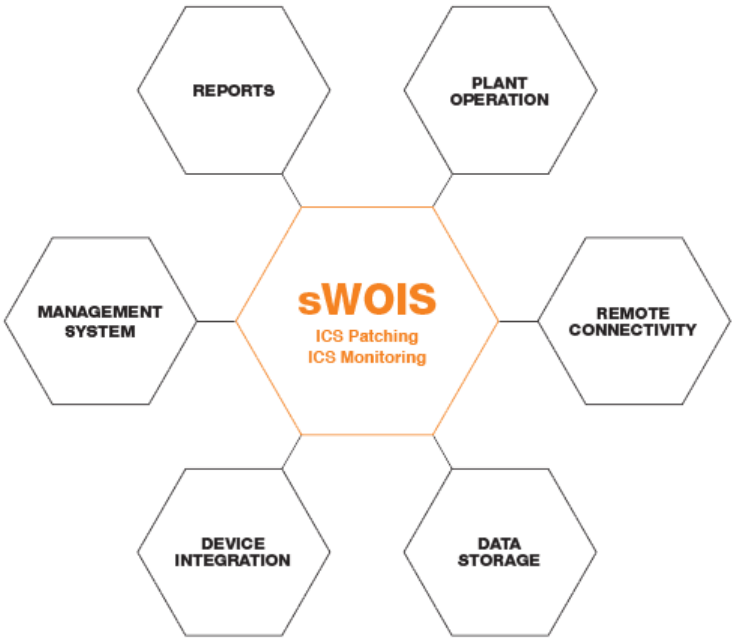

Figure 4. Wärtsilä Operator Interface System (Wärtsilä, a)

All these modules can improve the operation of a powerplant and enables services that Wärtsilä lifecycle solutions offers. The plant operation module is the operator interface, and the device integration module is on the other hand the interface for the control network. The storage module enables long-time storage of process data gathered from the site and the remote connectivity module makes it possible to establish a remote connection to another system with remote monitoring possibilities. Reports can be generated from the system with the report module included, these reports can be based on operational data gathered from the powerplant. The management system of the sWOIS has three main functions, these are backup, restore system and system health monitoring. (Wärtsilä, 2019)

4 Remote support

Supporting customers remotely has become popular and issues that the customer is experiencing can be solved more quickly. The COVID-19 pandemic had a big impact on the need for remote support. However, there are different types of remote support and the requirement of equipment may change depending on the level of support. The main purpose of remote support is to provide technical support and solve problems together with the customer.

Remote support can be done in different ways but one of the simplest types of support is to take a voice call over a phone and discuss the problem. This kind of support does not require any specific software but solving the problem is more difficult when technicians cannot have a direct interaction with the problem. Problems can be identified easier if the customer for example also sends pictures of the issue. This will allow technicians to have a better understanding on what the customer is struggling with.

Today it is more common to take a support session over an internet-based communication software. There are various kind of software on the market, but they often enable functions like voice calls, camera sharing, file sharing, remote view, instant messaging, and remote control. Support technicians can use this software to remotely access a computer with the customers permission. This will give the technicians a better view to troubleshoot the problem and solve the issues.

Remote access means that there is an opportunity to connect to a network or system remotely and control or view it. If the customer faces a problem with their computer, device, or system, they can call for tech support. Technical support can then request for remote access. If access is granted by the customer, there is a possibility to have full control over the system depending on the type of remote access.

There are two types of remote access, these are attended remote access and unattended remote access. The difference is simple, attended remote access is a real-time support session between the customer and technical support. Unattended remote access does not need the attendance of the customer and tech support can remotely solve it on their own at any time. (Rescue, 2022)

To be able to communicate with a remote computer or system, a remote connection is needed. A remote connection from one site to another can be established in multiple ways. Which connectivity method is used depends on the purpose and the degree of cyber security needed. One secure method to remotely connect to another site is an VPN connection, which will be described more closely in the following subchapters.

4.1 Virtual Private Network

A Virtual Private Network abbreviated as VPN makes connections over the internet more secure from cyber threats. VPNs is often used within businesses, but individuals also want to use VPN to secure their data communication. Data that is sent over this connection is encrypted which makes it unreadable for others.

A VPN can be used to securely connect to a remote site over the internet. It is a private network and can be routed from for example a business's private network or a third-party VPN service to a remote site. VPNs usually use the internet to create this connection between the two sites. There are different types of VPNs but in this thesis work we will mostly be focusing on the site-to-site VPN.

VPNs can encrypt data to secure it from others, only a decoder can read data that is encrypted. To be able to encode or decode data, an encryption key is needed. With this encryption key, a computer will know how to calculate and open the encrypted data. There are different forms of encryption methods, such as symmetric-key encryption and public-key encryption. A symmetric-key encryption only has one key which all computers utilize to encrypt or decrypt data. A public-key encryption, all computers have a public and private key. The private key can encrypt the message and the public key can decrypt the message. When a VPN connection is made, data will then be encrypted before the message is sent to the receiver. The receiver will then decode the message to be able to view it.

A VPN uses a more comprehensive encryption method depending on the VPN setup. There are two different protocols that site-to-site VPN uses, such as internet protocol security (IPSec) or generic routing encapsulation (GRE). (howstuffworks, 09.04.2021)

4.1.1 VPN Tunnel

VPNs often use tunnels to transport data over the internet. A VPN tunnel is created between two sites and data is sent through this tunnel. This tunnel is virtual and the communication within the tunnel is hidden from the public. When transportation of packets is sent, another packet is added, and this extra packet will protect the content from others viewing it. This extra layer of packets is known as encapsulation.

