YRKESHÖGSKOLAN
NOVIA

Analysis of a Wärtsilä power plant control system network layout

Tobias Holmqvist

Degree Thesis for Bachelor of Engineering

Degree Programme in Electrical and Automation Engineering

Vasa 2022

EXAMENSARBETE

Författare: Tobias Holmqvist
Utbildning och ort: El- och automationsteknik, Vasa
Inriktning: Automationsteknik
Handledare: Jan Berglund, Benny Lassus

Titel: En analys av styrsystemets nätverkslayout för ett Wärtsilä kraftverk

---

Datum: 10.5.2022 Sidantal: 34 Bilagor: 1

Abstrakt

Detta examensarbete gick ut på att göra ett överskådligt dokument över hur automationslayouten för ett Wärtsilä elkraftverk är sammankopplad och vilka standarder detta kraftverk följer. Syftet med detta examensarbete var att få en bättre uppfattning om automationslayouten och att samla väsentlig info för Technical Sales Support-avdelning. Technical Sales jobbar mycket med offerter och klargör för kunden för vilka protokoll och standarder Wärtsilä följer.

Examensarbetet börjar med en teoridel där utomstående research tas upp och behandlar grunderna över de viktigaste standarderna och kommunikationsprotokollen. I följande kapitel behandlas hur dessa fungerade i praktiken i Wärtsiläs elkraftsautomationssystem.

För att förstå sig på hur allt fungerar i praktiken behövs mycket bakgrundsfakta och kunskap för att kunna förstå de väsentliga delarna för varje standard. Bakgrundsfakta togs främst från artiklar på nätet men även från hemsidor för grundarna av standarderna. Den praktiska delen gick ut på att intervjua kollegor och experter från de olika områdena inom elkraftsautomationssystem. Wärtsilä har även en bred databas med väsentliga dokument som kunde användas som informationskällor till examensarbetet.

Detta examensarbete kommer användas av både personal på Wärtsilä och även av kunder ifall de behöver tilläggsinformation om vad Wärtsilä kan erbjuda. Detta examensarbete har också gett mig mycket kunskap och erfarenhet för mina framtida arbetsuppgifter. Mina arbetsuppgifter har varit att komplettera automationslayoutsritningar. Med examensarbetet finns det möjlighet för utveckling och förbättringar i dessa layouter.

Språk: engelska
Nyckelord: standard, kommunikationsprotokoll, cyber security

OPINNÄYTETYÖ

Tekijä: Tobias Holmqvist

Koulutus ja paikkakunta: Sähkö- ja automaatiotekniikka, Vasa

Suuntautumisvaihtoehto: Automaatiotekniikka

Ohjaajat: Jan Berglund, Benny Lassus

Nimike: Analyysi ohjausjärjestelmän verkkolayoutista Wärtsilän sähkövoimalassa

---

Päivämäärä 10.5.2022 Sivumäärä: 34 Liitteet 1

Tiivistelmä

Tämän opinnäytetyön tarkoitus oli tehdä selvä dokumentti, miten automaatiolayout Wärtsilän sähkövoimalassa on kytketty yhteen ja mitä standardia se seuraa. Tämän opinnäytetyön tarkoitus oli saada parempi käsitys automaatiolayoutista ja kerätä tärkeää tietoa Technical Sales Support -osastolle.

Technical Sales Support tekee paljon työtä tarjouksien parissa, ja selventää asiakkaille mitä protokolleja ja standardeja Wärtsilä seuraa.

Opinnäytetyö alkaa teoriaosuudella, jossa ulkopuolinen tutkimus ja tieto otetaan esille, ja siinä käydään läpi tärkeimpien standardien ja kommunikaatioprotokollien perusteet. Seuraavissa luvuissa käydään läpi, miten nämä toimivat käytännössä Wärtsilän sähkövoima-automaatiojärjestelmässä.

Jotta voi ymmärtää miten kaikki toimii käytännössä, tarvitaan paljon taustatietoja, että voi ymmärtää välttämättömät osat jokaisessa standardissa. Taustatietoja otettiin suurimmaksi osaksi artikkeleista ja teksteistä netistä, mutta myös standardien perustajien kotisivuilta. Käytännön osa koostui kollegojen ja asiantuntijoiden haastatteluista sähkövoima-automaatiojärjestelmän eri alueista. Wärtsilällä on myös laaja tietokanta tärkeitä dokumentteja, joita oli mahdollista käyttää tietolähteenä opinnäytetyöhön.

Sekä Wärtsilän henkilökunnalla että asiakkailla on mahdollisuus käyttää tätä opinnäytetyötä, jos he tarvitsevat lisätietoa siitä, mitä Wärtsilä voi tarjoa. Tämä opinnäytetyö on myös antanut minulle paljon tietoa ja kokemusta tuleviin työtehtäviin. Työtehtäväni on ollut automaatiolayoutien piirustuksien täydennys. Opinnäytetyöni kautta näitä layouteja voidaan edistää ja parantaa.

Kieli: englanti
Avainsanat: standardi, kommunikaatioprotokolla, tietoturva

BACHELOR'S THESIS

Author: Tobias Holmqvist
Degree Programme: Electrical Engineering, Vasa
Specialisation: Automation
Supervisor(s): Jan Berglund, Benny Lassus

Title: Analysis of a Wärtsilä power plant control system network layout

---

Date 10.5.2022 Number of pages: 34 Appendices 1

Abstract

This thesis work is based on writing a document on how Wärtsilä's power plant automation layout works. The document contains how the automation components are connected and what standards and communication protocol Wärtsilä is using. This thesis aims to get a better understanding of what protocols and standards Wärtsilä is utilizing in power plant automation. This information will be gathered for the Technical Sales Support department.
Technical Sales daily work is offering projects to clarify for the customers what standards and protocols Wärtsilä is applying.

The thesis begins with a theory chapter where all the extern research is brought up. The main part examines the basics of communication protocols and how to secure the communication within the network automation.

In the following chapter, a closer look is taken at how these protocols and standards are implemented in the automation system for a Wärtsilä power plant. The basic knowledge for every protocol is needed to understand how communication works within an automation system. Most of the basic information was taken from articles on the internet but also the internet websites by the founders of the standards. The information of the more practical part of the thesis work is based on interviews with colleagues and experts in different departments in the company. Another method was gathering information that was found in Wärtsilä's internal database.

