

Atte Suutari

# **WIRELESS COMMUNICATIONS ON AUTOMATED CHARGING SYSTEMS IN MARINE INDUSTRY**

Engineering and Natural Sciences  
Master of Science Thesis  
April 2020

# ABSTRACT

Atte Suutari: Wireless communications on automated charging systems in marine industry  
Master of Science Thesis  
Tampere University  
Automation Engineering  
Examiners: Professor Jose Luis Martinez Lastra and Professor Luis Enrique Gonzalez  
Moctezuma  
April 2020

---

Building fieldbus-based applications with wireless technology is a hot topic in maritime in 2020. Wireless communication provides vessels with freedom but it also creates new kinds of demands. The focus is to resolve the key issues in a wireless fieldbus system on automated shore to ship charging applications and the usage of wireless technologies in maritime in general.

The main goal of this thesis is to build a big picture of the problems and complexity that arise when planning to implement standardized wireless technologies like IEEE 802.11, BT, LTE or IEEE 802.15.4 on shore to ship charging applications. This is studied without forgetting the aspects of cyber security and specific requirements that the industry itself requires to be fulfilled.

In this thesis, a proposal for wireless communication in automated charging system is presented. It includes a single communication protocol and two different redundant wireless technologies. The proposed system was successfully implemented and tested on land. Sea trials were not possible to carry out. The main result of the thesis is that the UHF IP radios are more suitable than Wi-Fi routers for automated charging systems in maritime environment.

Keywords: Automated charging system, maritime, wireless communication, wireless technologies, cybersecurity, Wi-Fi, UHF, classification societies.

The originality of this thesis was checked with the Turnitin OriginalityCheck service.

# TIIVISTELMÄ

Atte Suutari: Langaton kommunikaatio meriteollisuuden automatisoiduissa latausjärjestelmissä

Diplomityö

Tampereen yliopisto

Automaatiotekniikka

Tarkastajat: Professori Jose Luis Martinez Lastra and Professori Luis Enrique Gonzalez

Moctezuma

Huhtikuu 2020

---

Kenttäväyläpohjaisten sovellusten kehittäminen langattomilla tekniikoilla on polttava puheenaihe meriteollisuudessa vuonna 2020. Langattoman kommunikaation tuoma vapaus asettaa kuitenkin uudenlaisia vaatimuksia. Tämän diplomityön painopiste on ratkaista avainkysymyksiä liittyen langattomien tekniikoiden käyttöön olemassa olevien kenttäväylien kanssa alusten automatisoiduissa latausjärjestelmissä ja langattoman tekniikan käyttöön yleisesti meriliikenteessä.

Opinnäytetyön päätavoitteena on luoda kuva ongelmista, joita syntyy, kun suunnitellaan standardoitujen langattomien tekniikoiden kuten IEEE 802.11, BT, LTE tai IEEE 802.15.4 käyttöönottoa sähkölaivojen latausjärjestelmien kommunikaatiossa. Tätä tutkittiin unohtamatta kyberturvallisuuden näkökulmaa ja meriteollisuuden erityisvaatimuksia.

Ehdotus automatisoidun latausjärjestelmän langattomaan viestintään sisältää yhden kenttäväyläprotokollan ja kaksi eri langatonta tekniikkaa toimimaan toistensa varajärjestelminä. Ehdotettu lähestymistapa toteutettiin ja testattiin onnistuneesti maalla. Testausta merellä ei ollut mahdollista toteuttaa. Opinnäytetyön tuloksena on, että UHF IP -radiot soveltuvat parhaiten kyseiseen tehtävään suorituskykynsä ja meriteollisuuden asettamien vaatimusten vuoksi.

Avainsanat: Automaattinen latausjärjestelmä, meriteollisuus, langaton kommunikaatio, kyberturvallisuus, Wi-Fi, UHF, luokituslaitos.

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

# PREFACE

This thesis is my final project before graduating from Tampere University (former Tampere University of Technology). The project was undertaken by the request of ABB Oy and the topic was formulated with my mentor, Tatu Virta. I developed the solution and wrote this thesis from February 2019 to April 2020. Although it has been a huge mountain to climb, at the same time it has been the most profitable project in terms of learning.

To be honest, I wouldn't have reached my current level of success without the support I got. The biggest thanks go to my lovely parents, who believed in me and supported with love and understanding. Next, I want to thank my mentor Tatu Virta and all the other awesome co-workers that I have, Aki Kurri, Timo Lätti, Niklas Peltoniemi and Mika Paukkeri to name a few. A huge thanks to Tomi Tonder for your attention to this thesis. I also want to thank my professors Jose Luis Martinez Lastra and Luis Enrique Gonzalez Moctezuma for teaching and helping me with this thesis. I am grateful for your dedication and work you do at the university. There are no words to thank my fellow students with whom I shared these memorable years. Last but not least, thank you Tampere for taking care of me during my studies.

Espoo, 26th April 2020

A handwritten signature in cursive script that reads "Atte S".

Atte Suutari

# CONTENTS

1. INTRODUCTION .....	1
1.1 Background.....	1
1.2 Problem definition .....	3
1.3 Objectives and structure .....	3
2. THEORY.....	5
2.1 Shore charging.....	5
2.2 Communication protocols.....	7
2.2.1 Profibus DP.....	8
2.2.2 FOUNDATION Fieldbus HSE.....	9
2.2.3 PROFINET.....	10
2.2.4 MODBUS TCP .....	11
2.2.5 Self-defined TCP communication .....	12
2.2.6 Self-defined UDP communication .....	13
2.3 Wireless technologies .....	15
2.3.1 Wi-Fi .....	16
2.3.2 Bluetooth .....	18
2.3.3 Software defined radios .....	20
2.3.4 Satellite link.....	21
2.3.5 LTE.....	22
2.3.6 WiMAX.....	24
2.4 Antennas.....	25
2.5 Environment in the marine industry .....	27
2.6 Classification society and legislation .....	28
2.7 Cyber security.....	29
2.8 State of the art projects .....	32
3. PROPOSAL .....	35
3.1 Problem statement and requirements .....	35
3.2 Structure of the system .....	36
3.3 Communication protocol between the stations .....	38
3.4 Wireless technologies and antennas.....	40
4. IMPLEMENTATION .....	43
4.1 Hardware .....	43
4.2 Developed software with Compact Control Builder AC 800M.....	47
4.3 Configuration of the wireless network devices.....	49
4.4 Test setup.....	52
5. TESTS AND RESULTS .....	55
5.1 Tests.....	55
5.2 Results.....	57
6. CONCLUSIONS.....	61

REFERENCES.....	63
APPENDIX A: MASTER STATION CODE .....	68
Master Station.....	68
Slave Station.....	72

# LIST OF FIGURES

<i>Figure 1: On-shore module is ready to plug the vessel and charge the batteries [8].</i>	6
<i>Figure 2: Diversity of the fieldbuses. MAC protocols [11].</i>	7
<i>Figure 3: Illustration picture of range of omnidirectional antenna[42].</i>	26
<i>Figure 4: Picture of a parabolic antenna. Antenna in picture is one grade of too huge for regular Wi-Fi access point [44].</i>	27
<i>Figure 5: Finferries' Remote control station on Turku, Finland. Picture by Niclas Lundqvist and Yle [57].</i>	33
<i>Figure 6: Design of Yara Birkeland [62].</i>	34
<i>Figure 7: Structure of the system.</i>	37
<i>Figure 8: Proposal of TCP/IP communication between stations.</i>	39
<i>Figure 9: Example communication between stations represented in a sequence diagram.</i>	40
<i>Figure 10: The technologies as function of the evaluated aspects.</i>	41
<i>Figure 11: Components: CI867 (UHF) [A], CI867 (Wi-Fi) [B], PM861 [C] and 10A power supply [D].</i>	44
<i>Figure 12: UHF IP Radio manufactured by Satel. The antenna showing is not the one used in tests.</i>	45
<i>Figure 13: Industrial Wi-Fi router by Phoenix Contact. It has very compact size if you don't count the antenna.</i>	46
<i>Figure 14: Fully equipped station ready to be transported to the test area.</i>	47
<i>Figure 15: Use cases of the implemented stations.</i>	48
<i>Figure 16: Web browser interface for Satel IP radio.</i>	50
<i>Figure 17: Centralized network configuration application, NETCO by Satel.</i>	51
<i>Figure 18: Web browser interface to configurate the FL WLAN 5100 router.</i>	51
<i>Figure 19: Master station on test bench wrapped to a homemade weather protection with long power cord and two Ethernet cables.</i>	53
<i>Figure 20: Test equipment: earth leakage circuit breaker and switch with a mirror port.</i>	54
<i>Figure 21: Pinging the slave station with Windows command prompt.</i>	56
<i>Figure 22: RSSI as function of distance.</i>	58
<i>Figure 23: Time on air as function of distance.</i>	59

# LIST OF TABLES

<i>Table 1: Structure of data by OSI model.</i>	14
<i>Table 2: Structure of IP Packet [21].</i>	15
<i>Table 3: Structure of UDP packet [19].</i>	15
<i>Table 4: Wi-Fi technologies are based on the IEEE Standards according to the table [22,25].</i>	17
<i>Table 5: IP addresses of the system.</i>	49
<i>Table 6: Summarized features of the solution.</i>	60
<i>Table 7: Parameters of the master station.</i>	68
<i>Table 8: Variables of the master station.</i>	68
<i>Table 9: Used Function blocks in the application of master station.</i>	69
<i>Table 10: Parameters of the slave station.</i>	72
<i>Table 11: Variables of the slave stations.</i>	72

# LIST OF SYMBOLS AND ABBREVIATIONS

ACS	Automatic Charging System.
AFH	Adaptive frequency-hopping spread spectrum.
Bluetooth SIG	Bluetooth Special Interest Group.
CDF	Cumulative Distribution Function of a real valued variable for example X is the probability that X will take a value less than or equal to x.
C-Plane	Control Plane latency is measured as the time required for the UE to transit from idle state to active state.
DSC	Digital Selective Calling is a standard for predefined messages used on maritime.
D2D	Device to device.
EUTRAN	EUTRAN is a protocol stack that includes following layers: Physical, MAC, RLC, PDCP, RRC, and the interfacing layers: NAS and IP.
FDD	Frequency Division Duplex is a method that makes the transmitter and receiver operate on different frequencies.
FEC	Forward Error Correction.
GFSK	Gaussian Frequency Shift Keying.
GOOSE	Generic Object Oriented Substation Event is protocol for sending and receiving signals.
GSD	General Station Description.
IEC	International Electrotechnical Commission is an international standards organization.
ISM	The industrial, scientific and medical (ISM) radio bands. Wi-Fi and Bluetooth uses them for example.
IEEE	Institute of Electrical and Electronics Engineers is professional association for technology industry standards.
IEEE 802	Set of Local Area Network protocols.
IoT	Internet of Things.
IP	Internet Protocol, the principal communication protocol in the Internet.
ITU-R	International Telecommunication Union Radiocommunication Sector.
EAP	Extensible Authentication Protocol is WPA-improvement.
EDR	Enhanced data rates.
LLDP	Link Layer Discovery Protocol is an open and extendable protocol to advertise a device's identity and abilities on LAN.
LOS	Line Of Sight.
MAC	Medium Access Control sublayer is the layer that controls the hardware responsible for interaction.
MBP	Manchester Bus Power is media where data and power are transferred via same cable.
MIMO	Multiple Input, Multiple Output.
MME	Mobility Management Entity is the control-node for the LTE access-network.
MMS	Manufacturing Message Specification is an international standard for transferring data and control information in real-time.
MTU	Maximum Transfer Unit.
NAS	Non Access Stratum protocol performs authentication and security control between UE and MME.
OPEX	Operating Expenses are the costs of developing or providing non-consumable parts for the systems.

OFDM	Orthogonal Frequency Division Multiplexing is a method of encoding digital data on multiple carrier frequencies.
OSI model	Open Systems Interconnection model standardizes the communication functions of a system without regard to its underlying structure or technology.
PAN	Personal Area Network.
PDCP	Packet Data Convergence Protocol provides services to the RRC and upper user plane layers.
piconet	An ad hoc network that links a wireless user group of devices with Bluetooth.
RLC	Radio Link Control is a layer used in UMTS and LTE interfaces.
RNRP	Redundant Network Routing Protocol enables two physically separate networks.
RRC	Radio Resource Control protocol is used in UMTS and LTE interfaces.
RSSI	Received Signal Strength Indicator is a measurement of the power present in a received radio signal.
RTLS	Real-time locating systems are used to automatically identify and track the location of objects or people in real time.
SAM	Slot Availability Masking.
SAS	Substation Automation System.
SCD	Substation Configuration Description it's a file format that contains the configuration of IEC 61850 substation devices.
SDO	Standards Development Organizations is standardization organization in the telecommunications industry including equipment producers and network operators.
SDR	Software Defined Radio.
SIL	Safety integrity level is a measurement of performance required for safety by IEC 61508.
SMV	Sampled Measured Values.
SNMP	Simple Network Management Protocol is application layer protocol to manage and monitor network elements.
SSID	Service Set Identifier which announce the presence of a network.
TCP	Transmission Control Protocol is one of the main protocols of the Internet protocol suite.
TDD	Time Division Duplex is a method to separate outward and return signals. It emulates full duplex communication over a half duplex communication link.
UE	User Equipment.
UDP	User Datagram Protocol is an alternative communications protocol to TCP.
U-Plane	User Plane latency is defined as one-way transmit time between a packet being available at the IP layer in the UE/EUTRAN edge node and the availability of this packet at the IP layer in the EUTRAN/UE node.
vishing	Voice phishing.
WAP	Network hardware device which allows Wi-Fi devices connect to a wired network.
WEP	Wired Equivalent Privacy is a security algorithm for IEEE 802.11 family.
WIPS	Wireless intrusion prevention system is a device that monitor the selected radio spectrum for unauthorized access to WLAN.
Wi-Fi	Technology for wireless local area networking via radio bandwidth.
Wi-Fi Alliance	A non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products.

Wi-Fi Direct	Wi-Fi standard is making possible devices to connect with each other without WAP.
WLAN	Wireless local area network.
WPA	Security protocol and certification that Wi-Fi Alliance created to secure wireless computer networks.
WWW	World Wide Web is an information system that can be read with web browser.
XML	Extensible Markup Language is file extension that shares the data and common information format on the World Wide Web. Similarities to HTML.

# 1. INTRODUCTION

## 1.1 Background

The successful use and massive popularity of wireless technologies in consumer applications have made the standardized wireless technologies a considerable and plausible technology for marine industry. At the same time International Maritime Organization (IMO) have set a 50% reduction in total annual greenhouse gases compared to the levels of 2008 [1]. Narve Mjøs, director of battery services and projects at DNV GL, states that: "Batteries are a prime enabler for reducing fuel consumption and costs, maintenance, and air emissions. What is more, electric power minimizes noise and vibrations and enhances vessel responsiveness and safety." The marine industry has interest in the development of electric vessels. 2010 there was 0 battery-powered vessels operating. Now 2020 Mjøs states that there are little less than 400 vessels operating or under construction. [2] These battery-powered vessels also need new infrastructure and technologies to charge the batteries effectively for example with automated charging systems (ACS).

The opportunity to save in cabling costs and attach wireless applications to an existing system is very attractive. Automation industry however has very strict performance requirements for fieldbuses. In professional aspect the bitrate is not the only quantity that the user wants to compare between protocols. Reliability and timing are the key factors in any industrial environment. When the communication between actuators, sensors and digital controllers are implemented in wired environment with present fieldbuses, the requirements for the reliability and the timing are well fulfilled. Whereas communication is built over wireless links, the unfavourable properties of the radio channels affects significantly to the ability to meet the requirements of reliability and timing. The creation of hybrid systems, like the modernization projects of vessels and ports, in which existing systems are linked wirelessly to a new subsystem, brings the project team to a situation where the amount of potential solutions is enormous. However, it is not just engineering companies that are solving fundamental problems of channel errors or the compatibility between the existing and the new systems or the most suitable wireless technology, there are also the classification society's rules on top of the international maritime legislation. [3,4]

The use of wireless links in the marine industry or in a factory floor setting grants diverse benefits. Already in the very beginning the costs and time needed for the installation of large number of cables are decreased. The industrial environment, for example a vessel, can be designed to be much more compact and thus much simpler. The simplicity eases future modernization projects because of the improved reconfigurability of a vessel's communication system. The benefits of wireless links come forth especially in harsh environments where chemicals, vibrations or physical stress are involved. The cabling can be potentially damaged even with appropriate support. In terms of flexibility, stationary systems, for example a charging station on a port, can be wirelessly connected to any already existing automation systems that could not be possible with through media. Along with the simplification of communication between subsystems, many commercial implementations exist that benefits of the possibilities of wireless technologies, for example autonomous vessels, robots and localization of IoT.

These industrial applications are widely implemented with wired protocols such as Profibus, Profinet or MODBUS. The interconnections of process automation and control automation applications are specially solved with fieldbuses. Fieldbus' mission is to create a real-time communication that is reliable and predictable. These systems basically guarantee a delivery of packets in predefined delivery time. In the thesis, one protocol will be chosen for wireless communication between the PLCs by its' compatibility. [4,5]

There are great range of different kind of solutions of wireless technologies, from datacentric solutions such as Wireless Local Area Networks (WLANs) and Wireless Personal Area Networks (WPANs), to voice oriented cellular network like Universal Mobile Telecommunications System (UMTS). WLANs are capable to transmit tens of megabits over range of couple of hundred meters for example the IEEE 802.11 technology [6]. However, WPAN is designed for low power consumption applications such as wireless connectivity between smart phones. [3] The most famous WPAN system is Bluetooth. Bluetooth's data rates are lower compared to IEEE 802.11 and the range is only up to few meters [7]. The pros of wireless solutions have been the reason of bringing vendors worldwide to offer devices compliant to these above mentioned standards also for industrial use. The latest solutions have made the battery driven vessels very interesting and prospective solutions for greener maritime. It wasn't possible earlier to meet the performance requirements with battery driven vessels, but now with automated charging systems and wireless communication technologies the table has turned.