The tunnel has two ends and network devices can be found at both ends. These devices can encapsulate packets and open incoming ones. The ends of the tunnel are configured, and this type of communication utilizes a tunnelling protocol.

A tunnelling protocol improves the security by adding a layer which protects the original packet sent over the internet. All data transport uses different protocols to be able to communicate with each other. However, the tunnel will not change the transport protocol that it was sent with, but it will add an extra security layer on top of the packet. So, for example the internet protocol (IP) can be seen in the inner packet. (howstuffworks, 09.04.2021)

4.1.2 Site-to-site VPN

A secure way to connect to another network remotely is the site-to-site VPN. The connection can be made for one or more remote sites, but all sites will be branched to one location. This will enable a secure data communication between the two sites.

Site-to-site VPN can be divided into two types, and these are intranet-based and extranet-based. Intranet-based can be a remote connection established for an internal communication within a company. Extranet-based is for data communication with for example customers or partners etc., and this will separate the connection from the intranet. (howstuffworks, 09.04.2021)

4.1.3 IPsec

A site-to-site VPN can use an IPsec protocol to securely transport data over the internet. The protocol can secure internet traffic through encryption of data between devices. These devices can send and receive data through the internet and with help of this protocol, data will be unreadable for other devices. The communication between the devices can be for example router to router, firewall to router, desktop to router and desktop to server. (howstuffworks, 09.04.2021)

IPsec is more correctly a group of protocols and is not only used by establishing a VPN. The purpose with IPsec is to encrypt data travelling over a public network. To be able to securely deliver packets over the VPN tunnel, the IPsec protocol includes three sub-protocols, encapsulated security payload (ESP), authentication header (AH) and security association (SA). (Cloudflare, 2022)

IPsec can operate in two different modes, known as IPsec tunnel mode and IPsec transport mode. VPNs operate IPsec in tunnel mode to encrypt data. (howstuffworks, 09.04.2021) When data is sent from a device, the ESP protocol will encrypt the IP header and payload. This is done by using the encryption method symmetric key (howstuffworks, 09.04.2021). To be able to know if data received is from a trusted source, the AH protocol is used. The AH protocol can also see if data or packets have been modified which would make it untrustworthy. The SA contains several protocols but are used for settle encryption keys and algorithms. (Cloudflare, 2022)

4.2 Wärtsilä – Operational support

Wärtsilä's operational support service can offer their customers remote guidance, troubleshooting and tuning support. The operational support service enhances the chances that issues are resolved as quickly as possible and the need for unscheduled maintenance visits are minimized. If for example Wärtsilä's customer is experiencing problems at their installation, a dedicated Wärtsilä Expert from the Expertise Centres is available for remote support. When a customer needs support, they can send a support request to an Wärtsilä Expert through a mobile phone or email. The customer can start the conversation by explaining the issue they are experiencing. The Wärtsilä expert can then remotely investigate the issue together with the customer's crew and give guidance, advice, and recommendations on how to solve the issue.

Remote guidance is part of Wärtsilä's operational support service and is an on-demand service. The remote support session can then take place on a phone or email but there is also a possibility to use a mobile application. A collaboration between a Wärtsilä expert and customer's crew will then occur on either of these options.

Remote troubleshooting is also part of Wärtsilä's operational support service. Wärtsilä remote troubleshooting is the next level of remote support with additional features compared to remote guidance. Additional tools can then be used by Wärtsilä's remote support crew if the customer has a Wärtsilä data collection system. The sWOIS system is one of them and from this system a remote access connection can occur. This remote access connection can then be from a customer's installation to Wärtsilä's Expertise Centres.

The remote access session will take place over a remote access computer software, where the installation's operator interface can be seen by Wärtsilä's remote support expert. Remote tuning and control functions can be applied by the Wärtsilä support with applicable equipment. Remote tuning enables the expert to tune the automation system remotely. This remote access software will also enable real-time communication with voice call, video sharing, instant messaging, and file-sharing functions. This remote access connection will then enable a live troubleshooting opportunity.

Real-time or historical data can be monitored by Wärtsilä experts with a data collection system. Wärtsilä experts can then analyse data gathered from the installations assets and give advice according to their analysis. Collaborations between site personnel and Wärtsilä experts can work more smoothly with these additional tools.

Wärtsilä's data collection systems are the key component to delivering the best remote support. Together with a data collection system and a cyber-secure connection, the Wärtsilä expert can remotely access an installation and troubleshoot issues together with the personnel on-site. With this remote access connection, more tools are available for Wärtsilä remote support to troubleshoot issues and solve them. (Wärtsilä internal document, 2022c)

5 Transfer data

To be able to view files remotely they need to be sent over the internet. Files can be sent to an online storage cloud and remote users can access them from there. Cloud storing could then be a way to store files securely and diagnostic tools can utilize the data from there. To be able to transfer data to an online cloud storage, a secure connection from site is required. (techopedia, 31.08.2021) When sending files over the internet, you need a file transfer protocol like SSH File Transfer Protocol (SFTP). In this chapter we will be looking what this is and how it works.

5.1 SSH File Transfer Protocol

A SSH File Transfer Protocol abbreviated SFTP is a file transfer protocol. The protocol enables a secure way to transfer files over the internet between remote systems. The File Transfer Protocol (FTP) is a similar protocol to SFTP but without the Secure Shell (SSH) encryption which makes SFTP more secure than FTP. All files transferred with SFTP are encrypted and there is no opportunity to send files unencrypted. SFTP only needs one network port for data and usually it is on port 22 which represents the SSH server. (phoenixNAP, 25.11.2021)

SFTP uses a transmission control protocol (TCP) to verify that computers can receive files. This is done by a three-way handshake, and this can be explained with a three-stepped communication between two computers. So, the sending computer sends a message “SYN” to the receiving computer and the receiving computer responds with “SYN ACK”. When the sending computer receives the message, it will send back “ACK RECEIVED MESSAGE” and a handshake is complete. This handshake ensures that the computer can receive files.