This thesis work will benefit both the staff within Wärtsilä and future customers. The work I have done has also given me a great amount of knowledge on how automation systems work within a power plant. This will benefit my daily work at Wärtsilä which has been helping with the automation layout drawings for projects.

Language: English
Key words: standard, communication protocol, cyber security

Content

Figures

1 Introduction

This thesis work is about some clarifications about Wärtsilä's automation layout for power plants. Prior documents and information about the automation layout are either unclear or outdated and most of the clarifications are outspread over several documents. That is why this document is going to involve all the updated information in one document to help the sales offering. This document can also be used for clarification to the customer about the standards and protocols Wärtsilä is applying to.

1.1 Background

Wärtsilä is a world-leading company in the Marine and Energy Business. Wärtsilä was founded in 1834 as a sawmill. Today, Wärtsilä sells engines and navigation systems for vessels in the Marine Business and power plant and battery storage solutions in the Energy Business. In the Energy Business Department, Wärtsilä is providing power plants that are mainly based on Wärtsilä engines. The power plants can be used as backup systems to prevent blackouts which are common for places such as islands and where the electrical distribution is more difficult.

What is new for Wärtsilä is BESS. Instead of using engines to provide the energy, the system is using batteries to be able to store the energy. This can also be combined with a Wärtsilä power plant. All these energy solutions strive for a sustainable environment and Wärtsilä trying to provide for a sustainable future.

1.1.1 Purpose

The main purpose of this thesis work is to clarify standards, protocols, and IT security practices for the automation system. Until this day, there is no general document that clarifies this information. This thesis will help to make the job easier for the Technical Sales department and the Sales offering department. Technical Sales Support is a department that supports in the sales phase where extra support is needed. The work is very variable depending on the project and customer.

Often these days the standard sales project needs to be customized according to the customer's request. This is very time and cost consuming and that is why my thesis work will hopefully help in the sales phase. In the early sales stage, everything what Wärtsilä can provide is going to be clarified for the customer. With the automation layout clarification, the document will help both the customers and the internal personnel in Wärtsilä.

1.2 Central terminology

BESS - Battery Energy Storage System

IEC – International Electrotechnical Commission

IED – Intelligent Electronic Device

MMS – Manufacturing Messaging Specification

GOOSE – Generic Object-Oriented Substation Events

SMV – Sampled Measured Values

WOIS – Wärtsilä Operator's Interface System

IACS – Industrial Automation Control Systems

BMBF – German department of education and research

MBP – Manchester Encoded Bus Powered

SL – Security Level

OPC – Open Platform Communication

UA – Unified Architecture

TCP – Transmission Control Protocol

IT – Information Technology

OT – Operational Technology

HTTP – Hypertext Transfer Protocol

SOAP – Simple Object Access Protocol

TCP – Transmission Control Protocol

IP - Internet Protocol

DMZ - Demilitarized Zone

GEMS – Wärtsilä's energy management system

ICS – Industrial Control System

CFAT – Cyber Factory Acceptance Test

WCSB – Wärtsilä Cyber Security Baseline

PPC – Power Plant Controller

AWS – Amazon Web Services

DoD – Department of Defence

DCS – Distributed Control System

RTU – Remote Terminal Unit

1.3 Sales offering

A sales offer for a power plant is quite complex, so in the next section, an example of a project offer will be presented. The customer first sends a request for information. If the request is approved, a first solution indication is given to the customer with an estimate of pricing and standard information and finally, a feasibility study. This first phase is called the discover sales. If the project gets approved, the customer sends an offer request which is getting reviewed and screened. If the project offer is approved the project proceeds to the plan sales phase. If there is any issue with the offer, then the project must get reviewed

and screened again to check if there are any solutions to the issue. If there are no possible solutions that Wärtsilä can provide, then the project offer is declined.

However, if the offer is getting all the approval that is needed, then a closer look at the customer's requirement will be taken. In this stage, a firm offer is being made for the customer to review if the offer should be updated or not. If the offer is not being updated, then it goes to a held opportunity or lost opportunity depending on if the offer is being updated later.

The department that I work for is Technical Sales Support, which is a team that supports the project offer mainly in the plan sales phase. The team can also be involved in the whole process of the offering, where expertise is needed. Typical daily work for the Technical Sales Support team is to clarify the details of the project with the customer and what Wärtsilä can deliver.