## 1.2 Problem definition

Building fieldbus-based application with wireless technology is not a simple challenge. Since there are possible transmission errors in a wireless channel followed by either channel outages or interference. Outages occur when the receiving signal strength drops below a certain level. The requirements of real-time and reliability are probably jeopardized which would not be the case with wired system. Wireless communication sets new kinds of requirements for the classification society and cyber security. Focus of this paper is to resolve these key issues in a wireless fieldbus system on automated shore to ship charging application and the usage of wireless technologies in maritime in general.

## 1.3 Objectives and structure

The goal of this thesis is to build a big picture of problems and complexity that arise when planning to implement standardized wireless technologies like IEEE 802.11, BT, LTE or IEEE 802.15.4 on shore to ship charging application. Also, the purpose is to research and find the answers to following questions:

- Which is the most robust combination of existing wireless technology and communication protocol on shore to ship charging application?
- How marine industry effects on the requirements of the implementation of wireless communication?
- What aspects need to be considered in cyber security?

This thesis leaves out of the scope the electrical charging system itself. Neither the side of the vessel or the equipment on shore of the automated charging system are explained with detail. The basic principle is explained. The interface between the communication and the system is also left out of the research. The scope is to answer to the questions above and verify the most robust wireless communication technology between two ABB's 800m PLCs with the requirements of the industry.

The discussion of this matter in this thesis has the following structure. Second chapter introduces the widely used wireless technologies and the communication protocols of interest for use in industrial marine environment. Given that marine industry has its own special characteristics to be taken in care compared to standard factory floor level, *Chapter 2* also discusses how the legislation and the cyber security sets few extra

requirements for the wireless systems. *Chapter 3* presents an approach how to build the wireless communication and achieve the goals described in this chapter. The implementation of the proposed equipment is presented in *Chapter 4*. In *Chapter 5*, test cases and the results are shown. Conclusions are provided in *Chapter 6*.

## 2. THEORY

The main focus of this chapter is on protocols to establish the communications between the programmable logic controllers. The only restriction for the protocols is that they need to be supported by ABB's 800M logic controllers. Other main subjects of this review of literature are the wireless technologies and cyber security of wireless communications in marine applications. Also, the thesis outlines the regulations and legislation of marine industry. In the end of this chapter author represents few state-of-the-art projects and the technologies used in them.

### 2.1 Shore charging

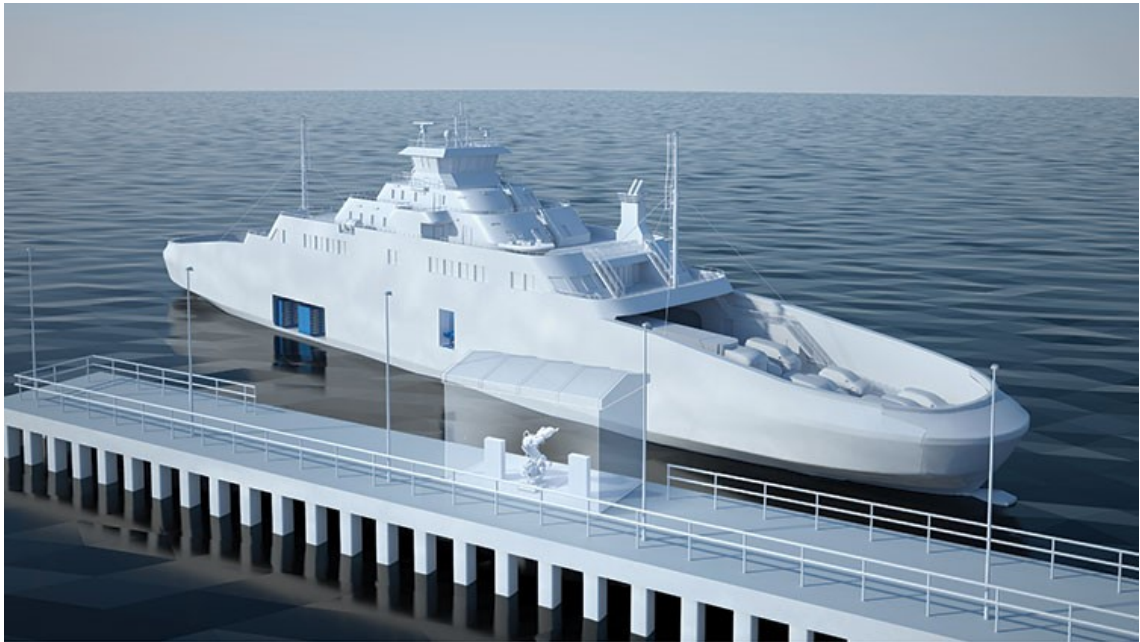
Shore side power utility infrastructure for vessel battery charging is an ideal solution for next generation electric and hybrid ships, but several crucial factors must be taken in consideration. The time next generation vessels spend at a dock can be less than 15 minutes, which is a huge challenge for charging technology. Following main aspects should be taken consideration when planning the shore charging system:

- Automatic or manual charging connection.
- Availability of power on shore.
- Transfer technology, AC or DC.
- Harsh environment.
- What are the voltage levels?
- Legislation and standards.

All these needs to be taken in care with aspects as high reliability and simple maintain program to maximize uptimes and minimize operating expenses (OPEX).

The Automatic Charging System (ACS) consists of an onshore module and an onboard module. Communication between the shore and onboard modules is maintained via wireless link to ensure safe way of operation. On approach, the system detects proximity of the dock and automatically the onshore module gets ready. The on-shore module continuously aligns the connector when the vessel is almost docked. The alignment is a difficult task even with specified cameras and sensors, because of the seafaring. Once the vessel has docked the on-shore module with a robot arm inserts a connector to the

on-board module and establishes the electrical contact. The current is ramped up and the status is monitored on the bridge of a vessel. Below there is a *Figure 1* of the on-shore module and a vessel with on-board module just before connection.



**Figure 1:** On-shore module is ready to plug the vessel and charge the batteries [8].

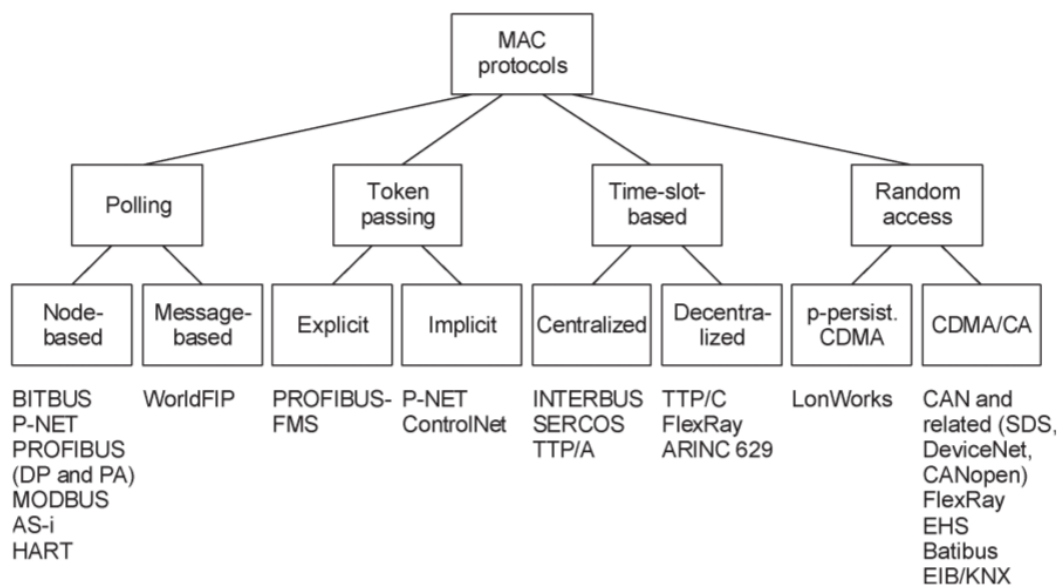
Compared to traditional method to use a physical connection for the communication, which needs to be aligned as the charging connection. Wireless communication decreases the failure rate and reduces the need of maintenance and replacements [9]. However, the security and the lower costs are not the main reason why wireless connection is needed. The short port call makes it almost impossible for the charging system without slight anticipation which wireless communication enables. The port can put the right dock with the right on-shore module on standby. As well, the vessel can have information about the docking from the port. Also, the Garcia and Co. states that wireless technology is also approved method also in safety applications and often implemented on land system in *Design and Development of a Wireless Emergency Start and Stop System for Robots* [10]. Off-the-shelf and certified wireless safety switch products are available.

In this study author focuses only applications with automatic charging connection and the wireless communication between its' components. The transfer technology and voltage levels are irrelevant criteria in this study, and these topics are so wide so these could be researched in other master's theses. Research of the different wireless technology, for example Bluetooth or Wi-Fi, is be conducted in the next chapters to

ensure that the technology is available. On other hand, it does not require high-end and unreachable technology, but still designed for robustness and redundancy. All in all, the requirements are set by vessel by vessel, but the automatic connection and the wireless communication has lot of similarities in specifications in every on shore to ship charging applications.

## 2.2 Communication protocols

Since the 1980s many fieldbus systems have been born, which are tailored to different application fields, and all the companies in the business developed their own fieldbus. The diversity of these approaches is huge and that can be seen on the *Figure 2* on. To ensure the fulfilment of the real-time requirements, companies have been inventive to solve the dilemma of concurrent access to shared resources. Medium Access Control (MAC) layer is not only part of a fieldbus protocol. Other aspects that are needed to be taken care are for example network management and the method to exchange of the two data classes, process and management data. These aspects made the engineers back in the 80s to develop their own buses for every different application.



**Figure 2:** Diversity of the fieldbuses. MAC protocols [11].

In this subchapter we are focusing on the protocols that are compatible with the ABB's 800M controllers and still have components available. The endless selection needed to be cut short and in the end following communication protocols were chosen: Fieldbuses

MODBUS TCP, FOUNDATION Fieldbus HSE, PROFIBUS DP and PROFINET IO and EtherNet/IP. All above-mentioned fieldbuses use their own communication interface components that enables the connection to a network. External devices and user-defined protocols communicate through Ethernet with User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) communication. For example, TCP/IP allows data blocks to be exchanged between devices. TCP is also international standard that is the backbone of the World Wide Web (WWW). Internet Protocol (IP) puts the messages on the right path and the TCP ensures that the received data is correct. However, the TCP/IP doesn't interpret the data. This job is to be done with the application protocol like for example MODBUS TCP.

### **2.2.1 Profibus DP**

The PROFIBUS DP (Decentralized Peripheral) is a well-known, standardized and widely used fieldbus. The European standard EN 50 170 defines PROFIBUS fieldbus. It is designed for communication between actuators in systems in production automation. PROFIBUS is not bound to any vendor and it's a fully open fieldbus, IEC 61158 defines the fieldbus to be compatible with other vendors[12]. It is possible to link devices from different vendors with PROFIBUS. For example, centralized automation where are controllers, which use a serial connection for communication with field devices, for example with motors, valves and I/Os. Data exchange between distributed automation devices is cyclic. PROFIBUS is suitable for real time applications as for complex systems. PROFIBUS DP supports following medias [13]:

- RS-485, twisted pair, transmission for universal applications.
- Optical fibers which grants greater transferring distances.
- Manchester Bus Power (MBP) is suitable in cases which has hazardous environment.

PROFIBUS device need to be set with specific parameters, which are necessary for device configuration. These parameters are saved in a file called General Station Description (GSD) file. The format of GSD fil is stated in European standard EN 50170 and is based on Extensible Markup Language (XML). The file includes following kind of information: the firmware version, the timing parameter, the baudrate and the length of I/O list. An automatic PROFIBUS master configuration takes care of the registration of different devices from different manufacturers. When communication is established, the

master will start request and send data to the slaves. Advantages of PROFIBUS DP [13] :

- Supports wide range of I/O units.
- Master and slave redundancy.
- Multiple masters are possible.
- Changes online.
- The fastest possible cycle time is around 1 ms.

Even with countless of advantages there are few limitations to be taken in concern when choosing the protocol for shore charging. Limitations of PROFIBUS DP listed below:

- Transfer rate up to 12 Mbit/s.
- The segment can only include 32 nodes.
- The maximum cable length is from 100m to 1200m which depends on the transmission speed. Even though it's enough for shore charging application.

PROFIBUS PA (Process Automation) is another version of PROFIBUS DP and is designed to replace older and conventional solutions like for example buses with 4-20 mA in process automation. PROFIBUS PA can deliver also power supply over the same cable as the data is transferred. It is also operational in very hazardous areas, there is even explosion proof option available for the fieldbus. All in all, PROFIBUS DP and PA work identically and can be operated the same way. [12,13]

## **2.2.2 FOUNDATION Fieldbus HSE**

FOUNDATION Fieldbus High Speed Ethernet (FF HSE) is a two way protocol used for communication of automation control systems. It is one of the first fieldbuses that supports Ethernet and dynamic host configuration. Like other Ethernet-based fieldbuses, the use of switched networks is a required and redundant systems can be built. It is a fieldbus used in a distributed automation system with distributed I/Os. Also, FF HSE fulfils the regulations and requirements for safety in dangerous and hazardous environments. The FF HSE devices are compatible with devices produced by other vendors because the protocol is open. There are two communication profiles for the FF HSE: H1 and HSE profiles. The H1 is capable transmission rate of 31,25 kb/ss and it is recommended to use with direct communication between field de vices. The second,

HSE profile got transmission rate of 100 Mb/s. HSE is in cases where speed is demanded and these subnets can be built with standard Ethernet cables. [13]

The advantages of FOUNDATION Fieldbus HSE are following:

- Possibility for redundant system with 800M.
- The control can be built in the used devices, reducing the need of controllers.
- Online upgrades are possible without a abort of a process, which makes maintenance faster and easier when working with the vessels.

The limitations of the protocol are listed here:

- Maximum 150 devices with H1 profile.
- The maximum amount of linking devices is 30.
- There is possibility to define 3000 channels but only 1000 of them can be used at the time.

FOUNDATION Fieldbus High Speed Ethernet supports function block scheduling that enables control and measurement features to be implemented same way regardless of a manufacturer of an FF HSE device. Benefits of the protocol is the self-testing and reduced downtime and improved safety with communication between devices based on microprocessors. The fieldbus is possible to be connected to the 800M controller with ABB's communication interface module CI860. The configuration of FF HSE subnets needs the own Fieldbus Builder FOUNDATION Fieldbus (FBB FF) to build the system. [13]

### **2.2.3 PROFINET**

PROFINET is an open fieldbus, as PROFIBUS DP standard. It is used used in manufacturing industry and in process automation. PROFINET protocol is an international standard which is based on IEC 61158 and IEC 61784 [14]. PROFINET IO and PROFINET CBA are the two types of PROFINET protocols. The first mentioned is Ethernet integration of distributed I/O and real time applications. PROFINET CBA (Component Based Automation) focuses on distributed automation systems. PROFINET IO is based on IEEE 802.3 [15]. It has variety of performance levels. PROFINET IO uses Ethernet as a base for communications and it's compatible with other IP-protocols.

The advantages of PROFINET IO are listed under:

- Maximum of 100 Mb/s with automated negotiation and automated crossover in a switched network.
- Supports devices regardless vendor. It exchanges data in a predefined arrangement, allowing replacement of devices from a vendor to a another without actions required from the user [16].
- Is capable to offer redundant build.
- PROFINET can use protocols such as Simple Network Management Protocol (SNMP), Link Layer Discovery Protocol (LLDP). [16]
- Online updates.
- The fastest cycle is theoretically 1 ms.

The protocol has very similar advantages and limitations as PROFIBUS DP. Parameters of the PROFINET IO devices are described in the GSD-file. When configuring the PROFINET IO devices, it is as similar as PROFIBUS. During configuration, the distributed field devices are assigned to a specific controller. PROFINET IO is also possible candidate protocol to be implemented on the hands-on phase with ABB's 800M controllers because there is good availability of ABB's own PROFINET IO modules and the protocol's diagnostics tools makes the network management more reliable. [13]

## 2.2.4 MODBUS TCP

MODBUS is a widely used and also open communication protocol. The protocol is a request response based and deploys services by specified function codes. MODBUS TCP is an messaging protocol in application layer, that is the 7th level of the Open Systems Interconnection (OSI) model. So, MODBUS TCP combines a physical network, Ethernet, with TCP/IP networking standard and represents the data. In simple way, the MODBUS TCP message is a MODBUS communication forced to Ethernet TCP/IP wrapper, where MODBUS TCP transforms a regular MODBUS frame into the frame of TCP. However, the end result lacks the MODBUS checksum. It is no needed, because of the TCP.

ABB's 800M controller implements master and slave functionalities of MODBUS TCP. Programming relays strongly to function block (FB) of standard IEC 61131-3 [17]. The master station executes function blocks like *connect*, *read* and *write*. ABB's communication interface module that supports MODBUS communication is called CI867

and it supports Ethernet cable with RJ45 connectors. Here is listed the advantages and limitations of MODBUS TCP [13]:

- Master redundancy.
- Multiple individual masters are supported as well.
- Slave redundancy by switching IP addresses.
- Online updates are supported.

Limitations of MODBUS TCP [13]:

- The ethernet ports 1 and 2 must be connected on two different subnets.
- The second ethernet channel (port) does not support cable break detection feature and supports only speed of 10 Mb/s.
- The maximum size of a message for write is 1968 bits and for read is 2000 bits.
- There are limitations for amount of function blocks:
  - The maximum amount of function blocks for slaves is 1120.
  - The maximum amount of function blocks per slave can go over 60.