SSH is a client-server protocol where a client is connected to a server. Storage of files can be found in an SFTP server, and the server gives clients information according to their requests. An SFTP client is a software that connects to the SFTP server. The client requests information from the SFTP server and clients can upload or download files from there.

The transfer protocol uses an SSH connection to securely transfer files. This is established by three steps and can be illustrated in **Figure 5**.

1. The SSH server is waiting for a request from the client and when a request is received, the server's identity is checked. If the client hasn't connected to the server before, a public key is needed, otherwise it will connect automatically.

2. A session key that can encrypt and decrypt data is agreed between the client and server. This encryption method is symmetric and is randomly generated.

3. An authentication is required from the server for the client to connect. The authentication is done by using a SSH key pair and this key pair consists of a public and private key. The public key is known for both, but the private key is only known by the client. The server then checks if the private key is correct and gives access.

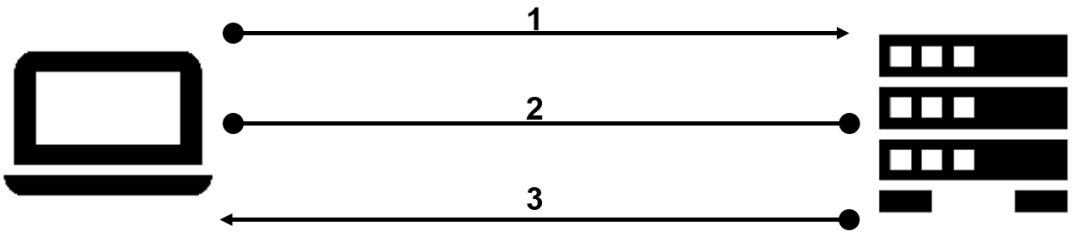

Figure 5. SSH connection (Nordmyr, 2022b)

When a three-way handshake and SSH connection have been established, a secure file transfer is ready. Files are transformed into packets and transferred through the encrypted SSH connection. The packets are then transformed back to the original files when they reach the end of the connection. (Thru, 25.10.2021)

6 Network protection

Industrial Control Systems (ICS) can be connected to the internet, and they might need to transport data or be remotely accessed by other users. Due to that cyber security is needed to protect the network. There are several of different methods to protect an ICS network from cyber threats. The intention of this thesis work is not to bring up all different security methods, but this chapter will contain information of basic components used to protect the network from threats.

6.1 Firewall

Firewall analyses all incoming and outgoing network traffic and blocks unwanted traffic. It can be a software or hardware and works as a security device. There are different types of firewalls depending on how much protection is needed and the size of the network.

Network traffic is monitored by the firewall and if any unknown traffic tries to access the operating system, they are blocked. A Firewall is configured to allow specific traffic to gain access to the network. This is done by defined security rules and only trusted IP addresses, or sources are welcome. A firewall protects the network from threats, and these can be for example hackers or malware.

A hardware firewall is a physical device that can protect the network from malware. It is often installed between the network and gateway. A software firewall on the other hand is not a physical device but is installed software on a computer. Traffic is then managed through port numbers and applications. (Forcepoint, u.d.)

6.2 DMZ Network

Demilitarized Zone abbreviated as DMZ, is a security method to protect the internal network. A DMZ is exposed to untrusted networks and is separated from the internal network. Inside the DMZ network are services that need to be exposed to untrusted networks such as mail servers, web servers and SFTP servers (goanywhere, 19.06.2019). The internal networks which are separated by the DMZ network are normally sensitive devices or data which need extra protection. That is why a DMZ network can give an extra layer of protection from untrusty networks like the internet.

Cyber threats can be detected and minimized before it reaches the internal network with help of the DMZ network. This is done by segregating devices in to separate sides of a firewall. Configuration of an DMZ network can be done in several different ways but there are two common methods, such as single firewall and dual firewall. **Figure 6** illustrates a dual firewall configuration. As the image illustrates the servers are now outside the firewall. Moving the servers outside the firewall will be more secure than having them inside the internal network because when people try to access the servers from untrusty networks, they will not reach the computers or sensitive data inside the internal network.

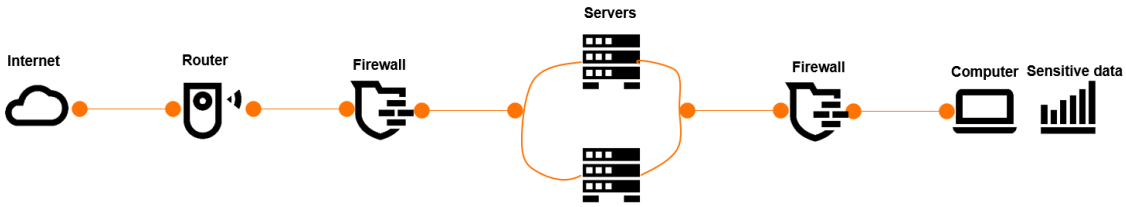

Figure 6. DMZ - Dual firewall configuration (Nordmyr, 2022c)

DMZ is surrounded by two firewalls in the dual firewall setup. The first firewall which is exposed to the untrusted network, only allows traffic to the DMZ. The second firewall which is faced to the internal network, controls the traffic from the DMZ to the internal network. The DMZ network is an important network security method to protect the internal network from threats. (Barracuda, u.d.)