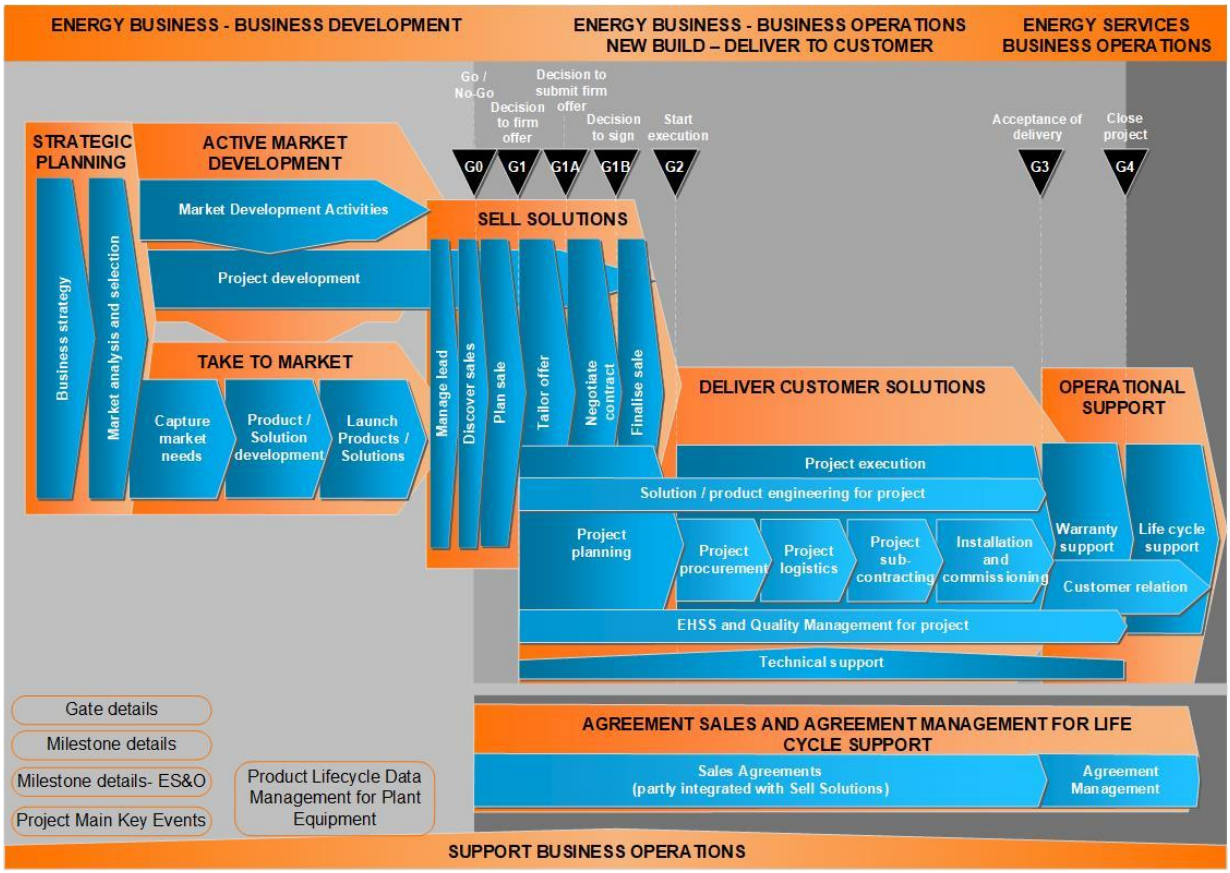

Figure 1 Sales offering stages

2 Communication Protocols

This chapter will present some general standards and protocols that they cover. Firstly, the chapter begins with an explanation of how the data is being sent by the OSI- and DOD models. Then the standard IEC 61850 standard will be presented and communication protocols that are being used in the Wärtsilä power plant automation network. Much of the standards are covering the basics of IT and OT network communication. Basics in remote connection and data traffic between networks will also be presented to clarify all the standards and terms.

2.1 OSI Model

OSI stands for Open Systems Interconnection and defines the framework of the functions in a network structure. It was developed in 1984 by the International Organization for Standardization. Seven layers describe how the network is structured.

Figure 2 OSI model layers

This model describes how the data is sent and received through networks. Each of these layers applies its own protocols. The application layer uses all the necessary protocols for web browsing, file transfer, and emails. This applies to the software that is used for

communication. Presentation layers receive the data from the application layer and make sure the data is converted to the right file format. It also defines how to encrypt, decrypt, and compress the data. The session layer is establishing the authentication and authorization of the communication. This layer involves communication coordination and setup. Usually, a computer connects to a server to retrieve data and with the session layer, this data transferring is possible.

The transport layer can be divided into services and protocols. Services can be provided in either connection-oriented transmission or connectionless transmission. The connection-oriented transmission uses transmission control protocol (TCP), and connectionless transmission uses user datagram protocol (UDP). The network layer defines the IP addressing and routing to establish the connection right. Datalink layer is framing the data packet and giving the mac address to where the data shall be sent to. And finally, the physical layer is providing the physical connection and converts the data into bits. After the data have gone through all these 7 layers then the message is completed. (OSI Model, n.d.)

Another Model that is a reference to OSI Model, is the TCP/IP Model, or also called DOD Model. This model is a more compact model compared with the OSI Model. It only consists of 4 layers that are based on TCP/IP protocol. (Shaw, 2022)

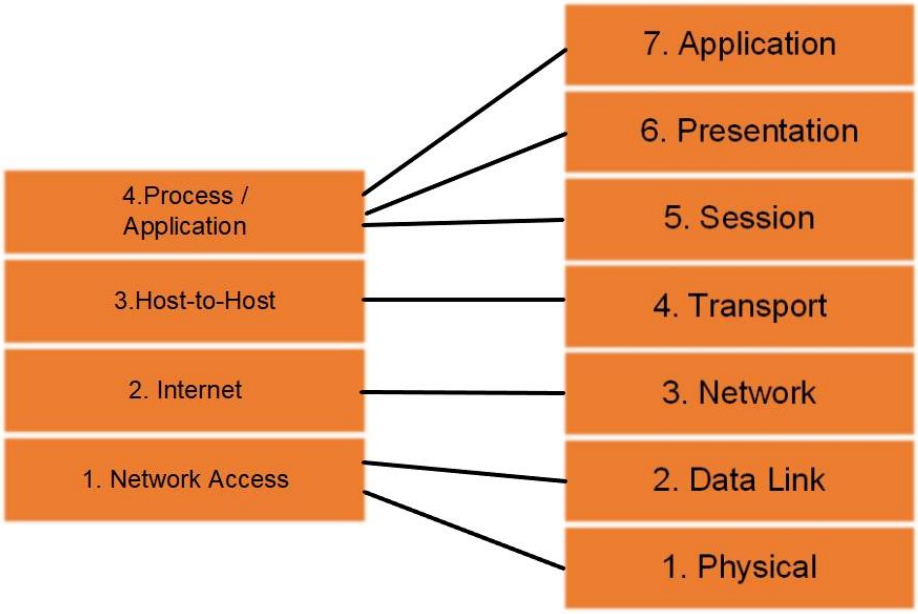

Figure 3 The DoD Model compared to OSI Model

2.2 IEC 61850

This standard was developed due to the great differences in communication protocols of the equipment in the substations or power generation facilities. To provide a clear definition to the manufacturer the IEC 61850 was developed. The standard is directed to IEDs. The purpose of the standard is to make the configuration between devices that are made by different manufacturers, more compatible. This reduces both time and costs in the installation phase. (Basic understanding of IEC 61850, 2021)

A typical architecture for IEC 61850 can be dived into 3 levels. The first level is Process Level which is the detailed level where all circuit breakers, switchgear, switches, and other devices are configured. The next level is on the Bay level where the IEDs are located that control the switchgear and breakers. The last level is the station level that is covering the monitoring aspects with Scada and HMI systems. To be able to communicate with an IED which is at a bay level, a station bus is implemented. Communication protocols that cover the IEC 61850 are MMS, GOOSE, and SMV. (Basic understanding of IEC 61850, 2021)