All in all, MODBUS TCP accessible to whoever, and it's highly supported by automation device vendors cross the globe. It is also easy to approach and widely used to built communication in industrial applications. Because MODBUS TCP uses the same physical and data link layers as Ethernet, it's fully compatible to be installed into an existing Ethernet network. [13]

### **2.2.5 Self-defined TCP communication**

TCP is connection-oriented in a way that it needs to establish a connection first, form of a handshake. TCP protocol uses name segments for data units. TCP entities exchange data sending segments, which consist of a fixed size of 20 bytes header followed by a variable size data field. TCP communication breaks down a stream of bytes into segments and reconnects them after receiving. Retransmitting segments is possible but it increases the latency. The segment size is limited by Maximum Transfer Unit (MTU) that is defined in the link layer. For example, through Ethernet it is possible to transfer MTU size of 1500 bytes. ABB's 800M controller can communication with external devices through Ethernet with TCP. Typical use cases are for example [18]:

- Use cases in public infrastructure network nodes e.g. traffic lights.

- Sensors and machine vision.
- The controller can operate as a client and as a server on the network. SCADA application are fine examples of collecting data from a server.

Limitations of TCP are listed below [13]:

- There is a limit of maximum ten TCP connections can be made with one controller.
- Fragmented Ethernet packets are not supported with ABB's 800M controllers.
- The TCP protocol defines the ports that are available. Some of the ports cannot be used because they are used by other functions. MODBUS TCP for example uses always port 502.
- Is advised that TCP communication between server and client needs to be restarted after a blackout.
- After a cold start both server and client have to be reinitiated. In the new connection the client cannot contact the server because the server is not yet enabled. It takes at least one scan round for the server to get up before the client side can reconnect.

Because headers of IP and UDP packets are all together 28 bytes, TCP packet is kind a UDP but it includes more information in TCP section. TCP header is larger with its' 20 bytes than UDP packet of 8 bytes.

## **2.2.6 Self-defined UDP communication**

User Datagram Protocol is a protocol that is message-oriented and used in the transport layer. Even though UDP provides integrity verification of the header and payload with the checksum, it provides no guarantees to the upper layers for data units have been delivered and the UDP layer doesn't retain state of UDP messages after sending. UDP can also be misspelled as Unreliable Datagram Protocol because of no verification of delivery. If reliable transmission is wanted, it must be implemented in application. Also, The UDP communication protocol doesn't ensure that the data was delivered to the correct receiver. [19] With ABB's 800M the UDP Communication with Ethernet is used for communication to external devices. The use cases are mostly the same as TCP communication has for example like the semaphores. Limitations of the protocol listed below [13]:

- Maximum of 10 different UDP connections can be formed with a controller.
- ABB's 800M controller does not support fragmented Ethernet packets.
- UDP traffic also might get lower priority than TCP on some network equipment when the network is fully loaded.

Packets are structured with the principles of OSI model. TCP and UDP packets are presented with following layers:

- Data link layer: Physical addresses, the destination and the source MAC addresses.
- Internet layer: Header and addresses (IPv4 or IPv6).
- Transport Layer: TCP or UDP data and related header.
- Application Layer: The actual sent data by user.

Structure of data is presented in following tables. Data link layer goes first and in the end there is footer frame. There is a IP packet data between the frame data and the footer. Internet layer data is first in IP packet, then the transport layer and in the end is the user data. [19,20]

**Table 1: Structure of data by OSI model.**

Data Link Layer			
Frame header (8bytes)	Frame data (14 bytes)	IP + UDP packet (Table 2)	Cyclic redundancy check (CRC) i.e. Footer frame

The IP and UDP packets are unpacked to the *Table 2* which can be found under.

**Table 2: Structure of IP Packet [21].**

IP Packet						
bits	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source Address					
128	Destination Address					
160->	Data (UDP Packet)					

Decompression of the UDP packet is represented under in *Table 3*.

**Table 3: Structure of UDP packet [19].**

UDP Packet				
bits	0-7	8-15	16-23	24-31
0	Source port		Destination port	
32	Length		Checksum	
64->	User data			

UDP is a connectionless transmission model without handshaking dialogue for providing reliability and integrity. Thus, packets can arrive out of order or even got lost. However, the checksum increases data integrity. Applications, which need low latency, usually use UDP, because dropping packets is more preferable than keep waiting for the delayed packet. Also, packet overhead is smaller with UDP so it's faster to deliver and doesn't reserve that much bandwidth. [19,20]

## 2.3 Wireless technologies

In this chapter there are introduced six wireless technologies. All of them are possible solutions for ASC in marine applications. All of chosen technologies to this thesis are very different and in the first place these have been designed for specific applications in mind. But after many updates and improvements it is good to do research about characteristics and performance of today.

### 2.3.1 Wi-Fi

Wi-Fi is Wireless Local Area Network (WLAN) technology that is based on the IEEE 802.11 standard. Wi-Fi the trademark is administrated by Wi-Fi Alliance. The non-profit organization restricts the use of the logo and the name Wi-Fi for devices that passes the strict testing according to the certification. [7]

Devices which are for example using Wi-Fi technology: PCs, consoles, smartphones, printers, cars and drones. The connection to the Internet is established via a WLAN and wireless access points. There are few versions of Wi-Fi which use different radio bands and bandwidths that effects for example to baud rates and effective range. Wi-Fi standards mostly use the 2,4 GHz and 5 GHz radiobands. The new standard IEEE 802.11ax can also be set on the 6 GHz. The bands can be divided into multiple different channels. It is possible to share the same channel with different networks by specific time stamps. There are lot of materials that absorb or reflect these radio waves, which restricts range, but this phenomenon is not just a negative thing. Absorption can help to minimise interference between different networks in busy environments. So, the wavelengths work the most efficiently with line-of-sight (LOS), but on the other hand it makes it easy to set different WLANs on specific sections of the area wanted to be covered. It also makes it harder for the intruders to get into the WLAN without being physically near the access point. [7,22]

Wired Ethernet networks are more secure against for example eavesdropping than Wi-Fi. Anybody inside the range of wireless network and with a wireless network interface controller can try to receive an access. Wi-Fi Protected Access (WPA) is a technology created to protect the communications via WLAN with Wi-Fi standard. The newest standard for Wi-Fi security is WPA3. WPA3 has for example Simultaneous Authentication of Equals (SAE) feature which is a method that use a secure password-based authentication and a password-authenticated key agreement. WPA3 will mitigate security risks that appears because of weak passwords and simplify the process of setting up devices with interface without display. [23]

The Institute of Electrical and Electronics Engineers (IEEE) doesn't perform tests for devices to fulfil their standards. The non-profit Wi-Fi Alliance was formed to execute this mission and enforce the IEEE standards in 1999. The mission is to increase interoperability, backward compatibility and use of WLAN technology [24]. Manufacturers whose products have passed the process of Wi-Fi Alliance can use the Wi-Fi logo on their products [24]. Devices without Wi-Fi certification can still be compatible with other devices that are certified.

Equipment with Wi-Fi certification usually supports multiple versions of Wi-Fi. The versions differ from the radio wavebands, the radio bandwidth, the maximum data rates and modulations.[25] Thumb of rule is that lower frequencies have better range but data rates are lower. *Table 4* under shows the differences of the versions.

**Table 4:** *Wi-Fi technologies are based on the IEEE Standards according to the table [22,25].*

IEEE Standard	Data rate (Mbps)	Frequency (GHz)	Modulation	Date of release
802.11a	54	5	OFDM	Sep 1999
802.11b	11	2,4	DSSS	Sep 1999
802.11g	54	2,4	OFDM	Jun 2003
802.11n	150	2,4/5	MIMO-OFDM	Oct 2009
802.11ac	867	5	MIMO-OFDM	Dec 2012
802.11ax	11000	2,4/5/6	OFDMA	Jul 2019

Wi-Fi Alliance has standardised numbering of the different standards of IEEE 802.11 so that equipment can be recognized faster and more easily which versions it supports. For example the Wi-Fi 4 stands for supports 802.11 and the latest implementation of the IEEE's standard is called Wi-Fi 6 (802.11ax). [25]

Mobile routers which are battery-powered can have both a 3G/4G modem and Wi-Fi access point. After subscription to a mobile network, it is possible for Wi-Fi devices within range to access Internet for example over LTE tethering technology. [26] This kind of technology is supported by all the most common smartphones in the market for example Android, iOS, Windows Phone, BlackBerry and Symbian. Also, most modern laptops can act as a WLAN access point.

Wi-Fi makes also possible to communicate directly from a device to a device without an external access point. This technology is called wireless ad hoc network and the Wi-Fi Alliance has standardized it as Wi-Fi Direct. Wi-Fi Direct was launched on October 2010. [27]. It is comparable to Bluetooth, which is handled more closely in the next chapter.

Compared to mobile phones the Wi-Fi transmitters are working with lower power consumption. ETSI is limiting the maximum output power that a Wi-Fi device is allowed to transmit. In the European Union (EU) the limit is 20 dBm and as converted it's 100 mW when operating with a frequency of 2,4 GHz, and the 5 GHz band is subdivided into two different bands of 5150 - 5350 MHz and 5470 - 5725 MHz, both band can have different power limits, but those limits are between 200 - 1000 mW. [28] A Wi-Fi access

point with the stock omnidirectional antenna is capable of range more than 100 meters within legal output power. [29]

Propagation of the radio signals with frequencies where Wi-Fi works is one of the most important matters for the range of Wi-Fi. Wi-Fi signals works best with line-of-sight (LOS), but signals are affected by absorption, reflection, and diffraction (wave encounters an obstacle or a slit and bends) through and around structures. This phenomenon does not apply fully to applications with long range and implemented with Wi-Fi, because these kinds of applications usually operate above the surrounding obstacles. The absorption and reflections are the reasons why Wi-Fi is not suitable for mobile devices over wider ranges. For example, a vehicle moving fast from access point to another access point. [27]

The communication through Wi-Fi devices can be disrupted with other devices in the same area. When there is a lot of access points in the same area, the phenomena is called Wi-Fi-polution. It is acceptable to use Wi-Fi bands with low transmitting power without a license. However, there have been cases where knowingly caused interference to restricted bands have been issued fines in Finland [30]. In the worst case scenario, Wi-Fi-pollution can even block the access to the network. On highly populous areas this can be a problem. These issues can become a problem in highly crowded areas. For example, in a vessel with ACS and public WLAN for the passengers. [29]

### 2.3.2 Bluetooth

Bluetooth is a wireless technology protocol for exchanging data in Device to Device (D2D) scenarios. The technology uses same frequencies as Wi-Fi and it is used for very short distances. Bluetooth is *de facto* technology for Wireless Personal Area Networks (WPAN).[31] IEEE refers to Bluetooth with IEEE 802.15.1 code. Nowadays the standard is managed by the Bluetooth Special Interest Group (SIG). Bluetooth devices used frequencies from 2,400 GHz to 2,485 GHz. Manufacturers have to pass the standardized process of SIG to produce devices with Bluetooth stamp to the consumers. [32] Use cases of Bluetooth are vast:

- Wireless control between a smartphone and phone accessories.
- Communications between nodes in a building automation.
- Medical equipment.

- Replace outdated communication technologies in field devices for example infrared and RS-232 standards.
- Wireless communication between two industrial Ethernet networks for example PROFINET.
- Tracking location in real time, Real-time location systems (RTLS).
- Wireless connection of motion controllers to a PC when playing VR headsets.

Bluetooth standard is evolving all the time like Wi-Fi so there are always lots of devices which doesn't support the newest versions and features coming with them, but Bluetooth is fully backward compatible and fully supports all its' previous versions. The most recent iteration of Bluetooth (Bluetooth 5) is designed for the Internet of Things (IoT). The newest implementation has twice the bandwidth of Bluetooth 4.2 LE and four times the range. In the official announcement they state that the range can be 500 meters in the best case scenario. Bluetooth 5 also has Slot Availability Masking (SAM) feature that can detect and prevent interference with for example LTE bands. [33]

Gupta explains in the book *Inside Bluetooth Low Energy* that Bluetooth supports ad hoc networks. It means that the devices are not relying on base stations or any pre-existing infrastructure. The devices can dynamically move into the effective area exchange data and go out of range. [31]

The effective range depends on propagation, material blockade, configuration of antennas and level of remaining battery. The exact same laws of physics apply to Bluetooth as applies to Wi-Fi. Most Bluetooth applications are for indoor use, where presence of walls makes reflections of the signal which makes the range way lower than what it could be with line of sight signal and products designed outdoors. [31]

Bluetooth equipment is categorized by the output power level into three different classes. Class 1 devices have a maximum transmission power of 100 mW and a range up to 100 meters. Class 2 devices have a maximum transmission power 2,5 mW and a maximum range of 10 meters. Class 3 devices have a maximum of 1 mW transmission power and the range varies from 0,1 to 10,0 meters. For example, the theoretical maximum bandwidth is 2 Mb/s with the newest Bluetooth 5. The Forward Error Correction (FEC) slows the theoretical speed. Bluetooth uses Gaussian Frequency Shift Keying (GFSK) modulation which filters the pulses with Gaussian filter. The Bluetooth architecture combines a circuit and a packet switching technology. [31,33]

All Bluetooth devices have four entities used for upkeeping the security on the link level. First, the Bluetooth device address that is a 48 bits long address which is unique for

every Bluetooth device. The address is defined by IEEE. Second, private authentication key, which is a 128-bit random number used for authentication process. Third, encryption of the handshake needs a private encryption key, which differs between 8 to 128 bits. Forth entity is a random number which is a regularly changing 128 bits long pseudo-random number that is created in the device itself. [31,34]

After listing few problems of security of Bluetooth Juha T. Vainio from Department of computer science and engineering of Helsinki University of Technology concludes in *Bluetooth Security* that: “All in all, there are several problems still in the security of Bluetooth. It seems to be adequate for smaller applications, but any sensitive or otherwise problematic data should not be transmitted via Bluetooth.” [35]

### 2.3.3 Software defined radios

Software defined radios (SDR) are a class of reconfigurable and reprogrammable radios of which characteristics of physical layer can be manipulated via software changes. SDRs are supporting different functions on the same platform, in its' software there are defined many different base band radio features for example error correction coding and SDRs has minor software control over RF front-end operations. Because there are so all baseband radio functionalities implemented by software, this means that different kind of modules can be stored in advance into the memory and to be chosen when needed for a specific task, for example a specific modulation or error correction coding. SDRs are very agile for any kind of communication because these functional blocks can be changed by a user or a software in real-time. [36]

Wyglinski A.M. and Di Pu remind in their book *Digital Communication Systems Engineering with Software-Defined Radio* that the definition of SDR is very wide. However, there are few characteristics mentioned in the book that generally defines SDR [36]:

- Multifunctionality, possesses the ability to support multiple types of radio functions.
- Global mobility, transparent operations with different communication networks located around the world.
- Compactness and power efficiency.
- Simple manufacturing, baseband functions are software features, which have nothing to do with the hardware.

- Upgradability, to enable functionalities of the latest communication standards, just firmware update needs to be uploaded to the SDR platform.

There are multiple manufacturers that produce SRDs. For example Netcontrol, SATEL and RACOM have a UHF and VHF radio modems in their catalogue. All their radios has custom made firmware, and the feature lists have enormous amount of features. Typical catchphrase is that their product has greater range than any other wireless devices [37]. It's true that the SDR overcome the devices of IEEE 802.11 and IEEE 802.15.1 standards in effective range, but when operating with VHF or UHF frequencies or even lower frequencies the data rates are also lower. Also, there is no point to implement a wireless communication system with SDR that works on 2,4 GHz because then standardized out of the shelf Wi-Fi products are more cost efficient. [36]

Wireless communication implemented with SDRs has strong basis, because these radios can be equipped with fully featured Linux firewall. There is also possibility for end-to-end tunnel with Internet Protocol Security (IPsec) which is a network protocol suite that authenticates and encrypts the packets of data sent over a network. Payload can be encrypted with AES256 with own or randomly generated cryptographic key. [38]

The first uses of SDR goes way back to 80s, but nowadays the use cases go beyond the traditional telecommunications. José Raúl tells in article *Software Defined Radio: Basic Principles and Applications* that there has been interesting experiments with software defined radios and those experiments have provided positive results about the possible future applications of the SDR. There are great possibilities in following areas to utilize SDR: aviation tests, multi-path communications, broadcast transmissions in multi-media, co-operative wireless networks diversity, quantum optical communications and particularly in marine industry. [38]

### **2.3.4 Satellite link**

Commercial satellite systems are another major component of the wireless communications infrastructure. These systems are used mainly for messaging and location tracking of vessel fleets. Also, satellite services are practical backup when no other system has an operating communication because of the extreme ranges on a sea.

However, via satellites, it is possible to transmit any type of data and not just the simple messages or location information. Data of mobile networks, broadcasts of television and navigation systems can be delivered through satellite link. The greatest fact about satellite systems is that large areas can be covered with just with a single satellite

antenna. The coverage of single antenna can be size of a single country. The functionality of satellite operated devices is comparable with those which work via terrestrial network. So, voice calls, text messages and internet access are supported on satellite link. Depending on the satellite system the services might vary, and the covered area may be even around the Earth. There is fixed installations available for the marine solutions where could be a dynamical antenna that tracks satellites to keep the best possible connection to it. The common phenomena for satellite telephony and satellite Internet service are that indoor reception is problematic, the satellite connection requires line-of-sight (LOS) or near-LOS connection in order to function correctly. In practice, the phones typically have external antenna connectors for the antenna installation in the external parts of buildings or vessels. In addition, there is the possibility to use repeaters for enhanced coverage. [18]

Subscriptions for satellite service are very costly and the amount of data is very restricted. Even the amount of data is not crucial characteristic of the wireless communication that is looked for, the satellite service is excessive service in this kind of an application that this thesis is focusing on.

### **2.3.5 LTE**

A mobile network is a communications network that covers a huge land area and can reach almost every corner of the world and is established wirelessly by transceivers that are known as base stations or cells. Usually a mobile network is a communication network that has wired links but the last link is wireless. [26]

A mobile network and a wireless network have similar functions, they are still completely different kind of networks. Wireless means having access to a wireless network such as LAN, WAN or a 4G/3G cellular network. A wireless network has a fixed or portable endpoint providing access to a distributed network. On the other hand, a mobile network creates access to a distributed network via a portable device, for example that makes possible to connect to a vessel, even a vessel is operating out of its' regular operation area.