7 Anomaly detection

When continuously measuring data, you acquire a large quantity of data points where behaviour patterns will emerge. Deviations can then be found if data points are outside the normal behaviour pattern, and this is known as anomaly detection. There are multiple ways to detect anomalies, among these are machine learning algorithms and rule-based systems. (Chandola, et al., 2007)

7.1 Machine learning

Machine learning is a technology that is built up by an algorithm. The key point of this algorithm is that it can be developed and learn from data by itself. This algorithm can then be improved over time with proper training and data input. There are different types of machine learning algorithms, but they are often categorized as supervised learning or unsupervised learning. Machine learning utilize different kinds of algorithms depending on the area of use. Machine learning is used for many purposes, for example anomaly detection, speech recognition, language translations and much more.

The machine learning algorithm can be simply explained with three keywords, such as task, experience, and performance. Machine learning is used to execute some kind of task and by executing these tasks experience is gained. The execution of the task needs to be evaluated continuously to be able to know how well the algorithm performs the task. In conclusion, a self-learning algorithm must be able to develop by itself with experience and evaluation of performance on the tasks. Without this self-learning function, it is a different type of algorithm.

Machine learning algorithms need data to be able to perform tasks. Data can be collected from various types of sources and a collection of many types of different data is called a dataset. A dataset can be used to train a machine learning algorithm. Predication of the output can then be made with help of the dataset. (Goodfellow, et al., 2016, pp. 96-161)

To get a better insight into how a typical machine learning algorithm works, it can be simply explained with the help of the illustrative **Figure 7**. First, divide the machine learning algorithm into three different parts, such as prediction, learner, and parameters. The training phase for the machine learning algorithm starts with a prediction on upcoming

values. The learner then differentiates real values with the predicted ones. Parameters will then be adjusted according to real values measured so the predicted outcome is more accurate. (Velthius, Frank (Wärtsilä), 21.08.2018)

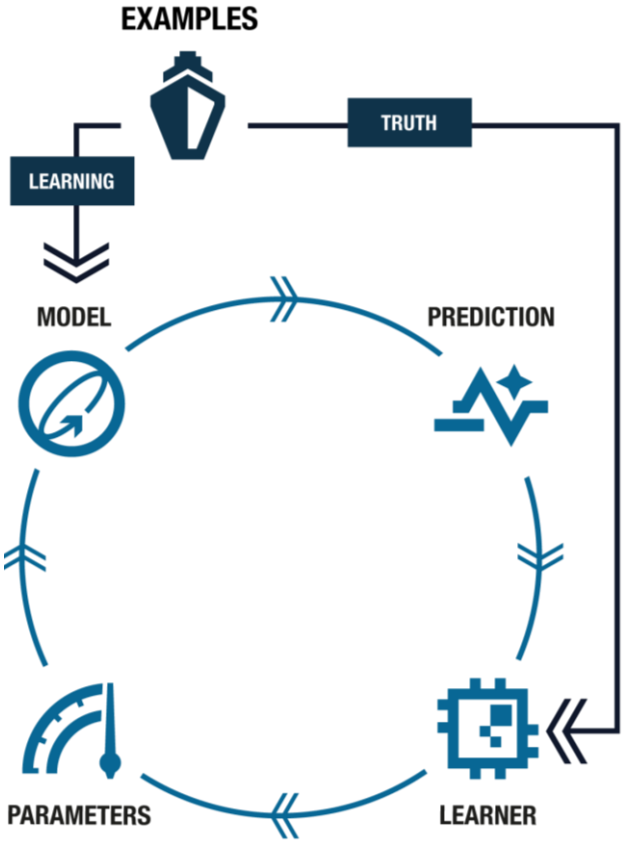

Figure 7. Example of a machine learning algorithm (Wärtsilä, 21.08.2018)

Supervised learning algorithms is a machine learning algorithm that requires a human being to supervise the process. The algorithm needs to be delivered with input and output data to be able to identify a relationship between the input and output. Data received is structured with labels. When the supervised learning algorithm has received enough data to train with, it can start to predict the output value itself. Therefore, it is called supervised learning because a human being needs to support the algorithm with output data.

Unsupervised learning algorithms is a machine learning algorithm that do not require a human being to supervise the process. The algorithm needs to be delivered with input data and it is unstructured. It will then analyse the data and find a pattern by itself. Therefore, it is called unsupervised learning because the algorithm can find the pattern between input and output data by itself, also structure the data collected. (Goodfellow, et al., 2016, pp. 96-161)

7.1.1 Wärtsilä Expert Insight – AI-based system

The Wärtsilä expert insight service uses an AI-based anomaly detection system. This AI-based system consists of several different machine learning algorithms to detect deviations or anomalies in operating data gathered from an installation. AI and a machine learning algorithm are not the same but the term of the two is often mixed up. Machine learning is many times used in the application of AIs, but the AI technology is a broad concept that uses many types of different technologies. (Velthius, Frank (Wärtsilä), 21.08.2018)

Machine learning provides systems the ability to find relevant patterns from historical data and fit a model accordingly. A machine learning system consists of an algorithm which is being trained on operational data from a power plant, this algorithm will try to create an optimal model by improving the parameters. Data is gathered from various sensors and a behaviour pattern will shape with the right amount of data collected. Data derived from the pattern is then found by the machine learning algorithms. The more data a machine learning algorithm gets provided, the better it will predict the outcome.