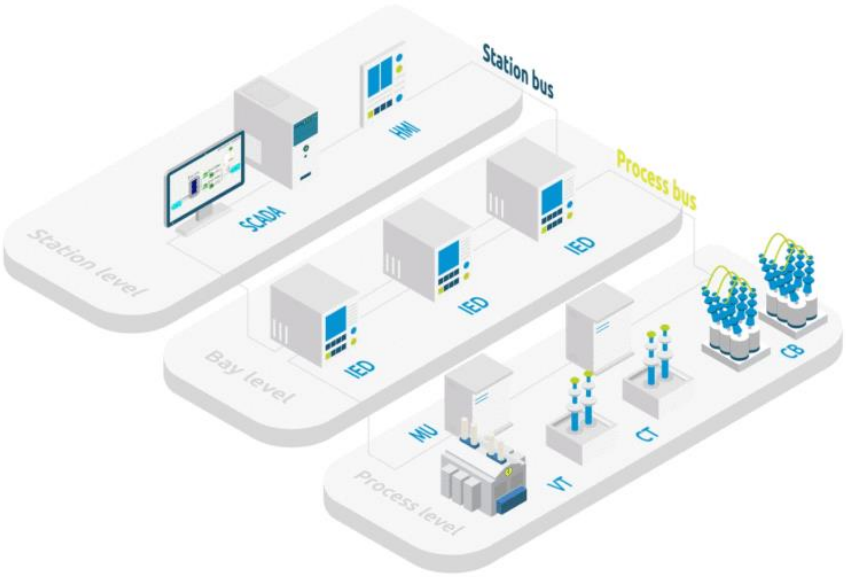

Figure 4 IEC 61850 architecture

The first protocol MMS is covering monitoring and configuration of the communication between the IEDs and SCADA system. The next protocol GOOSE is covering the status of the IEDs and is working as a safety measure to monitor that all devices are working

correctly. The third protocol SMV is covering the monitoring, protection, measurement, and control of the system transformers. (Lydon, 2009) (RealPars, 2020)

2.3 Profibus

Profibus is a standard for fieldbus communication in automation systems. It was founded in 1989 by BMBF which got later used by Siemens. Profibus is an open standard based on the standard IEC 61158 which covers fieldbus specifications. There are two types of Profibus protocols. Profibus DP, which is the most common type, and Profibus PA. With the Profibus DP, the physical layer is being used by RS-485. (Procentec, n.d.)

Profibus DP is mainly used for operating actuators and sensors through a controller. This method required a lot of cables that would individually be connected from the IO to the specific sensor. With Profibus PA, the actuators and sensors can instead be connected using only one cable. A segment coupler must be installed between the PLC and the sensors and all the sensors are then installed on a Profibus-PA bus. This method removes all the individual cables and now it requires only one Profibus-PA cable. The segment coupler converts all the Profibus-PA signals to a Profibus-DP device. The reason why to convert to Profibus-DP device is that PLCs only can connect to Profibus-DP device. All the sensors can either be connected to a general bus or together even called daisy-chaining. (RealPars, 2020)

2.4 Profinet

Profinet is a fieldbus system based on Ethernet. It is defined as an open industrial Ethernet standard developed in the early 2000s. Profinet has many similarities to Profibus, but it is also an improvement of the communication protocol. The standard is describing the data exchange between controllers and devices. The main difference between Profibus and Profinet is that Profinet communication can operate at a higher transmission speed. Another difference from Profibus is that Profinet is using the DoD model structure instead of the OSI model.

The Profinet has a safety protocol called Profisafe. Profisafe defines how the Profinet product is protected. The protocol has a detection measure for errors and failures in communication. A Profinet network can be constructed by five different network

topologies. The five topologies are tree, star, ring, line, and wireless. (Ayllon, WHAT IS PROFINET? – PROFINET EXPLAINED, 2021) (organization, 2021)

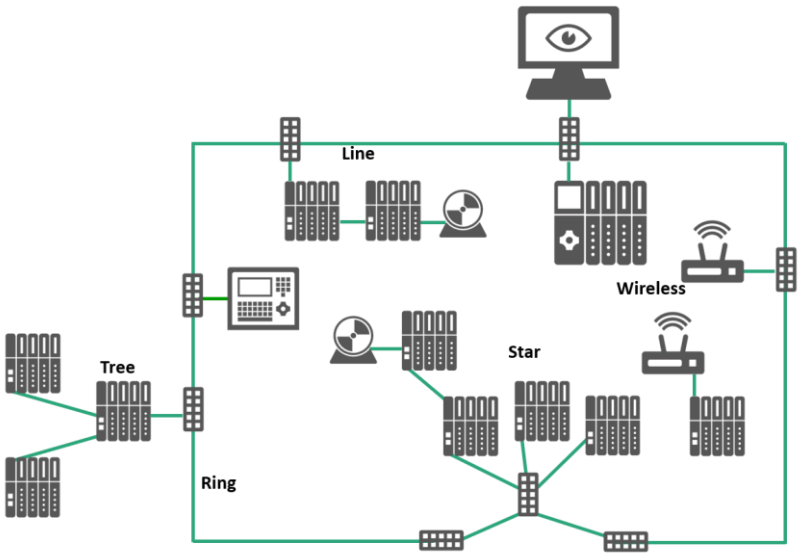

Figure 5 Profinet network topologies

2.5 Modbus

The Modbus protocol is a communication standard that was founded by Modicon in 1979 for Modicons' programmable controllers. With time the Modbus protocol has become a major industry standard for transferring analog- and digital information between several industry devices. Modbus is today an open and public-domain protocol but to be able to implement this into the system, a license is required. (Organization, n.d.)

The communication is built on a master-slave technique where some devices are only sending a request and then the other devices are giving a response by supplying the requested data. The master is only sending out a request and the slave only responds according to that. To be able to establish a connection, both master and slave should have the same baud rate. Baud rate or bit per second is the rate of speed of how fast a message can be sent.