Combining cells together makes possible radio coverage over a huge geographic area. Large coverage area is infinitely growable, because amount of towers are not limited by the horizon. This enables numerous portable transceivers, for example mobile phones, laptops and LTE-modems, to communicate with each other. There is not even a problem when the transceivers change their location from cell to another. The biggest

telecommunication operators have built mobile networks all over planet earth so implementing the practical part of this thesis to actual vessel would not be dependent of the location. There are also private mobile networks that can be set just for example ships, companies and all sort of organizations. [26]

In the book "*LTE - The UMTS Long Term Evolution : From Theory to Practice*" Sesia and Stefania states that the LTE system is completing the trend of expansion of mobile networks. The mobile network are just not for voicecalls, but more like moving towards being a wireless service for multimedia. The main goals of UMTS were similar, but the LTE has been designed from the beginning with the goal of improving the radio access technology to the direction that all functions should be done with packet-switching. Earlier model was the circuit-switching. [26]

The stated requirements from 3GPP, which is the global partnership of six regional Standards Development Organizations (SDO), for LTE standard are following [26] :

- Maximum data rate of downlink is 300 Mb/s and for uplink is 75 Mb/s with 4x4 MIMO support along with Control Plane (C-Plane) latency under 100 ms and User Plane (U-Plane) latency under 10ms.
- User throughput per MHz at the 5% point of the Cumulative Distribution Function (CDF) in down- and uplink.
- Mobility of user devices can be over 300 km/h.
- Spectrum flexibility, seamless coexistence with previous technologies and reduced complexity and cost of the overall system.

The requirements mean in practical that the handshake between cells has to be possible without interruptions. Also, the new protocol of fully packet-switched network makes it easier to merge it to existing networks. The bandwidth is faster than needed, but it's not a bad thing to have when keeping an eye on the future improvements. Also, the latencies fulfil the requirements of water transportation to operate as a real-time system. Sesia and Stefania reminds multiple times in the book that these requirements are evolving all the time through the advancement of technology. [26] All in all, the stated requirements for LTE of today, are kind of characteristics which are more than a suitable for developing wireless communication for shore charging application.

### 2.3.6 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communication technology and standardized by IEEE 802.16. Name for WiMAX comes from the WiMAX Forum. The Forum was formed in 2001 in order to enforce and widen the distribution of the IEEE 802.16 standard. WiMAX Forum promotes the WiMAX as follow: “*WiMAX is an OFDMA-based, all-IP, data-centric technology ideal for use in delivering mobile 4G services.*” [39] Standard’s version IEEE 802.16m or was a candidate for the true 4G technology. The biggest rival was LTE Advanced standard. [18]

WiMAX is capable of data rates of 40 Mb/s. However, theoretical speed is all the way to 1 Gb/s with specific base stations which fulfils the requirements of International Telecommunication Union Radiocommunication Sector (ITU-R). IEEE 802.16 is made to operate between 10 - 66 GHz band. WiMAX is in the portable communication category which means that the possibility of changing access points for communications. It requires separately initiated connections with both access points, the new and the old. WiMAX can switch access points sort of quickly with minimal packet loses so it is suitable for fast moving and high bandwidth needy solutions. [40]

The additional benefit of OFDM is that it allows flexible bandwidth utilization for the connections states Jyrki T. J. Penttinen on *Wireless LAN and Evolution*. In general, OFDM provides the scaling of bands of WiMAX in the range from 1,75 to 20 MHz. WiMAX supports both FDD (Frequency Division Duplex) and TDD (Time Division Duplex) capabilities like all OFDM supporting devices. FDD makes the transmitting and receiving to operate in different frequencies and TDD is a method to separate outgoing and return signals. It is full duplex communication working over a half-duplex link. [40]

WiMAX is designed to be a technology for systems that operates with long distances, but the high frequencies are not ideal for long distances compared for example to VHF. However, WiMAX Forum tells that they are researching possibility to have a block below 1 GHz. Frequencies under 1 GHz are more suitable for covering wide areas because of the propagation characteristics of the bands. The useful area of this band is evaluated to be limited to five kilometres. The theoretical range of the operational signal is more than ten kilometres. With the lowest power output WiMAX requires LOS, as the higher frequencies tend to be blocked or reflected from obstacles. [40]

Other typical technical characteristics of WiMAX are as follows [40]:

- Header compression.
- Encapsulation.

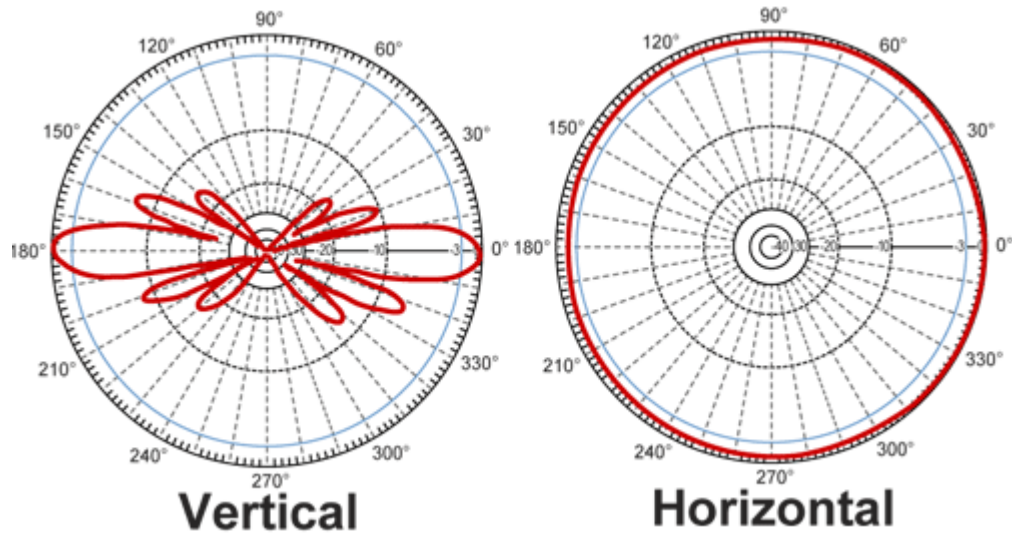
- Fragmentation of packets.
- Advances security measures such as PKM (Privacy Key Management) and EAP (Extensible Authentication Protocol).
- Fast channel change protocols.
- Variation in output power levels.

WiMAX was a good competitor in the WLAN offering, but as a losing technology it might not be a good decision to implement it with ACS. It is on it's best in difficult conditions, as open-sea, and sort of in long distance solutions. An example of this is the implementation of communications services to areas where public telecommunications infrastructure is lacking coverage or capacity. Some rural areas which are otherwise hard to access and which have been serviced previously with GSM and VSAT technologies. [18,40]

## 2.4 Antennas

The choice of antenna is one of the most important phases of the design of a radio network. The mission of antenna is to radiate as best as it can the transmission of a feedline. There are lot of different kind of antennas: directional, omnidirectional, highly directional Yagi antennas, dish antennas and much more. The type of the antenna is very crucial because there are multiple factors that impact to the performance of the antenna and its gain. Here is a list of a common factors: height, frequency, radiation pattern, polarization, materials, structure, wind load, IP classification. [41]

An illustration picture of omnidirectional antenna can be found under in the *Figure 3*. The horizontal range is the same in every direction. The power is spread differently with different kind of antennas and the gain is expressed in dB. The opposite of gain is attenuation, loss. In this thesis the author had to use intentional attenuation to limit the power of the UHF radios, when testing within short range 2 meters. [41]



**Figure 3:** Illustration picture of range of omnidirectional antenna[42].

The same kind of access points, one without and other with an extra semi parabolic antenna could have difference in range of 30 km because the signals are directing better to the receiver. Thiele explains in the *Antenna Theory and Design* that higher gain rating indicates further deviation from a theoretical, perfect isotropic radiator, and that's why the antenna can send a signal to specific directions, as compared to a similar output power on a more isotropic antenna. For example, 8 dB gain antenna with a 100 mW output power will have a similar horizontal range as a 6 dB gain antenna with 500 mW. So, it is possible to increase the range by upgrading a antenna which have higher gain to wanted directions, not just add transmission power. [43]



**Figure 4:** *Picture of a parabolic antenna. Antenna in picture is one grade of too huge for regular Wi-Fi access point [44].*

Wi-Fi certified devices can have multiple antennas, which grants faster bandwidth. The amount of interference can be reduced also with technic of multiple antennas. Also, multiple antennas make the useful signal stronger. Adding antennas increases significantly the range and network speed without passing the regulated limits of output power, but the antennas have to be compatible and set up right as mentioned before. [29]

## **2.5 Environment in the marine industry**

Marine industry brings few extra challenges for the implementations of control automation and the communication technology on board compared to on land factory floors. Of course, on land there are different kind of hazardous threats as mechanical, chemical and nuclear. At first hand, an environment where vessels navigate doesn't sounds as demanding as it is. There are for example lot of tremor, heat, water, salt and wind inside vessels and also outside of them.

Therefore, there is Ingress Protection code (IP code) based on the IEC standard 60529. This standard is applied in very different kind of environments and highly used in marine industry. IP codes are classified by categories. These codes condense the scale of protection offered against factors like physical objects, dirt and moisture. The IEC standard 60529 provides detailed information than more generic marketing terms often applied when talking about water resistance. The rating consists of letters "IP" and two numbers. The first number tells the level of protection against solids and the second indicates the protection against liquids. [45] It's important that the components or the casing of the chosen components are chosen with caution to fill the required protection level.

Also, the human factor needs to be taken in to account when designing the wireless communication system especially when implementing system to a retro fit vessel. There is lot of dangerous areas to access when installing required components to vessel, for example oxygenless spaces and high drops. Continuous processes of vessels can also be fatal for a commissioning engineer. Today the shipyards and stakeholders are more aware of the safety risks and doing improvements to progress the overall safety. In the end, when designing and implementing wireless communication systems the special needs for the safety and protection of the components in this specific environment should be taken consideration.

## **2.6 Classification society and legislation**

The international Maritime Organization (IMO) is an agency of United Nations which mission is to enforce safety, security and efficiency of shipping on clean oceans. Over 60 years IMO has developed more than 40 conventions and protocols and more than 1000 recommendations and codes to improve safety of vessels and decrease pollution at seas. The recommendations of IMO are mainly universal and need to be followed in international trade. Implementation of these codes and protocols are measured through worldwide cooperation programs, consultancy and advisory. IMO also organizes training for stakeholders to increase the knowledge of maritime safety. [46]

The most important convention of maritime safety is the International Conventions for the Safety of Life at Sea (SOLAS). SOLAS is widely acknowledged and followed when building a new vessel. The latest edition of SOLAS is SOLAS Consolidated edition 2014 which is huge collection of requirements for different sections of safety of vessels and some of the protocols are in effect even from 70s. [46]

In regards of wireless communication of automated charging system SOLAS states exact requirements for the radio equipment. There are for example requirements for the emergency radioequipment in Regulation 7.1.6.3 as follows: “- ready to be manually released and capable of being carried by one person into a survival craft”. [46] As you can conclude that it leaves lot of details for the designer and there are no simple and accurate regulations for wireless communication on automated charging systems. Eventually the final design need to be approved by superintendent by classification society. Lot of the requirements of SOLAS are very specific, for example the frequencies of Digital Selective Calling (DSC). All fleets and single vessels might have their own characteristics which come from the different utilization and needs of owners. SOLAS however ties all the regulations together and the classification societies base their own rulebooks to SOLAS. Different shipping companies, owners of the fleets, use different classification societies therefore there is different methods to interpret the SOLAS. These differences in the working processes, interpretation of SOLAS and different classification societies makes the new build vessel projects very complex to implement and requires lot of cooperation from all the stakeholders. [47]

## **2.7 Cyber security**

There is no easy and single way to define cybersecurity. Lehto and Kähkönen define it as follows: “It is actions to countermeasure the cyber attacks and managing the risks of cyber attacks” [48]. The focus of this chapter is in the security mechanisms of IEEE 802.11 systems because of the wireless network to be designed and created for the on shore to ship application.

The connectivity between automation and operational systems of vessels are not increased only together but also more connected to the Internet states Jorgensen at ABS CyberSafety webinar. He also tells that: “Ship or platform systems, such as propulsion plant and ship control and ballast and cargo management combined to digital accesses, for example web-based systems and remote access methods, enable the appearance of new threats such as malware, phishing, poisoned links and attachments.” In the marine industry, third-party access to a control systems of cruisers and tankers and third party service providers are very common nowadays, explains Jorgensen. These factors add cyber security related requirements from the organizations of shipyards and requirements are also targeted for all the stakeholders. Safety critical systems should be prioritized when assessing and mitigating the cyber risk states Jorgensen. [49]

Jorgensen also teaches that cyber risk management starts with the identification of cyber risks, which can be external and internal. At the moment there are no evidences nor the records of incidents which makes it a challenge of aspect of cybersecurity. When there is no facts and documented information about incidents and their impact, in author's opinion it's crucial to make it requirement by legislation or classification society. However, the organizations of marine industry needs to take in account all the aspects of their operations that are increasing their vulnerability for cyber-attacks. There are multiple motives for criminals and criminal organizations to search these vulnerabilities. [49]

In the book "*Power Plant Instrumentation and Control Handbook*" by Swapan Basu, Ajay Kumar Debnath states as follow, the wireless medium is an open medium and without countermeasures it is easy task for an attacker to eavesdrop, to add malicious packets, or just simply jam the medium, this way challenging the reliability and the timing of the transmission[50]. Wired networks are way more secure than wireless ones, for example in many public buildings a intruder doesn't need to be physically inside and they can try to access the network wirelessly by taking advantage of a backdoor such as Back Orifice [51]. On the other hand, ensuring confidentiality and accountability is not the main goal when designing a fieldbus. The authors teaches, that the recent trend to connect fieldbuses to the Internet by means of gateways has led to securing the gateway, but it is also required to protect a fieldbus against attacks from the inside, for example with encryption and authentication protocols. [50]

There are two major security problems which concerns industrial applications. First is the issue on signal integrity which means interference or alteration of data that causes possibility for malicious users with bad intentions to simply disconnect a whole network. Even a slight alteration in the data can be crucial. Preserving the network online is very important for some industrial applications, for example the shore charging. This kind of problem can be even harder for technologies like Bluetooth and IEEE 802.11, which area of operation have high chance for interference by other technologies operating in the same ISM band. These two standards implement the spread spectrum techniques to overrun the interference problem in most cases by channel hopping. To maintain integrity, it's important also ensure that authorized system users are only able to edit the data that they are legitimately authorized to edit. [52,53]

The second major matter of information security is confidentiality, authentication and authorization problems. Unauthorized users should not be granted for accessing the WLAN and exploiting the shared resources. In other words, it is matter of preventing sensitive information to be reached by wrong people. Data encryption is basic method to ensure confidentiality. The encryption involves the process of reforming the transmitting

data so that it is non-understandable by anyone who does not have the key for decryption. After encrypting the data exchanged between a client and a server, the risk of interception and misuse are lower. The IEEE 802.11 standard provides a native technic to enforce the authentication of WLAN. The Wired Equivalent Privacy (WEP) is implemented at the MAC layer. [52] The security level of WEP protocol has proven to be insufficient in some aspects, states Dhiman and Deepika on the *WLAN Security Issues and Solutions* [54]. In response to the insufficient performance of WEP, Wi-Fi Protected Access (WPA) and its' next versions were developed. [53]

In addition to integrity and confidentiality there is a third very important aspect about information security in marine industry. The third major aspect is availability. The availability means that system users which have the permits to access information can have access to it when they really need to. Disruption of availability for a quick moment can lead to a grounding and physical damage to a vessel or a port structure. To improve availability, it's important to have for example sufficient communication bandwidth, redundant components and features to recover from disasters. [55]

All the mentioned wireless technologies in this thesis have security vulnerabilities. Even a minor bug can make a security breach possible. For example, via Bluetooth it is possible to connect a group of wireless devices to one another with ad-hoc, thereby forming a small scale network consisting two or more devices, a piconet. In this kind of case, the network topology may be changed dynamically because of physical movement of the devices within same piconet. There is no centralized security management system in ad hoc network. The frequency hopping sequence of a piconet can be determined through the use of inexpensive tool kit and free open source software. [56] As stated earlier, all the Bluetooth devices have a unique Bluetooth device address. With this unique address, the device can be identified, tracked and monitored. These facts solo and together make Bluetooth devices vulnerable for cyber attacking. This was just one case and it's a good reminder that cyber security is a process and needs to be improved continuously. [52]

All in all, cybersecurity increases after the cyber risk is lowered. For organizations an overall risk management and risk-based approach are the main tools to achieve better and increased security against cyber attacks.

## 2.8 State of the art projects

Now the horse race is intense what comes to the autonomous shipping and the fast charging solutions for ferries and why not even for a bigger vessel in the future. In this chapter we take a short glance to the state of the art projects which are related by matter of wireless communication regarding autonomous control or automated charging in marine industry. The biggest competitors in the business which have made a outlet about the accomplishments of their solutions are Wärtsilä, ABB and Rolls Royce, but Rolls Royce sold it's marine business unit to Kongsberg on summer 2018 [57]. There is not much public information to be analysed so this chapter is more like directional in matter of making a proposal for wireless communication in ACS.

Wärtsilä published impressive Youtube video where they introduced a wireless charging for a ferry, MF Folgefonn, in Norway. The benefits of the system seemed to be great efficiency of the wireless charger which is based on electromagnetic induction. Wärtsilä also stated that the wireless charging has benefits what comes to the seafaring. The most interesting part of the Youtube video is that they don't hide the communication technology which they use between port and MF Folgefonn: "Armed by Wi-Fi connection between shore and ferry, the charging system is automatically prepared during approach..." Wärtsilä has made their research and votes for Wi-Fi. [58]

On December 2018 ABB announced that the Suomenlinna 2 was remotely piloted through test area near Helsinki harbour. The test proved that human oversight of vessel from on-shore command centre is possible with today's technologies. There is no public information about the wireless technologies used with the remote control system. Their marketing video tells: "...we have cameras, we have lidars, we have radars and we have a GPS system for accurate positioning of the vessel and connecting that to control system that is able to control the vessel position, speed and heading is very unique..." so the bandwidth of the wireless link has to in a decent level to deliver all that information in real-time and the range needs to be in a good level also. [59] Therefore, it could be inferred that the link wasn't established with SDRs or Bluetooth.