Figure 8 provides a simple view on how the AI-based detection system works. When operational data gets processed by the AI-based system, it will start to predict the outcome on its own. When the system compares the predicted outcome with the actual value, an anomaly is detected, if the predicted value differs from the actual. The AI-based detection system predicts all signals by itself retrieved from the installation's assets sensors. (Wärtsilä internal document, 2022a)

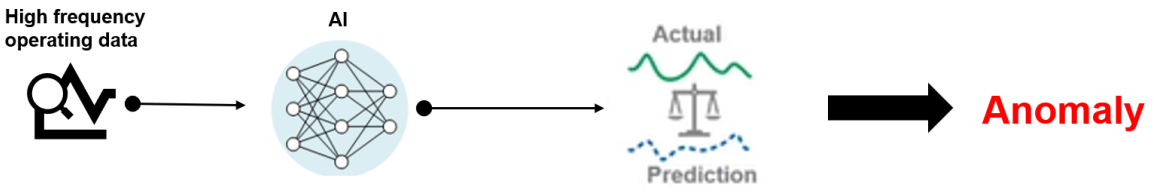

Figure 8. AI-based anomaly detection (Nordmyr, 2022d)

7.2 Rule-based system

A rule-based system like the name of the system reveals consists of rules for sorting, manipulating, or storing data. It can be used for many different things and among this is anomaly detection.

A rule-based system needs to process data to be able to use the configured rules applied. Data is processed by the rules and the outcome can then be an automated action if the rules is configured to do something. One simple example of an action that can be set up by a rule is to search for a specific word in a received email. If the rule has found an email containing the word, then the automated action could be to forward the email to another person.

These rules are created by human beings and is also known as “if statements” because rules often follow the concept of “IF X happens THEN do Y”. In a “if statement” the “IF” could be the specific word in the example mentioned and the “THEN” is the action like forwarding the email.

Machines can be controlled by using these rules but if there are many different actions there must be the same number of rules. For example, if there are 10 different actions, there must be 10 rules executing these actions. A rule-based system typically consists of seven basic components, such as the knowledge base, database, explanation facilities, user interface, external interface, interface engine and working memory. (Engati, n.d.)

7.2.1 Wärtsilä Expert Insight – Rule-based system

Wärtsilä Expert Insight service also uses a rule-based system and algorithms to identify deviations in operational data. These mathematical rules and algorithms are built upon product expertise, recommendations, engine specifications and asset configurations. With help of these rules and algorithms can the Expert Insight service capture the behaviour of the installation's assets.

When implementing these rules and algorithms on an installation, dynamic thresholds will be created. A dynamic threshold is an area where data is expected to land (LogicMonitor, u.d.). The dynamic thresholds are created upon a normal operating condition. Factors that can have an impact on the operating condition, can be for example ambient temperatures and engine load level.

A simple view of how the rule-based detection system works can be illustrated in **Figure 9**. Operational data is processed by mathematical rules and algorithms. The dynamic thresholds are then created by the rule-based system and are compared with the data gathered from the installation. If the operational data differs from the area created by the dynamic thresholds, then an anomaly is found. (Wärtsilä internal document, 2022a)

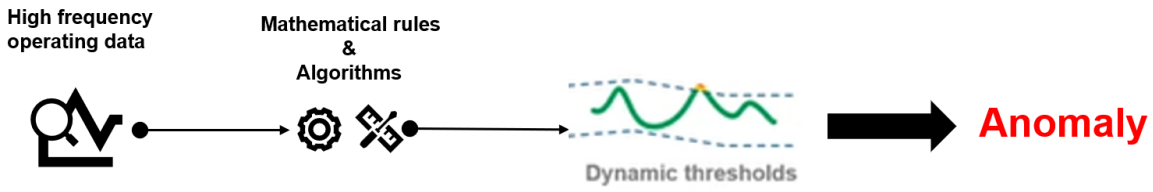

Figure 9. Rule-based anomaly detection (Nordmyr, 2022e)

7.3 Wärtsilä Expert Insight – Anomaly detection system

As mentioned, both AI-based and rule-based technologies are used in Wärtsilä's expert insight service. These technologies work together to detect deviations in operating data and try to prevent major incidents from happening to the installation's assets.

When data retrieved from an asset is deviating from either the predicted behaviour pattern or outside the dynamic thresholds, it will be highlighted for an Wärtsilä expert to investigate it. This could lead to an early detection of issues occurring at an installation, which could otherwise lead to major problems. Deviations detected do not necessarily have to be a major problem, but it can for example be an error value from the sensor or something else. **Figure 10** illustrates how both anomaly detection systems operate together. (Wärtsilä internal document, 2022a)