The most common form of serial communication is RS-485 or Ethernet. The Modbus protocol can be divided into Modbus ASCII, Modbus RTU, and Modbus TCP/IP. Modbus ASCII is the original protocol that was built on encoding the messages by using ASCII

characters. This protocol is still used today but on a smaller scale compared to the other two protocols. Modbus operates according to memory registers for configuration, monitoring, and controlling devices. It uses the OSI model to send and retrieve data. (Company, 2013)

2.5.1 Modbus RTU

The most used type of Modbus today is the Modbus RTU. The protocol uses binary coding to send a message. There are three forms of serial communication: RS-232, RS-422, and RS-485. The reason why RS-485 is most used with Modbus RTU is the ability to connect to 32 nodes maximum with a range of about 1,2 km. In a Modbus RTU network, there can only be one master and 247 slaves but if there are more than 32 nodes a repeater must be used. The network topology with Modbus RTU is a daisy-chained network and can't function in a star topology. (Technology, 2014)

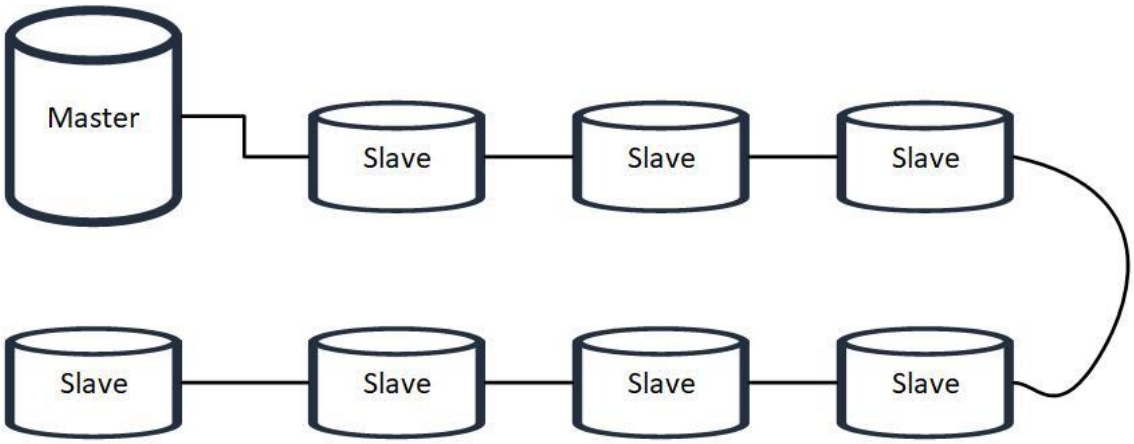

Figure 6 Modbus RTU Network

2.5.2 Modbus TCP/IP

Modbus TCP/IP runs on Ethernet and requires a network connection either LAN or WLAN. The TCP protocols ensure that all data packages are received correctly. IP protocol is the part that addresses where the data shall be sent to. Instead of master and slave, the TCP/IP uses Client and Servers. The Servers are connected to a switch which is then connected to the Client. With Modbus TCP/IP there can be more than one master/client, unlike the Modbus RTU. (INCORPORATED, 2005)

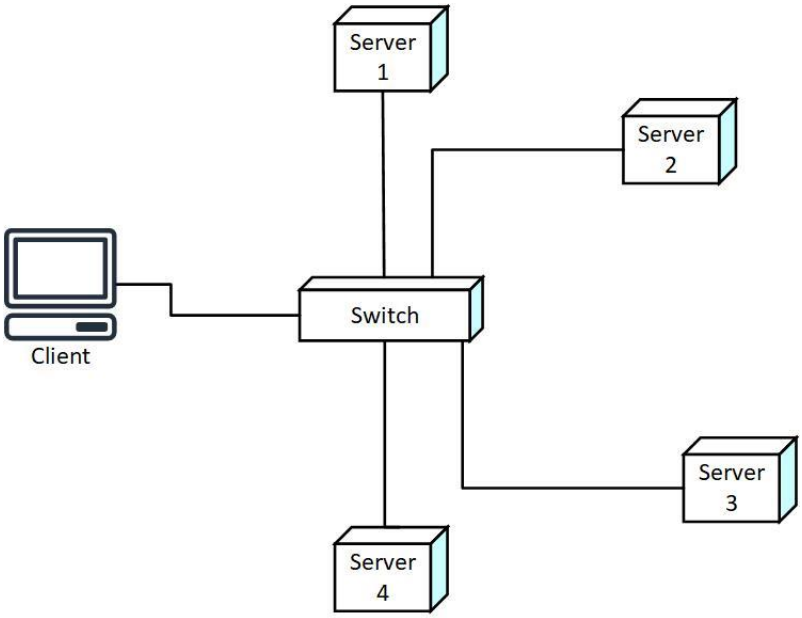

Figure 7 Modbus TCP/IP Network

2.6 S7 – protocol

S7-protocol is associated with Siemens's communications that are used with Ethernet that relies on ISO TCP, a package-oriented data formatting with combined data transfer methods. Its functions are oriented where the package or message is containing a command and a reply. Each command consists of a header, data block, parameter data, and a set of parameters. (IGSS, n.d.) S7 commands can be divided into 9 categories:

- Data read/written from/to SCADA
- Cyclic data read/written from/to SCADA
- Directory info
- System info
- Blocks move
- PLC control
- Date and time
- Security

- Programming PLC

The protocol is used for communication between Siemens PLC or other Siemens devices that support S7 communication.

2.7 OPC

Another standard that is essential for communication within the automation system is OPC. The OPC Foundation has been responsible to define and develop the standard and stands for Open Platform Communication. In the industrial automation in the 90s more automation organization was developing their own devices, and this led to complications for the customer if there had a system with different branded devices. To be able to avoid these issues a general standard was created, called OPC. (What is OPC?, 2022)

It was founded in 1996 and had the purpose to apply specific protocols to PLCs and make a standardized interface for them. The OPC could provide several specifications such as data access (DA), alarms and events interface (A&E), and historical access (HA). These specifications were needed to be able to gather data from all the devices in the same interface. (Foundation, 2022)

It was originally based on Microsoft technologies COM and DCOM and therefore restricted to only Windows operative systems. This way of communication is called OPC Classic. This standard is however not often optional due to its limited communication compatibility. (Foundation, 2022)

2.7.1 OPC-UA

The disadvantage with this way of communication was that OPC Classic is limited, which is why OPC UA was created. It was now not only for Windows and could be used by other operating systems. OPC UA can be described as a machine-to-machine communication protocol for industrial automation. Now the communication could be between other platforms as well and not be as limited as the OPC Classic standard. OPC UA can provide more complex data compared to the OPC Classic. It is a standard of information interchange that is built on a Client/Server model. The standard is built on a multilayered design to fulfill

goals. The goals are mainly to provide security and the ability for updating in the future. (What is OPC UA? A practical introduction, 2022)