Company ForSea operates two fully electrical ferries on a 4km route between Denmark and Sweden. The vessels were powered by diesel engines but ABB's conversion project for Tycho Brahe and Aurora started a new ear on these ships. Conversion project included 4160 kWh battery on board for both vessels. Also ports in Helsingør in Denmark and Helsingborg in Sweden got the ACS. Unfortunately there is no mention of implemented communication method with Tycho Brahe and Aurora. [60]

Rolls Royce has made successful autonomous maneuver tests with Falco ferry which operates on Nauvo, Finland. The car ferry Falco successfully navigated autonomously its basic route between Parainen and Nauvo. The return journey was conducted under remote control refers Rolls Royce's public announcement. [61]



**Figure 5:** Finferries' Remote control station on Turku, Finland. Picture by Niclas Lundqvist and Yle [57].

On news of Yle there is a video showing LTE antennas and also the Rolls Royce referred to the tech as follows: "When the ship is manoeuvred out of the congested harbour – In this type of operation a high bandwidth and low latency communication link is needed. In certain areas this can be provided by the land-based communication networks and satellite communication systems remain as back up." [57] Conclusion is that Rolls Royce has implemented their system with multiple wireless technologies and not just rely on a single wireless link.



**Figure 6:** Design of Yara Birkeland [62].

Kongsberg is implementing world's first fully electric and autonomous container vessel called Yara Birkeland at the moment. In Kongsberg's official announcement they state that they can start testing the ship on December 2019. There is also listed the used sensors and communication technologies. Because the ship is designed to be fully autonomous, it is interesting to notice that the communication technologies are sort of outdated or more like the ship has a regular communication equipment on board when comparing to the other vessels: "Maritime Broadband Radio, Satellite Communications and GSM". The vessel doesn't need Wi-Fi or LTE components because it can fully operate without external control from shore. [62] Interesting part of the Yara Birkeland project is that it's supposed to operate with fully autonomous container loading system by Finnish Kalmar [63].

## 3. PROPOSAL

This chapter explains the proposal for communication protocol and wireless technology between a port and a vessel for automated charging system. Proposal took shape through a product development which had concrete requirements and a problem to be solved. The proposal includes the general structure of the system including the two similar stations and the explanation how the communication between the stations is established and verified. There is also a proposal for the antennas even though those were not in the main focus of this thesis.

There are four subchapters in this third chapter. In the first subchapter author sets the requirements for the system that would solve the problem. The second subchapter introduces the general structure of the proposed system to fulfil the requirements. The third subchapter presents the proposed communication protocol and the last subchapter proposes the wireless technology and the suitable antennas for them.

### 3.1 Problem statement and requirements

Main focus of this thesis is to resolve which are key issues in a wireless fieldbus system on automated shore to ship charging application and the usage of wireless technologies in maritime in general. Starting point for this product was that there is not out of the shelf product to establish wireless communication to automatically charge a battery driven vessel. After extensive theoretical background work there was carte blanche for the author to implement a solution. Even top-quality theoretical overview can't create an all-encompassing idea, so the practical part is compulsory and splendid opportunity to learn and apply the theory to the real world. When developing a new product, it is a sort of trial and error kind of situation like this future product. Product development is long process and in the extent of master's thesis, there was no possibility to have implementation of many proposals or better and better iterations of chosen proposal. This fact made the author to rely on one proposal that is introduced in this chapter.

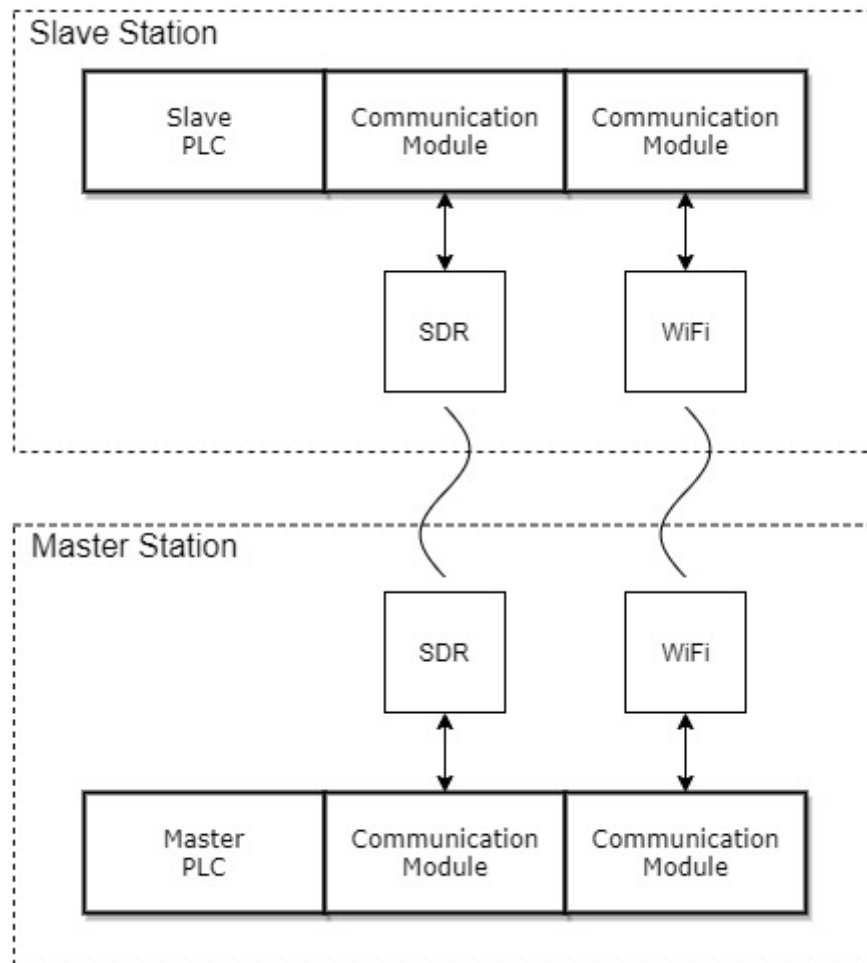
There are few requirements for the physical structure for the future product. Only compulsory components are ABB's 800M controllers which of course also limit little bit other components because of possible compatibility errors. All the used components also need to be commonly used in the marine industry and be able to survive in harsh open-sea environment. Unfortunately, the budget of this thesis does not provide the possibility to have the final tests at sea. There are no requirements for the communication

protocol. Author could choose the most suitable communication protocol for the product. However, the wireless link has two requirements: latency and range. The latency doesn't have to be a so-called factory level real-time, but it has to be under 1 second. The requirement for the range didn't have a specific measure. It must be sufficient and that is hard to point out without tests with a real vessel and in real environment. The sufficient range is bound to the end users, operated vessels and ports.

### **3.2 Structure of the system**

This master's thesis proposes an approach for the communication protocol and the wireless link between two similar stations which simulates the components in a port and a vessel in automated charging system. The approach tries to keep the system simple and verify the robustness of wireless communication with ABB's controllers. The proposed system is designed to have a redundant communication which is requirement in critical communication in marine industry. The proposal includes single communication protocol and two different technologies for the wireless communication to work as backups of each other.

These two similar stations in the system have the same hardware and only difference is in the downloaded programs in the programmable logic controllers. Main components of the stations are PLC, communication modules, power supply, Wi-Fi router, SDR and antennas. Wi-Fi router and SDR are connected to their own communication modules which are linked to the controller. Communication modules are responsible establishing the communication between the stations. Other station works as a master when the other station as a slave therefore it only replies to the enquires of the master. The proposed structure of the system is shown in *Figure 7*.



**Figure 7:** Structure of the system.

This proposal shows a station as it were a simple machine that includes all the needed components in a compact case but the stations should be seen as a individual system which components locate in the same operation area not in the same casing, for example one stations is responsible of the port's side of the communication but the components can be shattered around the port area with certain restriction.

PLC and communication modules need to be connected physically to each other and to the same DIN-rain. Components for the wireless communication should be install to a location where the attenuation of the link is smallest. Both SDR and Wi-Fi router with antennas requires individual power supply if they are positioned elsewhere then the PLC and the communication modules.

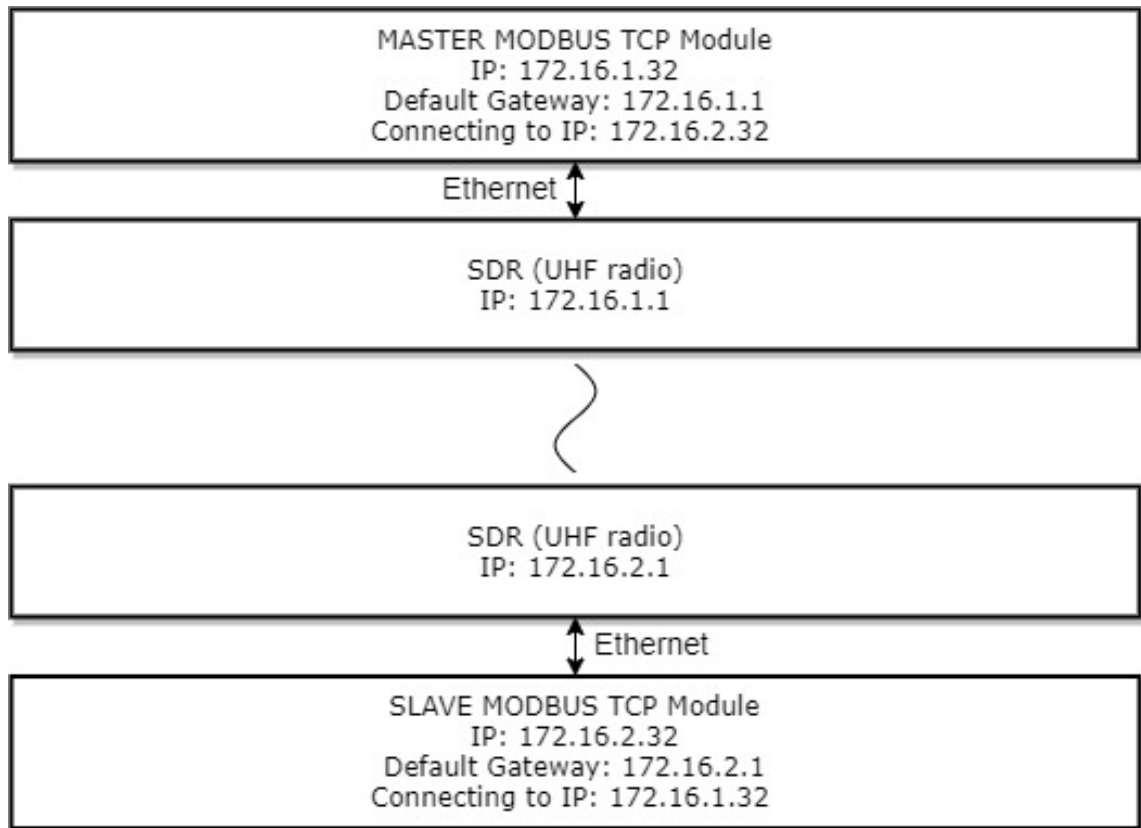
This approach proposes the use of MODBUS TCP communication protocol so the communication from the communication modules to the beginning of the wireless links is done with TCP/IP via Ethernet. MODBUS TCP embeds a standard MODBUS data frame without the checksum into a TCP frame, as explained in the second chapter. For

a wireless technology this thesis proposes system where the communication relies for multiple technologies, in this case in SDR with ultra-high frequency and Wi-Fi technologies.

### **3.3 Communication protocol between the stations**

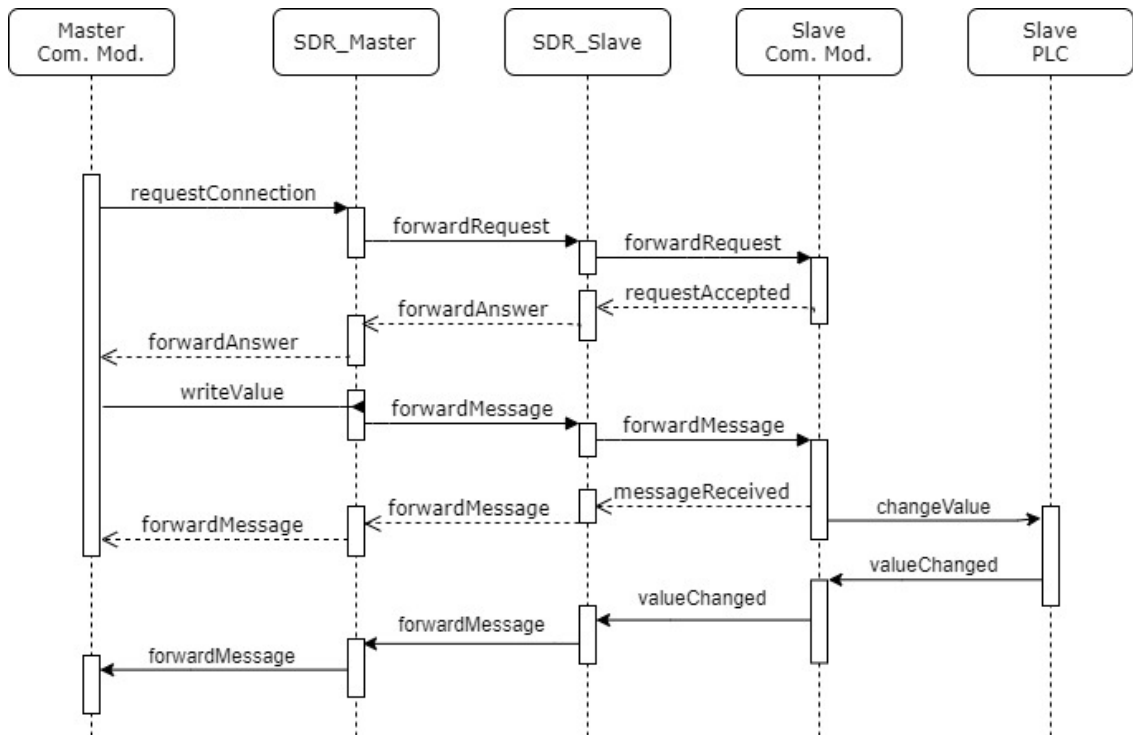
This subchapter explains in detail how the connection is established and how does the communication process work on TCP/IP between stations. The proposed communication protocol is MODBUS TCP which is fully compatible with ABB's 800M controllers when additional MODBUS TCP communication modules are added. Also, MODBUS TCP is de facto protocol in automation industry and has long history of successful implementations on real life applications.

MODBUS TCP uses a master-slave type of communication. The other station acts as a master and the other as a slave. To open a connection, the master needs to know the gateway IP address, where to start asking the MAC address of the slave. MODBUS TCP always works on gate 502 which is defined in the MODBUS protocol [64]. Connection between the devices can be established even they are in different subnets in Ethernet network. There needs to be an open connection between stations so the stations can communicate and ensure the essential data between the vessel and port in a real-life situation. When the connection is established, it will stay that way until either the master or the slave closes it or when the signal strength of wireless link weakens.



**Figure 8:** Proposal of TCP/IP communication between stations.

TCP/IP is two-way communication so both stations can send and receive messages. Yet, the Ethernet is full-duplex communication on wire, but the wireless communication is only half-duplex. In the implementation phase the master station will establish the connection by sending a request for a communication to the slave. The slave is waiting a request from the master stations. The slave stations reply to the request and is ready to receive the real message from the master station. However, in this proposal only the master is for example establishing connection or writing new values. The point of this kind of master-slave proposal is that there is no need to build master-master system to find the answers to the set research questions and evaluate the latency of the communication or signal strength suitable for ACS system. Even though the ACS would require in real life application a master-master sort of solution.



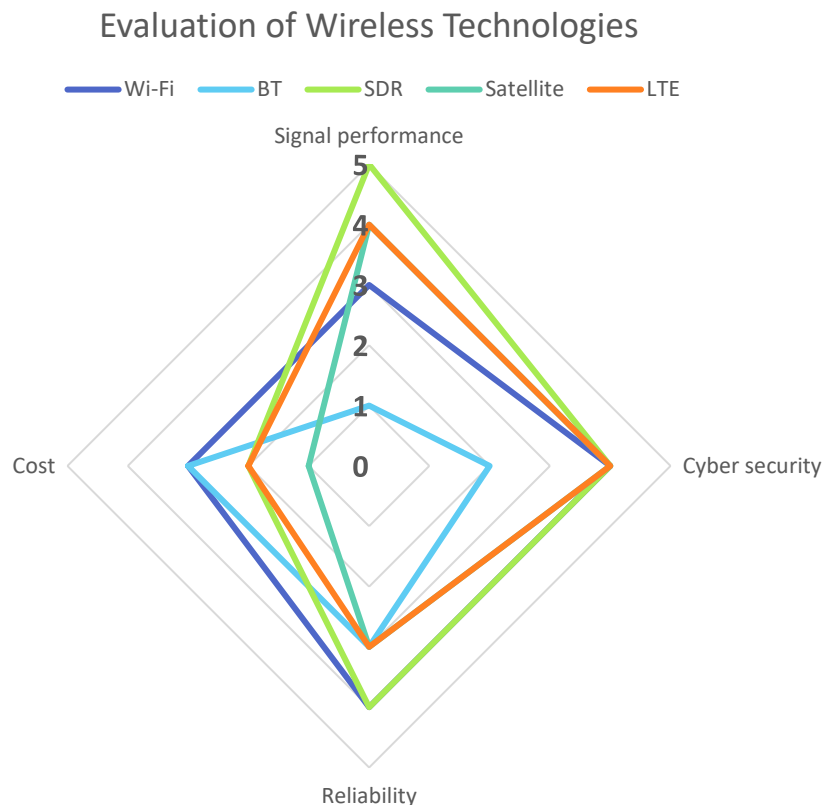
**Figure 9:** Example communication between stations represented in a sequence diagram.