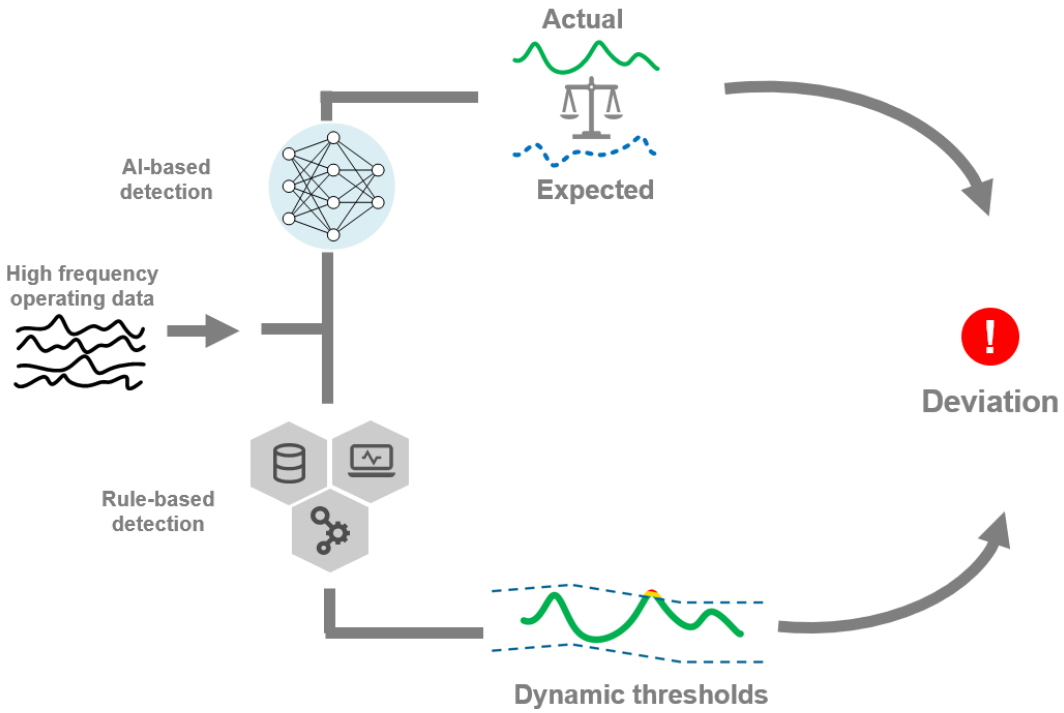

Figure 10. Expert Insight - Anomaly detection system (Wärtsilä internal document, 2022a)

8 Execution of the thesis work

The idea of my thesis work on Wärtsilä's remote digital services was brought up by my supervisor at Wärtsilä. My supervisor works as a sales manager at the Agreements Proposal Management department at Wärtsilä and he thought there was a need for a technical guide on these remote services. A meeting was then scheduled with a connectivity expert from Wärtsilä, where the thesis work idea was discussed. It was then agreed that there was a need for a guide that explains what these remote solutions are. The execution of the thesis work began by examining Wärtsilä's remote solutions and obtaining a table of content for the project.

8.1 Table of content

I started the investigation by researching what type of remote solutions Wärtsilä has and how they work. I read many of Wärtsilä's internal technical documents to get an understanding of the topic, besides that I also read literature that explains the type of technologies these solutions use.

When I had an idea of what the manual could contain for the practical work, I began to note what questions and topics this guide could explain and contain. I then scheduled a new meeting with the same members of the previous meeting and presented my idea of the table of content. The table of content got approved at this meeting and I started to investigate further in the topic.

The table of content for the practical work was mostly focusing on Wärtsilä's operational support and expert insight services but the technical documentation manual also covers information about other services that Wärtsilä has. The practical work made for Wärtsilä brings up several things like how these remote solutions work, connectivity, benefits they bring in Wärtsilä's Lifecycle Agreements and equipment requirements. In the thesis work I have chosen to describe only the operational support and expert insight service. Some of the content in the practical work has been left out from the thesis work because it contains confidential information about Wärtsilä and is not relevant for the thesis topic.

8.2 Investigation methods

I started the examination of the practical work by going through several internal Wärtsilä documents to collect the information needed for the work. Employees of Wärtsilä have supported me with relevant material and helped me to understand how these remote solutions work. When I had received enough material and understanding of the work, I started documenting.

Meetings were arranged from time to time with my supervisor and other employees at Wärtsilä to go through the practical work. During these meetings I got guidance and found out if the work has progressed correctly and where I can find further information. One of the attendees of these supervising meetings was a connectivity expert and he has connected me to experienced people at Wärtsilä and taught me how the connectivity works with these remote solutions. I had several conversations with experienced Wärtsilä employees to gather the information needed and find suitable material.

After I had worked for a while on the practical work, I decided to start working on the thesis work. I chose to work parallel on both works and finished them at the same time. I made this choice because the theory around these remote solutions is brought up in the thesis work and I thought that this information could be used in the practical work as well. This also led to me having the practical work in fresh memory and not forgetting anything of value in the thesis.

When I started working on the thesis work, I researched all types of theories that could be useful. The literature that has been used to execute the thesis work are webpages, books, articles, and studies made on the subject. Other than that, I have also had access to Wärtsilä's internal documents and meetings with both of my supervisors from school and Wärtsilä to get guidance.

Wärtsilä's remote digital services relies on data and connectivity. I chose to describe in my thesis the basics around these services and not go too deep in any subject. The material for my thesis topic is very wide and other technologies could also be included.

8.3 Completion of thesis work

When I had collected the information needed for the practical work, I checked with my supervisor if it was enough or if something else should be included in the manual. My supervisor then thought that the manual fulfilled his vision of what the practical work would contain. After that I tidied up the document and checked that the technical details were correct.

The completion of the practical work began when I had a first draft of the practical work, I sent it to my supervisor and the connectivity expert from Wärtsilä to review it. We scheduled a meeting to review the content where I got feedback and improvement suggestions. The technical documentation manual was then completed after I had made some minor adjustments to the document.

9 Results

In this chapter, I will present the results of the internal guideline made for Wärtsilä. In section 9.1 I will briefly explain what the technical guide contains, then in section 9.2 I will present my own view on what value this guide can have for Wärtsilä's employees.

9.1 Remote digital services - Guide

The technical documentation manual is a guide on the remote digital services that Wärtsilä offers in their lifecycle agreements. This guide will be internal and is intended to be used by people working within Wärtsilä, who want to improve their technical knowledge of these remote services. The guide is comprehensive, and the entire document is 39 pages long. The document is divided into seven different chapters, which I will briefly explain what these chapters contain below:

1. Chapter one introduces the guide and describes general information about its content.

2. The second chapter provides a short introduction of Wärtsilä's Expertise Centres and the remote services that are supported by them. This chapter goes deeper into what the operational support and expert insight services deliver and how they work. The chapter also covers information about other services that are supported by Wärtsilä's Expertise Centres.