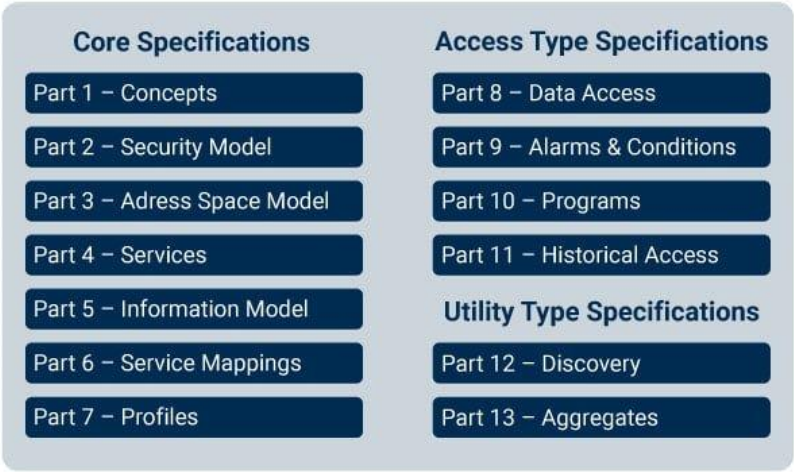

Figure 8 OPC UA Specifications (What is OPC UA? A practical introduction, 2022)

2.7.2 OPC Client

OPC is built in a Client-Server architecture where the OPC Client is in control over the server. It is software-based, and the client is doing all the demanding tasks such as retrieving data or other requests and the server is providing those requested data. It is like Modbus where master-slave communication is used. (SolUK, 2019)

2.7.3 OPC Server

The OPC Server is only performing actions when the OPC Client is sending a request. It is software-based and is managing all the devices such as PLC. The OPC is responding to requests both by retrieving data or sending data values to specific PLCs. The software is then easily implemented by the manufacturer of the hardware. (SolUK, 2019)

3 Cyber Security

With today's technology and digitalization, cybersecurity has become an essential factor in both IT and OT systems. More products and devices are using network connections and

could be a weak spot if not right security countermeasures are being considered. With the modern digitalization of the OT systems and the cross-communication to IT systems, access to the network needs to be limited and secure. To connect to an OT system outside the local network, a network connection is needed. The OT system is then exposed to the internet if not right cybersecurity countermeasures are done.

Cybersecurity shall not only cover how to protect a system but also what shall be done if malicious access has occurred. In this chapter, we will first learn about the standard IEC 62443 that is used in cybersecurity and then go through how to protect the system with firewalls and DMZ networks.

3.1 IEC 62443

The standard IEC 62443 is a developed standard for industrial automation and control systems. Following the standard does not only comply with technology but also with the work process and employees and countermeasures. (Team, 2021)

The IEC 62443 can be divided into four layers. The first layer is the general layer that is covering concepts, introductory information, and models. The second layer is policies and procedures which focuses on methods and processes. This layer is directed towards the asset owners and covers all from maintenance of the cybersecurity to training for personnel to maintain a secure system. The third layer is the system layer where requirements and design for the system are covered. For example, a system could be divided into several security zones to protect the automation system and prevent those cyber-attacks from getting access to the whole system at once. Finally, we have the fourth layer which is the component layer that covers more detailed product requirements such as product development lifecycle and technical security. This layer is meant for the manufacturers of the products. (Foster, 2020)

All these different types of standards are categorized in the chart below:

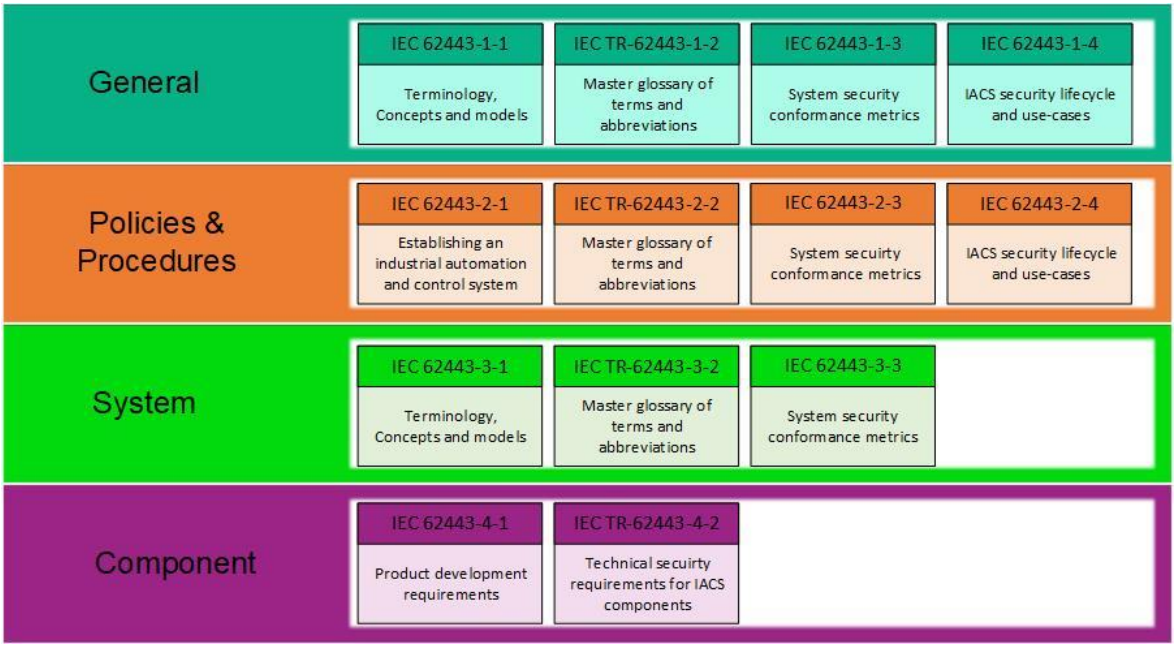

Figure 9 IEC 62443 layers

To achieve cyber security according to IEC-62443, training is needed for the personnel if the company shall comply with the standard. The standard can also be divided into several security levels. There are three security levels the IEC 62443 can be divided into:

1. Target security levels (SL-T)
2. Capability security levels (SL-C)
3. Achieved security levels (SL-A)

These are sub-levels that define the minimum capabilities of the device or system. There is also another defining level of maturity that defines how the security process looks like and how an organization is handling cyber security. (Medoff, 2018)

3.2 Firewall

A firewall is a good way to protect a network in form of either hardware or software. The firewall provides a filter for data traffic and blocks access from all outside unauthorized communication to the network. Filtering is checking what source or IP address grants access and through the configuration of the firewall the access granted sources will get data access. Another way of protection that the firewall can provide is also to block

malicious software from spreading to your computer. It was created in the late 1980s and has with time developed into advanced technology. (Johansen, 2021)

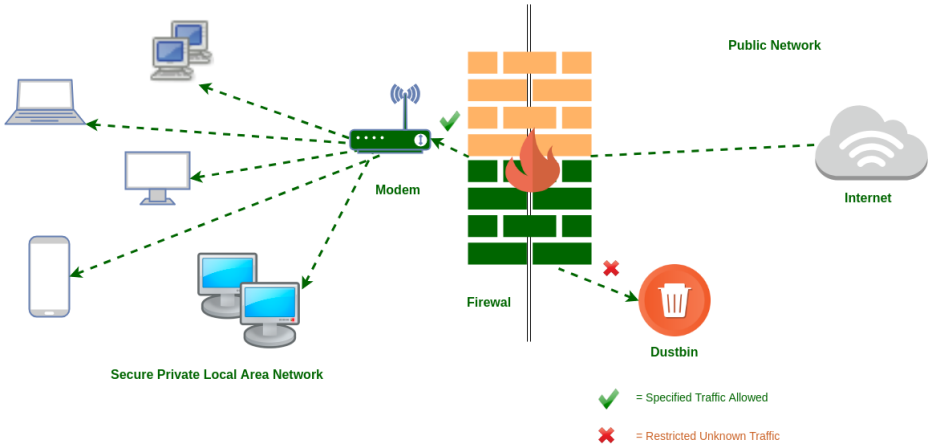

Figure 10 Firewall Gateway (Packet Filter Firewall and Application Level Gateway, 2021)

Several types of firewalls can protect the network. A hardware firewall can be a broadband router that is placed between the network and gateway. A software firewall is typically software that filters data traffic and blocks malicious software. With the software, you can protect applications on the device. The third firewall type is a cloud-based firewall that can be provided as a service. It is based on virtual firewalls that work both over physical and virtual networks. It can be an advantage for a larger company to use this type, as no hardware needs to be changed over time.

There are many methods and many different types of firewalls to protect the network. A Proxy service firewall is usually hardware that works as a gateway between the internal network and the internet. It manages to filter data messages at the application layer. Packet filtering is another way to monitor and analyze the incoming data. Two other types of firewalls are UTM and NGFW. UTM firewalls are a bundle with several services and are very complex firewall systems. NGFW is the most advanced firewall type and unlike the classic firewall, it is developed to prevent network security breaches before the attack occurs. (Packet Filter Firewall and Application Level Gateway, 2021)

3.3 DMZ Network

A DMZ network could be described as protecting a perimeter network that has similarities to firewalls. The purpose of the DMZ network is to add an extra security layer to the local network and is recommended for a network where the user is outside of the local area network. To optimize the internal network two firewalls are ideal with the DMZ server. The DMZ itself works as a security gateway that isolates the internal network from the internet but enables outside network usage to the servers. A DMZ server cannot access confidential data and therefore the hosts have very limited access. The firewall is filtering and separates data traffic between DMZ and the internal network. (DMZ Network, n.d.) (DMZ, n.d.)

So why is DMZ Network so important? For home networks, it would not be essential when the user is often just using data traffic from the internal network to the internet and not the other way around. This can be relevant for larger networks for companies that need data trafficking both ways.

The most common services that use DMZ are web servers, mail servers, FTP servers, and internet routers. Web servers are maintaining communication and can interact directly with the internal database. For security reasons, it is placed between the internet and the firewall. Mail servers are servers where all the email and personal contact information are stored. The server is also placed between the internet and the firewall. The router shall also be in the DMZ network for ordinary web browsing which often can be a weak spot and an opening to the internal network. The picture below illustrates what the DMZ network architecture looks like. (Lutkevich, DMZ in networking, 2021)

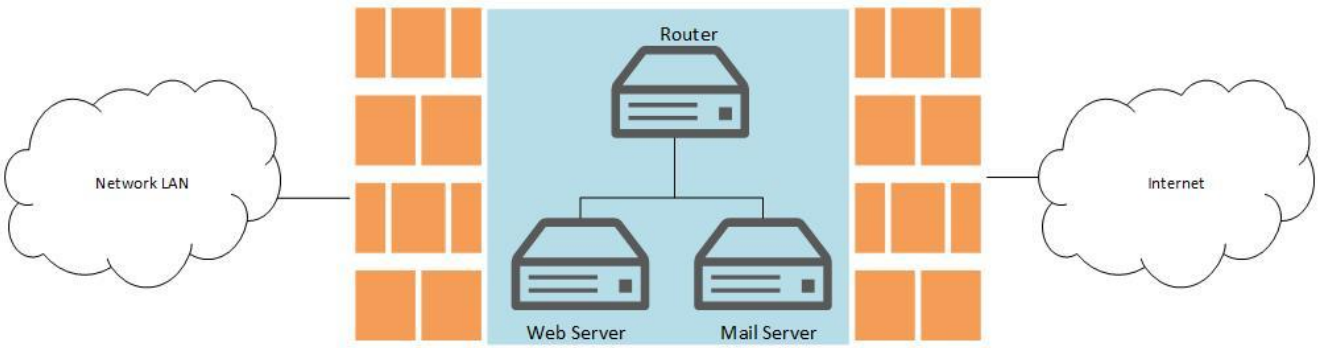

Figure 11 DMZ network architecture (Lutkevich, DMZ in networking)

4 Conclusion

In this chapter the analyse of the result will be presented and an explanation of how this will benefit the company. A theory will also be presented on how to move forward and future improvement on clarification of the standard automation layout.

4.1 Summary

To summarize this thesis, it is good to look at automation in the big picture and analyse how the different communication protocols are interacting. Cyber security is essential to analyse how a system is protected and what countermeasures are being used. It is hard to say that all that has been presented is 100 % accurate in all projects because Wärtsilä is evolving its standard solution constantly and may be changed project-specific wise. The presented result is the general standard Wärtsilä is striving to accomplish, especially Wärtsilä products as the GEMS and WOIS. The Wärtsilä products are constantly being updated and changed, but the core automation itself is built on the same principles.