In the beginning of the sequence that is presented above in the *Figure 9*, the master sends the connection request to the communication module of the slave station. The slave gets the forwarded messages through SDRs and answers with an approval for the communication. When the function request is accepted, the slave does what the master requested, and it informs master when the function is done.

### 3.4 Wireless technologies and antennas

There are six different wireless technologies presented for automated charging system in *Chapter 2*. Support for WiMAX is however ended and as well components of the technology are very tricky to get so WiMAX was not chosen to the final evaluation. In order to choose the suitable technology or technologies for the implementation of the wireless connection, the wanted characteristics and benefits should be discussed. The main factors which are evaluated when choosing a technology on this marine application are signal performance, cyber security, reliability and cost. The capacity to deliver great amounts of data is not a big factor in this kind of application, because of the small messages that the automated charging system needs to exchange between a vessel and a port. Even the bandwidth is not the thing to measure in the signal performance, range and signal penetration are. Levels of cyber security these technologies have was

measured according to the three main aspect of information security mentions in *Chapter 2*. The reliability is sum of signal performance, cyber security and other specific features that effect the reliability aspect for example the technologies were evaluated with a fact in mind that there could not be any repeaters implemented for the link because of the environment of a sea. The cost consists single payments plus possible monthly payments. The radar chart below is showing the technologies as function of the evaluated aspects.



**Figure 10:** The technologies as function of the evaluated aspects.

Evaluation was done subjectively by the author but strongly relying on the research done in this paper. Higher score is better and grades goes from 1 to 5. SDR got the best grade from the signal performance. Its' range and penetration of the signal is customizable and performing excellent. Also, Satellite and LTE have great range, but the penetration of the signal is not as great as SDR's. Bluetooth is lacking strongly the range and Wi-Fi is mediocre in this aspect. Costs are similar with Wi-Fi, Bluetooth and LTE components. SDR components are expensive but satellite communication supported components are even more expensive. Satellite and LTE systems come with monthly subscriptions. Wi-Fi, SDR, Satellite and LTE systems come with the required tools to tackle cyber security risks. Wi-Fi and SDR are the most reliable technologies of these five, because there are

no need for monthly subscriptions, easy to build redundant system and the implemented system would not need external system to operate.

Specifications mentioned above and requirements for communication in marine applications bring forth two technologies, Wi-Fi and SDR. Because of the requirement of redundancy and the different characteristics of the proposed technologies, it is proposed to use two different wireless communication technologies simultaneously. Both Wi-Fi and SDRs has very strong cyber security features and wide range of antennas available to build a signal as wanted. The maximum range of VHF and UHF SDR's are greatly better than Wi-Fi's but the cost of Wi-Fi components is lower because of the vast number of different vendors compared to SDRs. These two are also good combination together compared to other combinations of the presented technologies in this thesis.

For reasons abovesaid, the implementation of the wireless communications will be done with two technologies, Wi-Fi and SDR. Both will be equipped with dipole antennas, because of the easy install and to test the system more with an off the shelf kind of components. With directional antennas it is possible to countermeasure the attenuation better and increase the maximum range, but it was discussed that this thesis should focus on pointing the performance with basic components. The specific components that were chosen to the implementation are introduced in next chapter.

## 4. IMPLEMENTATION

This chapter presents an implementation of the proposal presented in *Chapter 3*. This chapter introduces the hardware and software developed during this master's thesis. During implementation phase the author build two stations to simulate the communication of ACS. There are four subchapters in this chapter. The first subchapter describes the installation and the details of the used components, which could be used in a real-life ACS. The second subchapter describes the development of the software with ABB's Compact Builder. The third subchapter represents the configuration of the wireless network components and explains the chosen setups. The fourth subchapter explains the test setup and the special needs and changes for the testing phase.

### 4.1 Hardware

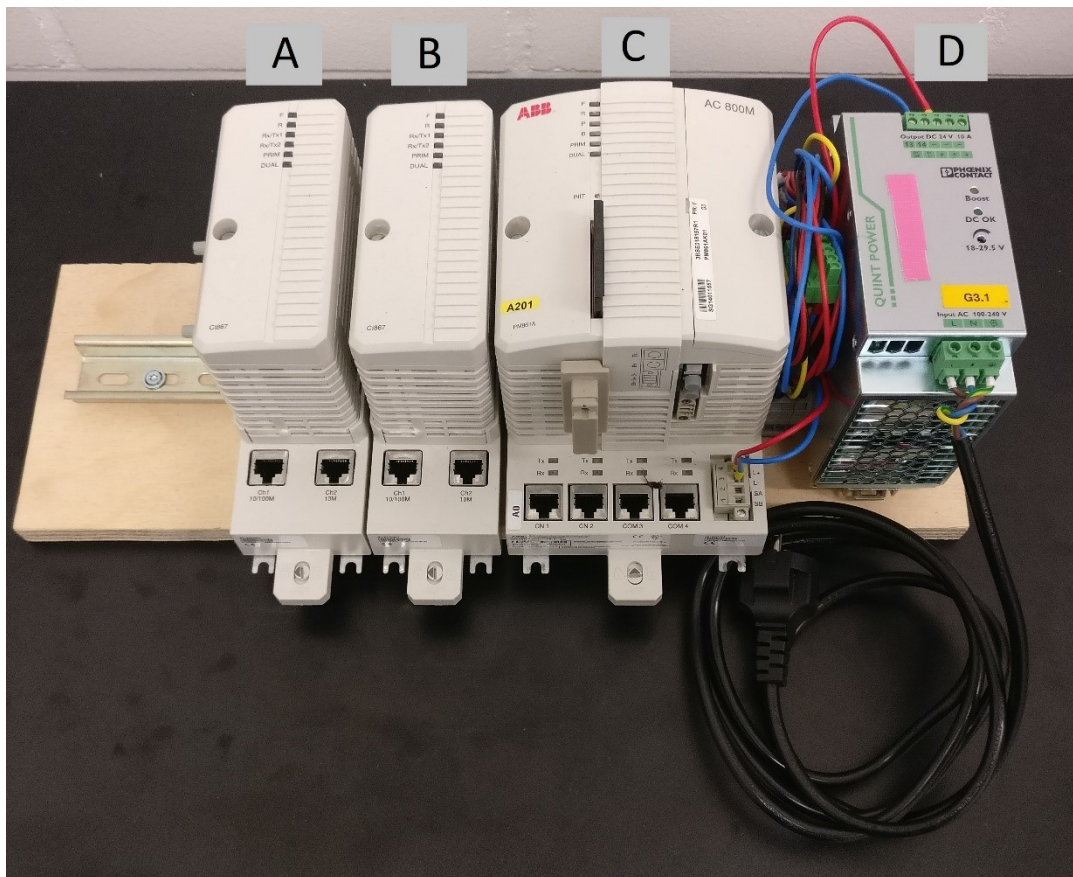
As mentioned earlier implemented system have two stations which have same components. The main components of a station are a PLC, two communication modules, a SDR, a Wi-Fi router, a power supply and antennas. There were also lot of different equipment needed to build the test setup, for example: power drill and circular saw. On top of these there were also three routers to ease the implementation.

The PM861 PLCs are manufactured by ABB. PM861 has microprocessor clocked 48 MHz and 16MB of RAM-memory, controllers for all built-in communication interfaces, real-time clock, LED indicators, initialization push button and a Compact Flash interface. It also has four communication ports: two Ethernet ports and two serial ports (RS-232C). To set up the IP address for the first time, it needs to be done through the serial port in channel 4. Best method was to have a USB-A to RS-232 cable and in addition correct drivers and Ipconfig software for the task. The controller has also Redundancy Control Link which enables to connect to PM861 to each other and configurate them to work redundantly in the Compact Control Builder. In this implementation, there was no redundant design for the controllers. However, the wireless communication was redundant.

The communication modules, CI867 MODBUS TCP, are also manufactured by ABB. This communication module integrates MODBUS TCP in to the 800M system, enabling the MODBUS TCP communication on the PLC. The communication modules are physically mounted to the side of the PM861. There are two Ethernet ports in the modules, but only the first channel is full-duplex and supports 10/100 Mb/s. The other

one is half-duplex and only 10Mb/s. The CI867 MODBUS TCP communication module also has LED indicators to indicate the status of the module.

The communication modules are powered through the connector of PM861, so the PM861 was powered by 10A power supply manufactured by Quint Power. Requirement for the supply was minimum 19,2 VDC for the PM861. After measuring the power supply supplied steady 24 VDC.



**Figure 11:** Components: CI867 (UHF) [A], CI867 (Wi-Fi) [B], PM861 [C] and 10A power supply [D].

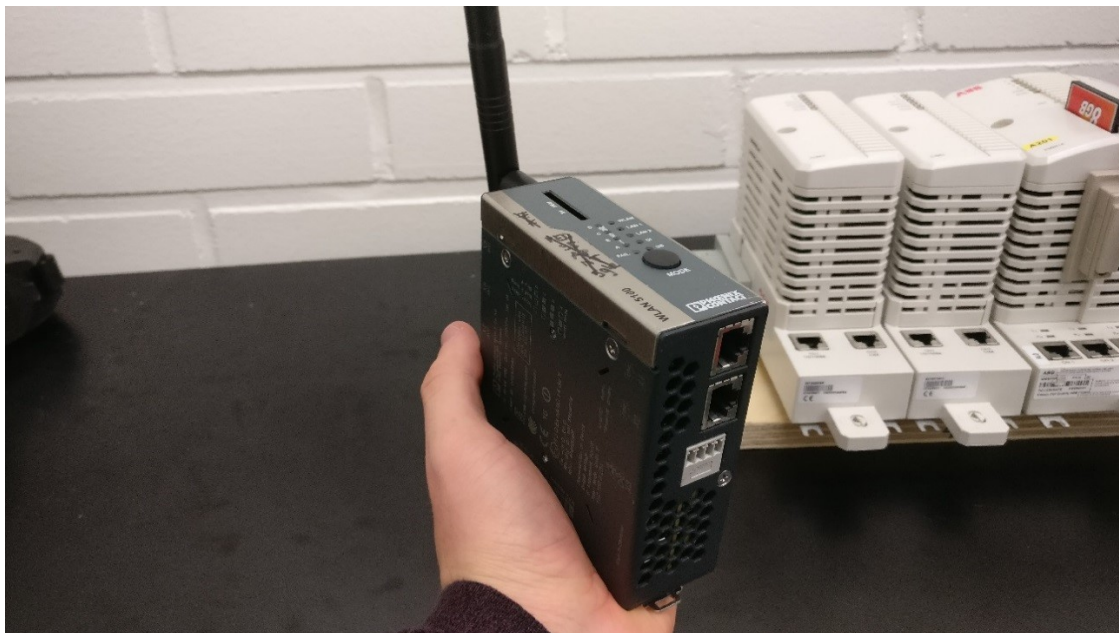
The chosen SDRs are Satel TA-26 UHF IP radios. It supports both IP and serial data low latency networking. The frequency range of the radio is between 360 to 485 MHz with Frequency Shift Keying (FSK) modulation and 360 to 445 MHz with Quadrature Amplitude Modulation (QAM) modulation. The modulation method effect on the range and how much data it can carry. The channel width is selectable in the Linux based operating system. The remote management is easy with the intuitive user interface NETCO or straight with the web browser but more about it in the *Subchapter 4.3*. Satel's IP radios also support all the way to AES-256 encryption and built-in firewall and user authentication. The selected IP radio has radio unit and optional central unit attached to the radio unit which adds the display and Ethernet interface to it. There are also S-232,

RS-422/48, USB-A and USB-B connectors. The radio frequency connector is a female-TNC.



**Figure 12:** UHF IP Radio manufactured by Satel. The antenna showing is not the one used in tests.

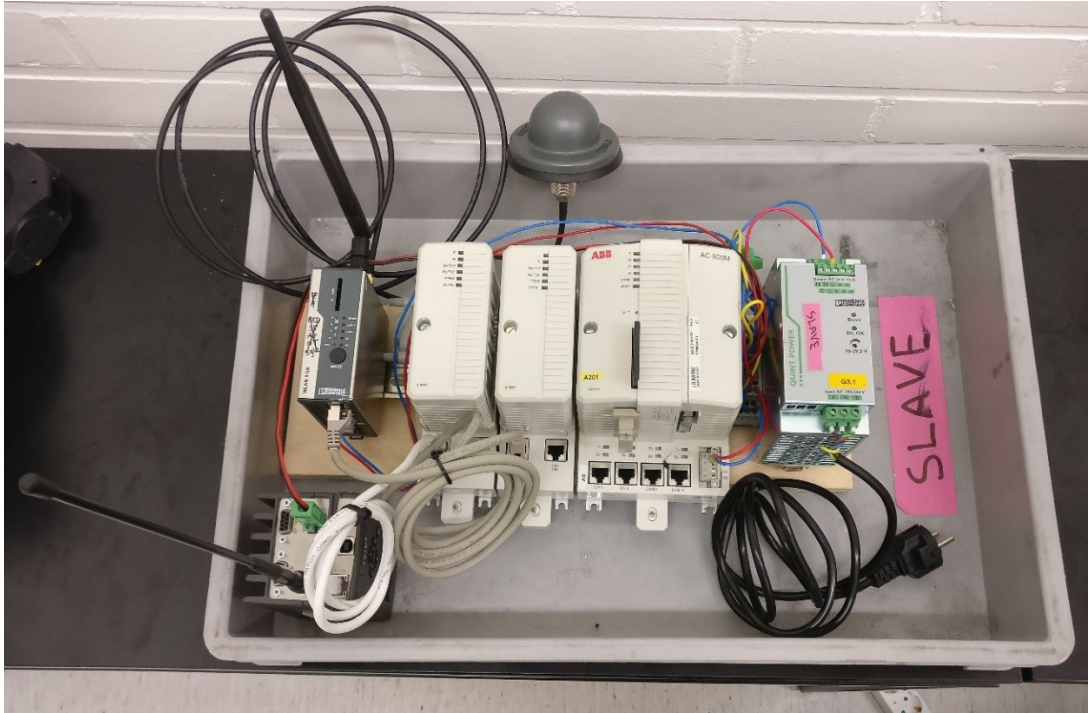
The Wi-Fi router is Phoenix Contact's FL WLAN 5100 which can operate as a AP or as a client. It supports WLAN 802.11 a, b, g and n standards. FL WLAN 5100 operates in the ISM band at 2,4 GHz or in the 5 GHz. The supports all the latest cyber security features according to the 802.11i standard: WPA2 and AES. The router is supported MIMO technology, so it supports connection of three different antennas at the same time. There are also two Ethernet ports for easy reconfiguration while connected to the wanted network. FL WLAN 5100 supports also SSH like the TA-26 IP radio. There are several status LED indicators and one push button for easy mode selection.



**Figure 13:** Industrial Wi-Fi router by Phoenix Contact. It has very compact size if you don't count the antenna.

In this test there were only dipole type antennas. Two antennas were connected to the Wi-Fi router. One +8 dB gain dipole antenna was connected straight to the back of the device and other 6 dB gain dipole antenna with coaxial cable 1 meter above the station (See *Figure 19*). The 8 dB gain antenna was TP-LINK TL-ANT2408CL and the +6 dB gain antenna was RAD-ISM-2459-ANT-FOOD-6-0-N from Phoenix Contact. The third dipole antenna used with UHF IP radio was K7153216, which has 4dB gain, produced by Gainflex.

The PM861 and two CI867 modules with the power supply were installed to the same DIN-rail as they would be in real life. Author cut board of wood where to install the DIN-rail for each station. This way it was easy to move the components and keep the test bench in order. Even a simplest setup like this can be messy with all the power cords and Ethernet cables without building the stations systematically from the beginning. Separating the stations and keeping the components of the same station close to each other also decreases the change of human error.



*Figure 14: Fully equipped station ready to be transported to the test area.*

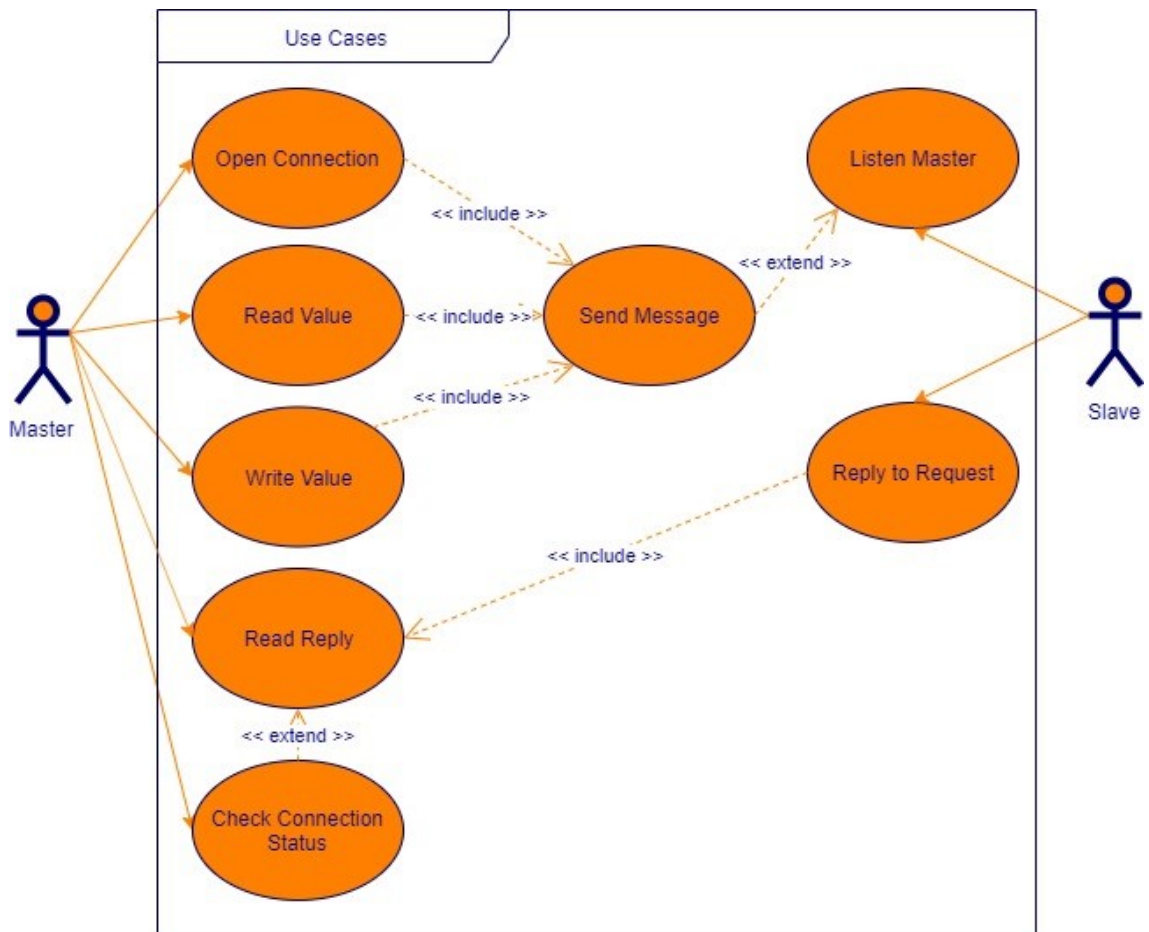
Marking up the hardware and using cables as exact length as possible clarifies the system even more and specially for a outsider who hasn't built it from the beginning.