3. Chapter three presents Wärtsilä's data collection systems. The chapter is mostly focused on Wärtsilä's sWOIS system and includes a central explanation of what the sWOIS is and its components.

4. The fourth chapter explains how data is transferred over the internet and how a remote access connection is established from Wärtsilä's Expertise Centres to the powerplant.

5. Chapter five lists general connectivity requirements like internet connectivity needed for these remote solutions.

6. Chapter six lists the required hardware needed for utilizing the remote services described in the manual.

7. The last chapter explains how these remote services impact Wärtsilä's Lifecycle Agreements and the benefits they can bring for the customer. The remote solutions are important in performance-based agreements, when Wärtsilä is offering guarantees.

9.2 Value of the guide

Increased knowledge of the remote services could benefit sales for Wärtsilä. I believe it is important that salespeople have an understanding of the service or product they are trying to sell. I have listed five points below that I believe could be improved within sales with help of this technical guide:

1. The confidence of sales personnel can be increased

2. Increased customer satisfaction

3. Trust of customers can be increased

4. Sales personnel can easier identify customer needs

5. Higher demand of these remote services

Confidence can be increased among salespeople because they have an understanding of how these remote services work and are not unsure whether they provide incorrect information to the customer or are afraid to answer questions. This can then also lead to the customer being more satisfied with the customer service they receive from the salespeople and provide higher trust in the company.

Increased knowledge of the services that the salesperson sells can facilitate the work of finding the customer's needs. For example, if the customer explains what he/she wants, so can the seller find a solution for the product or service they are selling. If you do not understand the services that you sell, you also do not know what they can do for the customer. The technical manual can also lead to higher demand for these services. If more people gain an understanding of what these services are, the information that these services exist can be spread internally and externally. Other than sales so can the guide also save time for Wärtsilä employees, instead of having to research multiple sources to gather information needed.

10 Conclusion

In this chapter I will present my conclusions of the thesis work. Challenges with this thesis work will be presented in section 10.1 and improvement suggestions will be presented in section 10.2. In the last section 10.3 I will summarize my own thoughts on the thesis work I have made.

10.1 Challenges

The most challenging part of this thesis work was knowing when to limit the content. The topic is very broad and includes many different types of technologies and subjects. The practical work did not have a clear scope from the beginning, so that also made this work a bit challenging, knowing what to include or not. This led me to do research in a wide area.

The practical work will be used for a pedagogical purpose of these remote services. This gives some challenges as well, when I had to explain technical things as simply as possible. I have also tried to explain the theory mentioned in this thesis work as simply as I could.

10.2 Further development

As mentioned, these solutions contain many different technologies. So, there may be more technical theories that could be included in this thesis work. I chose to take the most basic theories around the work, but these theories could be deeper explained.

The practical work was mostly focused on the operational support and expert insight services but Wärtsilä also has several cyber security services. These cyber security services could be further explained in the practical work.

10.3 Summary

The thesis work has been very time-consuming but rewarding. I have learnt a lot about the subject and the technical area around it. Most of the technical knowledge that the work required I had only a basic understanding of, but this thesis allowed me to get a deeper understanding of how everything works. I believe I will benefit greatly from this knowledge I have learnt from the thesis in the future.

I think that the technical documentation manual created for Wärtsilä, and the thesis can be of good use for Wärtsilä. In the practical work, employees at Wärtsilä can gain an understanding of the remote services and in the thesis an understanding of the theory.

By ending this thesis, I would like to thank everyone who has supported me with the thesis work:

I would like to thank my supervisor Willy Lågas from Wärtsilä for all the support that I have received with this thesis work. The idea for my thesis was first raised by him and it has been a very interesting thesis work.

I would also like to thank the connectivity expert Mattias Nilsson from Wärtsilä, he has helped me to understand how the connections work and connected me to other experienced employees of Wärtsilä to gather information.

I would like to thank everyone else at Wärtsilä who has helped me to carry out this thesis, in the interviews I have had to gather information and materials that have supported me throughout the work.

I would like to thank my supervisor Jan Berglund from Novia University of Applied Sciences, he has helped me to finish my thesis. I have received meaningful feedback that has helped me in situations where I have not known how to move forward with the thesis.

Finally, I would like to thank Wärtsilä for letting me write a thesis work for them. It has been educational to write a thesis for a successful company like Wärtsilä.

11 References

Barracuda, n.d. *Dmz Network.* [Online]
Available at: https://www.barracuda.com/glossary/dmz-network

Boyer, S. A., 2004. SCADA: Supervisory Control and Data Acquisition (3rd Edition). In: s.l.:ISA-The Instrumentation, Systems, and Automation Society.

Chandola, V., Banerjee, A. & Vipin, K., 2007. *Anomaly Detection: A Survey,* s.l.: s.n.

Cloudflare, 2022. *What is IPsec?.* [Online]
Available at: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

DPS Telecom, 08.08.2011. *SCADA Tutorial: A Quick, Easy, Comprehensive Guide.* [Online]
Available at: https://www.dpstele.com/pdfs/white_papers/scada.pdf

DPS Telecom, n.d. *How Do SCADA Systems Work?.* [Online]
Available at: https://www.dpstele.com/scada/how-systems-work.php

Electronics Hub, 02.04.2021. *What is a Sensor? Different Types of Sensors and their Applications.* [Online]
Available at: https://www.electronicshub.org/different-types-sensors/

electronics notes, n.d. *What is Data Acquisition.* [Online]
Available at: https://www.electronics-notes.com/articles/test-methods/data-acquisition-daq/understanding-data-acquisition.php

Engati, n.d. *Rule-Based System.* [Online]
Available at: https://www.engati.com/glossary/rule-based-system