This documentation will be helpful for the Technical Sales Support for future projects to minimize the time-consuming research when clarification is done to the customer of what Wärtsilä can offer. For customers' information and clarification, this document could be referred to giving some basic knowledge on how the automation system works in a Wärtsilä power plant.

My thesis work has been interesting but also challenging. The work itself has contained interviews with experts and a lot of digging in the Wärtsilä big database for relevant and accurate information. The main challenge has been questioning what part of the automation has a standard solution and what may change project-wise.

4.2 Further improvement

For further improvement, this work could be a good reference document for the automation standard layout improvement. The standard automation layout is currently built in a software called Microsoft Visio where the whole automation system is being built up by symbols and objects. As the automation system is constantly improving, a more detailed layout version could be useful, as well for Wärtsilä personnel as future customers.

4.3 Final Comments

This thesis has given me a lot of knowledge and experience working in the power-generating industry. I think this thesis has been a great introduction to my professional career and has given me a deeper understanding of how a power plant automation work. Cyber security has also been quite new for me and understanding what things should be considered when protecting automation systems. Finally, I want to thank my supervisor Benny Lassus, who has been helping by giving good advice and guidelines for the thesis work.

5 References

Ayllon, N. (2020, 11 11). *WHAT IS THE DIFFERENCE BETWEEN PROFIBUS DP AND PA?* Retrieved from PI: https://us.Profinet.com/what-is-the-difference-between-Profibus-dp-and-pa/

Ayllon, N. (2021, 02 10). *WHAT IS PROFINET? – PROFINET EXPLAINED*. Retrieved from PI: https://us.Profinet.com/Profinet-explained/

Basic understanding of IEC 61850. (2021, 04 30). Retrieved from SGRwin: https://www.sgrwin.com/basic-understanding-iec-61850/

Brash, R. (2021, 07 23). *The Ultimate Guide to Protecting OT Systems with IEC 62443*. Retrieved from Verve: https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/

Company, I. (2013, 03 19). *What is Modbus and how does it work*. Retrieved from Schneiders Electric: https://www.se.com/us/en/faqs/FA168406/

DMZ. (n.d.). Retrieved from FORTINET: https://www.fortinet.com/resources/cyberglossary/what-is-dmz

DMZ Network. (n.d.). Retrieved from Barracuda: https://www.barracuda.com/glossary/dmz-network

Foster, S. (2020, 07 29). *What Is IEC 62443? Overview + Security Level*. Retrieved from PERFORCE: https://www.perforce.com/blog/kw/what-is-iec-62443

Foundation, O. (2022). *Classic*. Retrieved from OPC Foundation: https://opcfoundation.org/about/opc-technologies/opc-classic/

IEC 62443. (n.d.). Retrieved from infineon: https://www.infineon.com/cms/en/product/promopages/iec62443/

IGSS. (n.d.). *Siemens PROFIBUS/MPI S7 Protocol & Siemens Industrial Ethernet S7 protocol ID:8*. Retrieved from igss.schneider-electric: https://igss.schneider-electric.com/plc-scada-driver-8/

INCORPORATED, A. (2005). *Introduction to Modbus TCP/IP.* Retrieved from prosoft-technology: https://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf

Johansen, A. G. (2021, 06 17). *What is a firewall? Firewalls explained and why you need one*. Retrieved from Norton: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

Kondor, R. (n.d.). *What is OPC*. Retrieved from OPC Training Institute: https://www.opcti.com/OPC-Overview.aspx

Lutkevich, B. (2021, 07). *DMZ in networking*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/DMZ

Lutkevich, B. (n.d.). *DMZ in networking.* TechTarget.

Lydon. (2009, 02 07). *IEC 61850 Power Industry Communications Standard*. Retrieved from Automation.com: https://www.automation.com/en-us/articles/2003-1/iec-61850-power-industry-communications-standard

Medoff, M. (2018, 07 12). *IEC 62443: Levels, Levels and More Levels*. Retrieved from exida: https://www.exida.com/Blog/iec-62443-levels-levels-and-more-levels

Organization, M. (n.d.). *Modbus News*. Retrieved from Modbus: https://modbus.org/

organization, P. (2021). *PROFIsafe*. Retrieved from Pi-Profibus-Profinet: https://www.Profibus.com/technology/profisafe

OSI Model. (n.d.). Retrieved from Imperva: https://www.imperva.com/learn/application-security/osi-model/

Packet Filter Firewall and Application Level Gateway. (2021, 11 03). Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/

Procentec. (n.d.). *What is PROFIBUS DP?* Retrieved from PROCENTEC: https://procentec.com/content/what-is-Profibus-dp/

RealPars (Director). (2020). *What is Profibus PA and How Does it Differ from Profibus DP?* [Motion Picture].

Shaw, K. (2022, 3 14). *The OSI model explained and how to easily remember its 7 layers*. Retrieved from Networkworld: https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html

SolUK, M. (Director). (2019). *OPC Server & Client Data Communications – Introduction and Overview (Kepware, KEPServerEX)* [Motion Picture].

Team, E. (2021, 02 26). *Understanding IEC 62443*. Retrieved from International Electrotechnical Commission: https://www.iec.ch/blog/understanding-iec-62443

Technology, P. (Director). (2014). *Understanding Modbus Serial and TCP/IP* [Motion Picture].

Understanding Profibus Network Basics and Diagnostics. (2021, 10 17). Retrieved from Bright Hub Engineering: https://www.brighthubengineering.com/consumer-appliances-electronics/125704-Profibus-protocol-in-plc-and-automation-technology/

WHAT IS A UTM FIREWALL? (n.d.). Retrieved from Firewalls: https://www.firewalls.com/what_is_utm_firewall

What is OPC UA? A practical introduction. (2022). Retrieved from OPC Router: https://www.opc-router.com/what-is-opc-ua/#OPC-Classics-OPC-UA

What is OPC? (2022). Retrieved from OPC FOUNDATION: https://opcfoundation.org/about/what-is-opc/

What is PROFIBUS? (2022). Retrieved from smar Technology Company: https://www.smar.com/en/Profibus