## **4.2 Developed software with Compact Control Builder AC 800M**

The software development started by figuring out the use cases so the functionalities of the stations could be understood better and implemented with supported functions. Also, the network needed designing even before going deeper into the programming. Software for the master and the slave stations are developed with Compact Control Builder AC 800M which is the only option when developing software for ABB's controllers.

The other station is configured as a slave. Its role is more like to be just counterpart for the master that does all the functionalities to test the communication. When the master station tries to establish the connection, the request is forwarded through the TCP/IP connection to the Wi-Fi router and to the UHF IP radio which delivers the request to their counterparts where the request reaches the slave's PLC. Both connections need individual approval to open the MODBUS communication between the stations. After the connection is established the master stations can execute other functionalities. The

functionalities of the master and the slave are shown below in the use case diagram in *Figure 15*.



**Figure 15:** Use cases of the implemented stations.

The Master can open a connection and the slave just waits a message from master. After receiving a message, the slave replies to it. Master can read a value, write a value, read a reply and check a status of the connection. Before choosing the right libraries with the needed function blocks to implement the functionalities, it was needed to plan the IP addresses of the network as well.

The implemented stations were designed to be under different subnet. The chosen IP addresses was planned to be rational and have characteristics that could be deduced, but after multiple iterations of configuration and pretesting the IP addresses moulded to have different logic then it was originally planned. Below there is a *Table 5* which has all the IP address of both stations.

**Table 5: IP addresses of the system.**

	Master	Slave
PM861	172.16.1.30	172.16.2.40
CI867 Wi-Fi	172.16.1.31	172.16.2.41
CI867 UHF	172.16.1.32	172.16.2.42
Wi-Fi router	172.16.1.100	172.16.2.200
UHF IP radio	172.16.1.1	172.16.2.1

Programming language in Compact Control Builder AC 800M is Structured Text and also very graphical as well. Function blocks are summoned through table and the variables are listed in a table also. First author connected the needed ready made libraries to the applications. The most important library was MODBUSTCPCommLib 1.4-2 which enables the function block for MODBUS communication. Next it was time to declare variables and the paths to them via page "Access Variables". Correct way of referring to the other stations variables was well documented in the Control Builder. After the variables were set up, it was time to implement the use cases and build the hardware tree into the Control Builder. "Read Value" use case was implemented with automatic timer triggered redundancy function so the application will change the communication module according to the errors received. Communication link for "Write Value" use case however was controlled with manually switchable "vWriteEnable" variable. After these were done it was time to link the applications to the hardware and make the first cold start. The full code and variables can be seen on Appendix A. In the beginning of implementation phase before the wireless communication was configured the system was pretested via Ethernet cables.

### **4.3 Configuration of the wireless network devices**

Configuration of the Satel UHF IP radios and the FL 5100 WLAN routers were done in web interfaces with a help of the documentation provided by the vendors of the devices. Satel also provided a licence for the centralized network configuration application, NETCO, to configurate the radios. Both devices and their counterparts in the network were configurated with the same state of mind that the testing will be done outdoors, to get as low latency as possible and to get as strong signal as possible. Short reminder to readers that do not ever turn on RF devices without proper antennas connected and reading the manual. Also, the author recommends to update firmwares in the beginning of implementation. Specially update the firmware if you are not the first user of the component.

In the first place configuration of IP radios were done manually with the web browser, and the radios could ping each other but they didn't work as part of the whole system. So Satel recommended me to use NETCO to configurate the network. NETCO's advantage compared to the web interface is automatic error checking and better graphical user interface. *Figure 16* and *Figure 17* show the outlooks of the both interfaces.

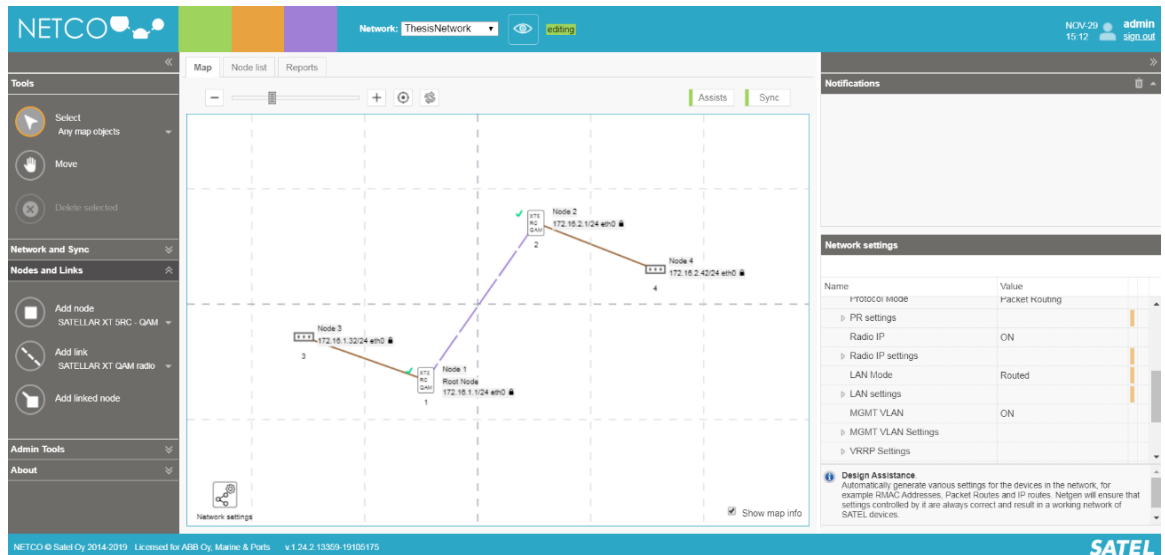
The screenshot shows the Satel web browser interface. At the top, there is a navigation menu with tabs: Modem Settings, Modem Info, Routing, Diagnostics, Firmware Updater, NMS Import, Tools, Encryption, Logs, Administration, and Logout. Below the menu is a dark sidebar with a 'Go to Settings Wizard' link and a list of settings categories: Network Protocol Mode, Radio (selected), Serial Connector Configuration, Data Port Settings, Serial Data Flow Control, Packet Mode Radio Access Control, General, Services, Commands, Remote Devices, SNMP, Time Control, ATPC, NMS Modbus, and Testing And Calibration. At the bottom of the sidebar are 'Reload NMS values (NOTE)' and a 'Reload' button. The main content area is titled 'Node 2' and displays status information: 'Status: Voltage: 24.4 V RSSI: -128 dBm' and 'Time: 2019-11-26 17:00:43'. Below this is a configuration table with various radio parameters and their values:

TX Frequency	428.52500	MHz
RX Frequency	428.52500	MHz
RF Output Power	100 mW	
Signal Threshold	-100	dBm
Trellis Coding	ON	
Mobile Mode	OFF	
Auto QAM SNR Level Adjust	+0	dB
Over-the-Air Encryption	ON	
Encryption Type	AES-256	
Encryption Compatibility Mode	Legacy Mode	
Channel Spacing	25.00 kHz	
Modulation	8-QAM	
Link Specific Modulation	OFF	

At the bottom of the configuration area is an 'Apply Changes' button.

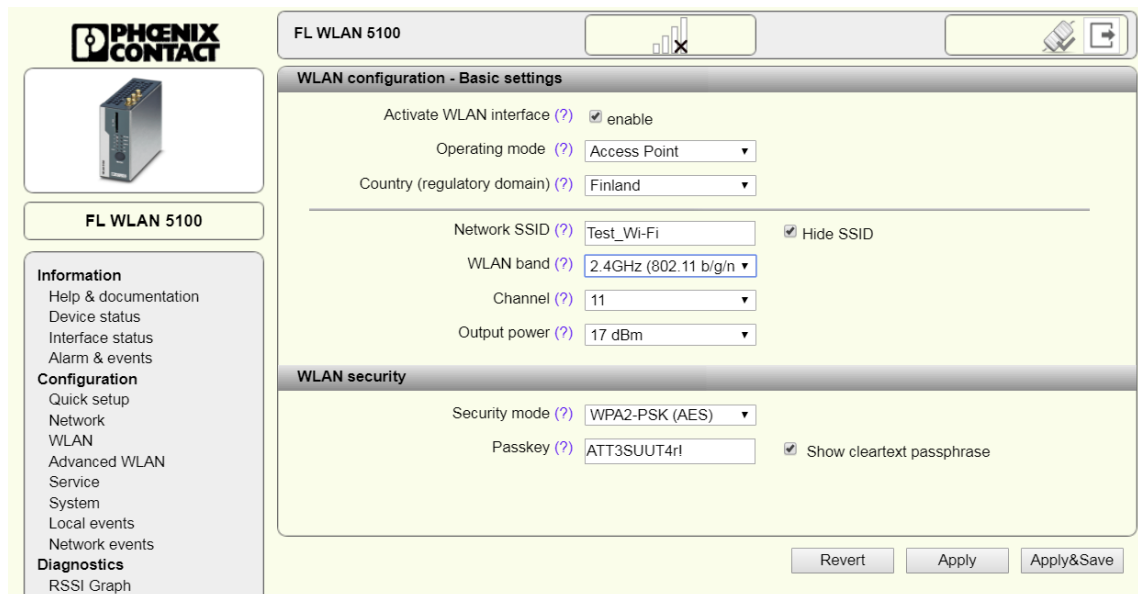
**Figure 16:** Web browser interface for Satel IP radio.

Radios were set on 428,525 MHz for transmitting and receiving messages because company Satel Oy had rights for that specific frequency and allowed the author to use it for the thesis. The output power was kept in the lowest possible level (100 mW), because still the radio's output power was double compared to the Wi-Fi routers' maximum output power which is only 50 mW. The AES-256 encryption in the communication was enabled. 8-QAM modulation was chosen because it was evaluated to be enough to carry out the messages but also has a decent range. Also, Robust Header Compression (ROHC) was enabled to decrease the latency by compressing the IP and TCP headers.



**Figure 17:** Centralized network configuration application, NETCO by Satel.

By drawing the network and choosing right devices in NETCO, the application creates automatically the IP addresses and IP routes for radios, so they know where to start asking the right MAC addresses to deliver the message from station to another. NETCO also makes the uploading easy and warns you if you accidentally mixed the devices compared to the information of last upload. The upload happens via USB-A to USB-B cable.



**Figure 18:** Web browser interface to configure the FL WLAN 5100 router.

The Wi-Fi was easier to set up because less options and the devices were more familiar to the author. Master station's Wi-Fi router was configured first and set as an access point with hidden SSID and security protocol WPA2 was enabled. Also, the login information was changed and the static IP address set to 172.16.1.100. The output

power was set to maximum level to 17dB which is 50mW to correspond as close as possible with the IP radio's output power. WLAN band was set to 2,4 GHz. There was also option to choose which one(s) of the antenna ports are used, two ports were selected. All the same options were chosen for the Wi-Fi router in the slave station except the IP address and the operating mode.

#### **4.4 Test setup**

The setup to be tested consisted of two stations, master and slave station. On top of these stations there was a need of extra components to execute the tests. In a real-life implemented communication of ACS would need some sort of monitoring system and it could be wireless as well but in this thesis the control and monitoring were done with cables. Also, the stations got improvised protection against environment and easily movable beds.



**Figure 19:** Master station on test bench wrapped to a homemade weather protection with long power cord and two Ethernet cables.

The author used two PCs for the testing. Other one was for the monitoring of the communication between the stations and other just to control the master PM861. There was no need for a wire connection to the moveable slave station. The PCs were connected to the master station, which was stationary, with two Ethernet cables. The monitoring of both SDR and Wi-Fi communication was done through a switch with a mirror port (*Figure 20*) and using application Wireshark. Wireshark is opensource application for analyse communication. The author just needed to add the filters according to the IP addresses and the monitoring was trivial after that.



**Figure 20:** Test equipment: earth leakage circuit breaker and switch with a mirror port.

Not all the extra components were needed for the testing itself. On *Figure 20*, presented earth leakage circuit breaker is crucial component for safe testing. Challenging weather conditions and self-made weather protection are huge risks for components and people working with the stations. These types of solutions are easily forgotten and safety should always come first. Also warning signs about the testing were placed and the power cords were fasten safely with duct tape to increase the change of fell or detachment.

## 5. TESTS AND RESULTS

This chapter is divided to two subchapters. The first subchapter presents the tests that verifies the functionality and measures performance of the implemented system in *Chapter 4*. The second part of this chapter is for the results of the presented tests in this chapter. The test that verifies the functionality of the implemented system is qualitative investigation and the tests of the communication latency and the signal strength are quantitative. At the end of the chapter, there is a summarization of features of the solution.

### 5.1 Tests

The objectives of the tests were the verification of seamless redundant wireless communication between ABB's 800M controllers, measure the latency of the communication with UHF radios and Wi-Fi and measure the received signal strength indication (RSSI) of both technologies on different distances.

All the tests were done in same environment and with all the same test tools mentioned in the previous chapter. The tests were executed on land. The set of tests started by moving the stations into their first position, where the bilateral distance between the stations were 50 meters and there was a continuous LOS. Both stations were turned on and they downloaded their applications directly from the memory cards installed into them. Control and monitoring of the system was done from laptops that were connected straight to the master PLC to control the statuses of the master station and to the switch which had mirror port to peer the communication between wireless communication devices and C1867s.

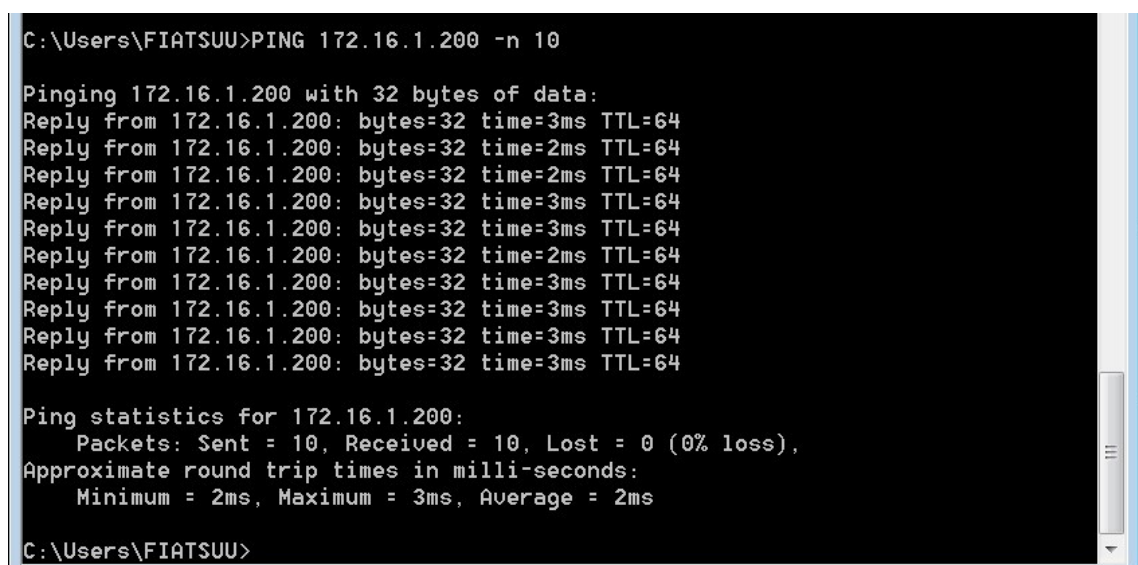
In the beginning, the MODBUS TCP communication between stations was confirmed and tested with read and write functionalities of the program. After confirmation of working communication, there was systematic failure mode and effects analysis (FMEA) done. First the Ethernet cables were removed one at the time and placed back after analysing, if the communication worked via the medium that didn't have an error. This kind of test simulates the break of a cable. After broken cable simulation was time to simulate blackout in one wireless device at the time. Blackout simulation tests the redundancy again but also checks if the system recovers from it. Blackout simulation was performed also for the controllers as well.

After FMEA there were tests for RSSI and latency as function of distance for both SDR and Wi-Fi. There was an assumption that the range of Wi-Fi would be less than 1 kilometer. Because of lack of test time and time consumed per set of tests and documentation at every range was close to half an hour, the increase of range after every set was decided to be 50 meters.

Both Wi-Fi router and the Satel's UHF IP radio can create the received signal strength indication and show it on the provided web browser interface. This UHF IP radio model can also create a .csv file that can be interpret with Microsoft Excel. The analyse of the timestamps and the RSSI is much more accurate with .csv file than with small graph in the web browser interface. Also, documentation is easier with the .csv file.