Forcepoint, n.d. *What is a Firewall?.* [Online]
Available at: https://www.forcepoint.com/cyber-edu/firewall

GeeksforGeeks, 22.09.2021. *Synchronous Optical Network (SONET).* [Online]
Available at: https://www.geeksforgeeks.org/synchronous-optical-network-sonet/

goanywhere, 19.06.2019. *What is a DMZ and Why Do You Need a DMZ Secure Gateway?.* [Online]
Available at: https://www.goanywhere.com/what-is-a-dmz-and-why-do-you-need-a-dmz-gateway

Goodfellow, I., Bengio, Y. & Courville, A., 2016. Deep Learning. In: *Machine Learning Basics.* s.l.:MIT Press.

howstuffworks, 09.04.2021. *How a VPN (Virtual Private Network) Works.* [Online]
Available at: https://computer.howstuffworks.com/vpn.htm

LogicMonitor, n.d. *Enabling Dynamic Thresholds for Datapoints.* [Online]
Available at: https://www.logicmonitor.com/support/alerts/aiops-features-for-alerting/enabling-dynamic-thresholds-for-datapoints

Nordmyr, A., 2022a. *Data collection process.* [Art].

Nordmyr, A., 2022b. *SSH connection.* [Art].

Nordmyr, A., 2022c. *Dual firewall configuration.* [Art].

Nordmyr, A., 2022d. *AI-based anomaly detection.* [Art].

Nordmyr, A., 2022e. *Rule-based anomaly detection.* [Art].

phoenixNAP, 25.11.2021. *What Is SFTP?.* [Online]
Available at: https://phoenixnap.com/kb/what-is-sftp

polycase, 10.09.2021. *What Is a Programmable Logic Controller (PLC)?.* [Online]
Available at: https://www.polycase.com/techtalk/electronics-tips/what-is-a-programmable-logic-controller.html

Rescue, 2022. *A Guide to Understanding Remote Access and Remote Support.* [Online]
Available at: https://www.logmeinrescue.com/enable-remote-work/what-is-remote-access-remote-support

Tatum, M., 20.03.2022. *About Mechanics.* [Online]
Available at: https://www.aboutmechanics.com/what-is-an-actuator.htm

techopedia, 24.04.2020. *Protocol.* [Online]
Available at: https://www.techopedia.com/definition/4528/protocol

techopedia, 31.08.2021. *Cloud Storage.* [Online]
Available at: https://www.techopedia.com/definition/26535/cloud-storage

Thru, 25.10.2021. *SFTP Basics.* [Online]
Available at: https://www.thruinc.com/blog/what-is-sftp-and-how-does-it-work/

Velthius, Frank (Wärtsilä), 21.08.2018. *AI makes experts more curious and proactive.* [Online]
Available at: https://www.wartsila.com/insights/article/ai-makes-experts-more-curious-and-proactive

WhatIs, 2021. *SCADA (supervisory control and data acquisition).* [Online]
Available at: https://whatis.techtarget.com/definition/SCADA-supervisory-control-and-data-acquisition

Wikipedia, a. *Functional levels of a Distributed Control System.* [Online]
Available at:
https://en.wikipedia.org/wiki/File:Functional_levels_of_a_Distributed_Control_System.svg

Wärtsilä internal document, 2022a. *Expert Insight.* [Online].

Wärtsilä internal document, 2022b. *Wärtsilä Operator Interface System.* [Online].

Wärtsilä internal document, 2022c. *Operational Support.* [Online].

Wärtsilä, 2019. *WÄRTSILÄ OPERATORS' INTERFACE SYSTEM sWOIS.* [Online]
Available at: https://www.wartsila.com/docs/default-source/service-catalogue-files/electrical-automation-services/wartsila-swois-brochure.pdf

Wärtsilä, 2021a. *Wärtsilä Operational Support – Expert advice and support.* [Online]
Available at: https://www.wartsila.com/docs/default-source/services-documents/wartsila-operational-support.pdf?sfvrsn=c38a4d43_3

Wärtsilä, 2021b. *Wärtsilä Expert Insight – Enable Predictive Maintenance.* [Online]
Available at: https://www.wartsila.com/docs/default-source/services-documents/wartsila-expert-insight.pdf?sfvrsn=778c4d43_3

Wärtsilä, 2022a. *History.* [Online]
Available at: https://www.wartsila.com/about/history

Wärtsilä, 2022b. *About.* [Online]
Available at: https://www.wartsila.com/about
[Accessed 07.02.2022].

Wärtsilä, 2022c. *Wärtsilä businesses in brief.* [Online]
Available at: https://www.wartsila.com/media/businesses-in-brief

Wärtsilä, 2022d. *Remote support and data management.* [Online]
Available at: https://wartsila.prod.sitefinity.fi/energy/services/lifecycle-solutions/remote-support-and-data-management

Wärtsilä, 2022e. *Expertise Centres graph.* [Online]
Available at: https://wartsila.prod.sitefinity.fi/images/default-source/power-plants-pictures/optimising-power-plant-operations/we-serve-you-all-the-way.png?sfvrsn=46408844_2

Wärtsilä, 21.08.2018. *Machine learning system graph.* [Online]
Available at: https://www.wartsila.com/images/default-source/twentyfour7/in-detail/ai-makes-experts-more-curious-and-proactive3095b504b7f0f601bb10cff00002d2314.tmb-thumb425.png?sfvrsn=80543044_1

Wärtsilä, a. *sWOIS graph.* [Online]
Available at: https://www.wartsila.com/images/default-source/power-plants-pictures/cyber-services/swois-_graph.png?sfvrsn=eccca044_0