When the measurement of the RSSI was on action, there was need to be sure that there was no physical interference around the stations. Even an object size of a human effect on the RSSI. The devices measure the RSSI automatically and the traffic between the stations does not effect on the result. Some of the effective factors are listed on *Subchapter 2.4*.

Latency tests were performed with command prompt and Wireshark. Wireshark produced a .pcapng file for documentation and command prompt was the tool to perform a ping. The idea of the test was to compare the latencies between the devices and the increase of it by the distance. In every case there was 32 bytes sent 10 times and minimum, maximum and the average time on air was calculated. The results of command prompt are rounder so the accurate results needed to be calculated with the timestamps from Wireshark. Also, the amount of lost packages during the test was documented.



```
C:\Users\FIATSUU>PING 172.16.1.200 -n 10

Pinging 172.16.1.200 with 32 bytes of data:
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64
Reply from 172.16.1.200: bytes=32 time=2ms TTL=64
Reply from 172.16.1.200: bytes=32 time=2ms TTL=64
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64
Reply from 172.16.1.200: bytes=32 time=2ms TTL=64
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64
Reply from 172.16.1.200: bytes=32 time=3ms TTL=64

Ping statistics for 172.16.1.200:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\FIATSUU>
```

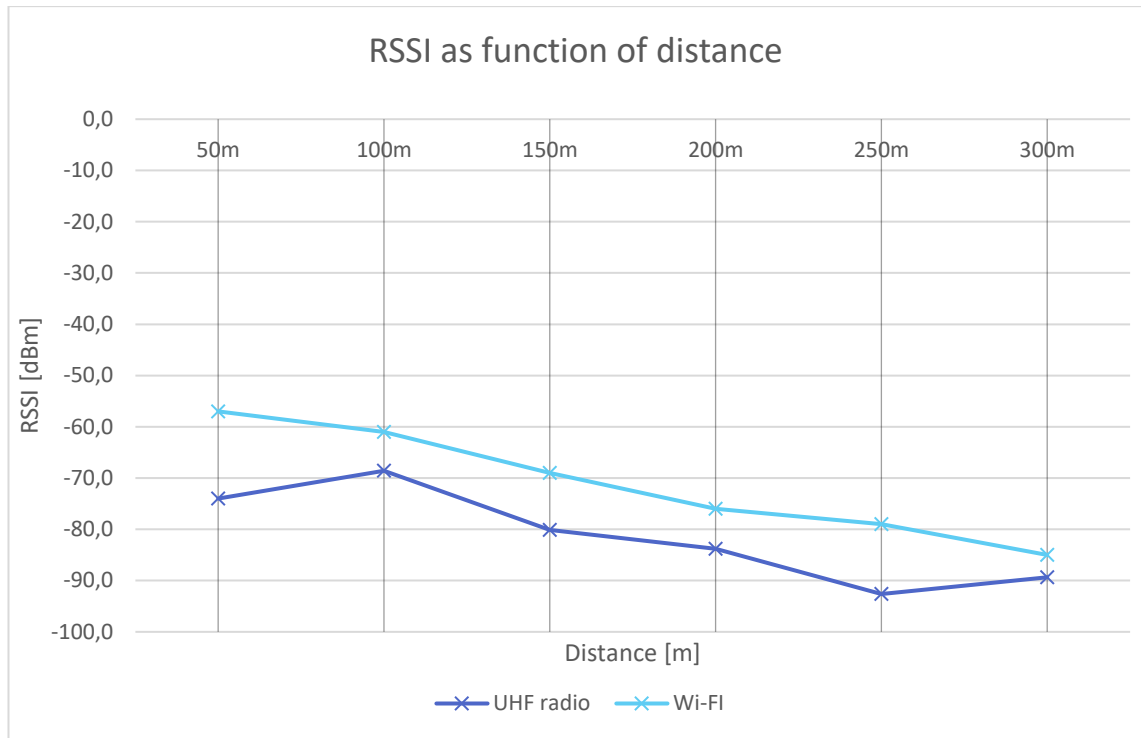
*Figure 21: Pinging the slave station with Windows command prompt.*

By knowing the IP address of the counter station's controller, it is possible to ping it. The command can be seen on *Figure 21*.

## 5.2 Results

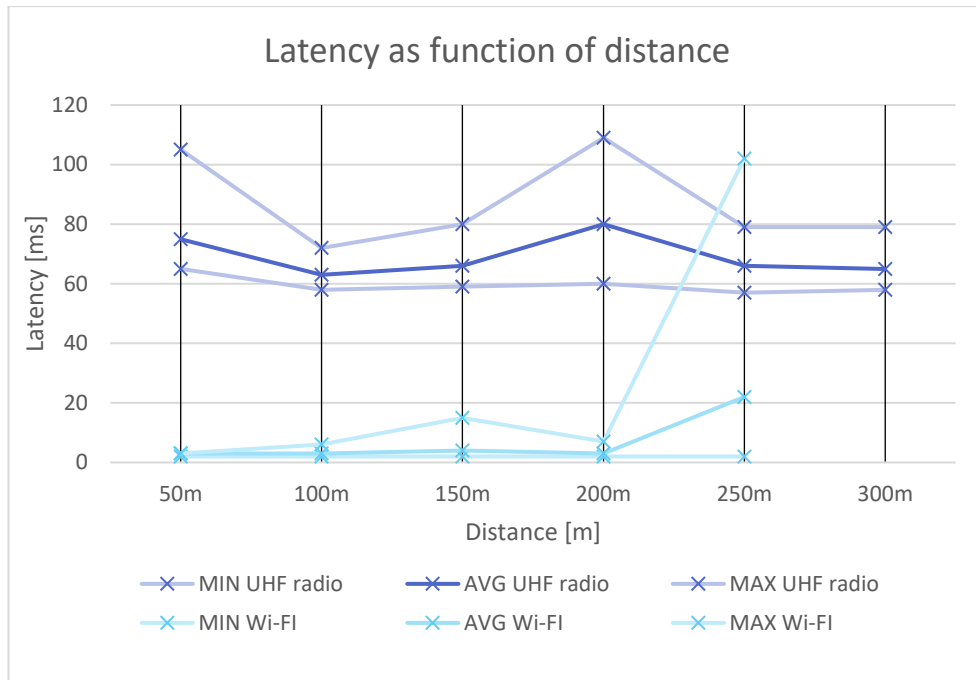
Failure mode and effects analysis pointed the correct functionalities of the stations. The MODBUS communication was working redundantly if the other wireless communication method went down. Even after full blackout test of an entire station, the tripped station restarted program and established the connection as it was designed. The implementation of a MODBUS TCP communication went successfully and after FMEA test it can be said that the communication protocol is very suitable and robust for ABB's controllers with ACS.

The received signal strength indication as function of distance is important when comparing the technologies from the maritime aspect. The threshold of decrease of RSSI differs between devices and the gain of the antennas varies. The antennas were similar by type but still not exactly same. Both technologies still had proper antenna setups for the use cases. Anyway, with the values it's possible to extrapolate and have an estimation of the maximum distance with the tested devices in that specific environment and conditions. In *Figure 22*, the Wi-Fi router has higher values than UHF radio. Higher values are better but as a reminder, the threshold of decrease varies and is usually the aspect that spot the difference between professional and commercial products from each other. Also, noticeable phenomenon is the decrease of RSSI by increase of distance is very similar between the technologies.



**Figure 22:** RSSI as function of distance.

However, the RSSI values of Wi-Fi are better than UHF's in *Figure 22*, the maximum range of Wi-Fi is shorter than the maximum range of UHF radio for TCP communication. This statement can be made by examining the following figure. The latency as function of distance on *Figure 23* shows the minimum, maximum and average time on air of the 32 byte packet.



**Figure 23:** Time on air as function of distance.

Wi-Fi is much faster and variation is smaller compared to UHF radio on distances below 250 meters. After 250 meters the TCP communication was not possible with Wi-Fi router. The upcoming failure was expected after noticing the huge increase in the latency on 250 meters on maximum time on air. In the end the Wi-Fi could not receive TCP packets on 300 meters even it could still measure the RSSI.

The latency of UHF radio varies a little bit but it's still in a tolerable scale for maritime and easily sufficient stated by the mentor of the author. The what is worth of mention is that in these distances the average latency didn't decrease notable or at all when TCP communication was run through Satel's UHF IP radios.

**Table 6: Summarized features of the solution.**

<b>Technology</b>	<b>Wi-Fi</b>	<b>SDR</b>
Router / IP Radio Manufacturer Model	Phoenix Contact FL WLAN 5100	SATEL TA-26
Antenna(s)	+6dB RAD-ISM-2459-ANT-FOOD-6-0-N, +8dB TL-ANT2408CL	+4dB K7153216
Modulation	MIMO-OFDM	8-QAM
Encryption	AES-128	AES-256
Frequency	≈2400 MHz	428,525 MHz
RF output power (used/max)	50mW / 50mW	100mW / 5000mW
Redundancy	YES	YES
Failure recovery	YES	YES
Web UI	YES	YES
Effective range by tests	250m	+300m

Here, in the *Table 6*, are all the main features of the implemented and tested solution. Redundancy means in this table that the technology was suitable for the redundant configuration and performed as designed during tests. Both technologies recovered perfectly after power failure test. Worth mentioning is also that both manufacturers of the chosen router and IP radio offer a configuration through web-based user interface. Other rows of the *Table 6* are explained in previous chapters.

## 6. CONCLUSIONS

In this conclusions chapter author summarizes the work done in the thesis and discuss about the results and possibilities for future research. The research questions are answered, and end results of the implementation is compared to the objectives presented in *Chapter 1*.

After comprehensive theory review, the proposed system for this product development project of wireless communication on ACS included two wireless technologies: SDR on UHF frequencies and Wi-Fi. UHF radios and the Wi-Fi routers were connected to two ABB's 800M controllers, which were executing the roles of the two stations needed for automated charging between a vessel and a port. Communication protocol was chosen to be MODBUS TCP. Implementation phase prove that chosen wireless technologies are fulfilling regulations of maritime and cyber security requirements of today.

SOLAS is an international maritime treaty that ties all the regulations together and the classification societies base their own rulebooks to SOLAS. Different shipping companies use different classification societies who again has different methods to interpret the SOLAS. Now the regulations for wireless communication is little dragging behind the needs of engineering departments of marine industry. There are many easily definable requirements which are there because of the harsh but known environment of seas, for example the IP rating for the used components. However, there are also lot of requirements for methods and protocols of marine communication which are completely outdated. The automated charging systems are not the only use cases in marine industry where state-of-the-art wireless communication applications are used so to keep up with the development all the stakeholders should focus more resources for research and training their personnel about the latest wireless communication technologies to update the methods for testing, verifying and documentation.

Signal integrity, confidentiality and availability are the biggest information security aspects with wireless communication in industrial applications. Both tested wireless technologies are using the latest features, e.g. AES-encryption standard, to fulfil the present requirements. The latest features however are outdated fast, if an owner doesn't update software and hardware as planned. Today there are multiple motives and methods for criminal organizations to find of the cyber security vulnerabilities. When a vessel is under a cyber attack, the person or organization behind it is probably professional, so communication plans should be done and tested way before the first

attack. Even multiple methods of communication and latest security features don't guarantee immunity against cyber attacks, so crucial operations of a vessel should be able to be completed without any communications. Now 2020 is the last moment to wake up and comprehend that cyber security is crucial part of risk management of maritime and it's everyone's job to assess and mitigate cyber security risks.

The most important performance indicators of wireless communication on ACS are received signal strength indication and latency as functions of distance. The Wi-Fi setup had a significantly better latency than UHF radios in their operational range. However, the range of tested Wi-Fi setup was only 250 meters which doesn't give a vessel and a port enough preparation time to maximise the charging time. Tests made in this thesis didn't confirm the maximum operational range of UHF radios with the antenna setup in question, but the alleged range from the manufacturer is multiple kilometres. The latency of UHF radios was bigger compared to Wi-Fi but within requirements. As a conclusion and an answer to the main question of this thesis, UHF radios are the most suitable option for wireless communication on automated charging systems in marine industry.

For the future product development, the author suggests focussing the research on SDR radios on UHF frequencies and the antenna setups to improve the signal quality on marine environment. The tests should also be done in marine environment for more accurate results and to test the suitability of the components in actual operation environment. Compatibility with actual ACS components, harsh weather conditions and requirements of a real harbour are the factors that were not tested in this thesis. Also, the requirements and use cases are transforming fast so fresh overview of 5G technology is mandatory for future research.

## REFERENCES

- [1] Organization IM. Low carbon shipping and air pollution control [Internet]. [cited 2020 May]. Available from: <http://www.imo.org/en/MediaCentre/HotTopics/GHG/Pages/default.aspx>
- [2] Seatrade, Liang LH. Shipping takes aim at battery-powered future [Internet]. 2019 [cited 2020 May]. Available from: <https://www.seatrade-maritime.com/opinions-analysis/shipping-takes-aim-battery-powered-future>
- [3] Sen SK. Fieldbus and networking in process automation. Boca Raton, Florida: CRC Press; 2014.
- [4] Kim H. Wireless communications systems design. Chichester, West Sussex, United Kingdom: Wiley; 2015.
- [5] Zhang KQT. Wireless communications : principles, theory and methodology. Chichester, England: Wiley; 2016.
- [6] Cooklev T. Wireless communication standards : a study of IEEE 802.11, 802.15, and 802.16. New York: Standards Information Network, IEEE Press; 2004.
- [7] Alliance W-F. Wi-Fi User Guide [Internet]. [cited 2019]. Available from: [https://www.Wi-Fi.org/download.php?file=/sites/default/files/private/Generational\\_Wi-Fi\\_User\\_Guide\\_20181003.pdf](https://www.Wi-Fi.org/download.php?file=/sites/default/files/private/Generational_Wi-Fi_User_Guide_20181003.pdf)
- [8] ABB, Räsänen J-E, Pohjanheimo P. Automatic shore connection enabled by the ABB Robotic solution [Internet]. Available from: <https://new.abb.com/marine/generations/technical-insight/short-sea-solution>
- [9] Harkins D. Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks. IEEE; 2008. p. 839–44.
- [10] Garcia D, Barber R, Salichs MA. Design and development of a wireless emergency start and stop system for robots. SCITEPRESS; 2014. p. 223–30.
- [11] Thomesse J-P. Fieldbus Technology and Industrial Automation. IEEE; 2005. p. 651–3.
- [12] PROCENTEC. What is PROFIBUS DP? [Internet]. [cited 2019]. Available from: <https://procentec.com/content/what-is-profibus-dp/>
- [13] ABB. AC 800M Communication Protocols. 2010; Available from: [https://library.e.abb.com/public/6a203d3016146ec6c12578570041d62a/3BSE035982-510\\_-\\_en\\_AC\\_800M\\_5.1\\_Communication\\_Protocols.pdf](https://library.e.abb.com/public/6a203d3016146ec6c12578570041d62a/3BSE035982-510_-_en_AC_800M_5.1_Communication_Protocols.pdf)

- [14] Powell J, Vandelinde H. Catching the process fieldbus an introduction to PROFIBUS for process automation. New York, N.Y.] (222 East 46th Street, New York, NY 10017): Momentum Press; 2013.
- [15] IEEE Std 802.3-2018 (Revision of IEEE Std 802.3-2015). IEEE; 2018.
- [16] University P. PROFINET Diagnostics Suite – Part 1 of 3 [Internet]. [cited 2019]. Available from: <https://profinetuniversity.com/profinet-diagnostics/profinet-diagnostics-suite-part-1-3/>
- [17] John KH, Tiegelkamp M. IEC 61131-3: Programming Industrial Automation Systems Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids. 2nd ed. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010.
- [18] Penttinen JTJ. The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems: Engineering Guidelines for Fixed, Mobile and Satellite Systems. 1st ed. Wiley; 2015.
- [19] IPv6. UDP – USER DATAGRAM PROTOCOL [Internet]. [cited 2019]. Available from: <https://www.ipv6.com/general/udp-user-datagram-protocol/>
- [20] SATEL. SATEL XPRS RADIO ROUTER RADIO UNIT SATELLAR XT 5R AND XT 5RC USER GUIDE VERSION 2.0 [Internet]. [cited 2019]. Available from: [https://www.satel.com/wp-content/uploads/2019/08/SATEL-USER-GUIDE-RU\\_V2\\_0.pdf](https://www.satel.com/wp-content/uploads/2019/08/SATEL-USER-GUIDE-RU_V2_0.pdf)
- [21] Baccala B. IP Packet Structure [Internet]. [cited 2019]. Available from: <https://www.freesoft.org/CIE/Course/Section3/7.htm>
- [22] Alliance W-F. Wi-Fi User Guide [Internet]. [cited 2019]. Available from: [4] [https://www.Wi-Fi.org/download.php?file=/sites/default/files/private/Generational\\_Wi-Fi\\_User\\_Guide\\_20181003.pdf](https://www.Wi-Fi.org/download.php?file=/sites/default/files/private/Generational_Wi-Fi_User_Guide_20181003.pdf)
- [23] Koziol M. Everything you need to know about wpa3 [Internet]. 2018 [cited 2019]. Available from: <https://spectrum.ieee.org/tech-talk/telecom/security/everything-you-need-to-know-about-wpa3>
- [24] Certification of Wi-Fi Alliance [Internet]. 2019 [cited 2019]. Available from: <https://www.wi-fi.org/certification>
- [25] Wi-Fi CERTIFIED 6 TM : A new era for Wi-Fi [Internet]. Wi-Fi Alliance; 2019. Available from: [https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi\\_CERTIFIED\\_6\\_%20Highlights\\_201909.pdf](https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_CERTIFIED_6_%20Highlights_201909.pdf)
- [26] Sesia S, Toufik I, Baker M (Matthew PJ). LTE--the UMTS long term evolution from theory to practice. 2nd ed. Chichester, West Sussex, U.K. ; Wiley; 2011.

- [27] Alliance W-F. Wi-Fi Direct™ [Internet]. [cited 2019]. Available from: <https://www.wi-fi.org/wi-fi-direct>
- [28] Guide to the Radio Equipment Directive 2014/53/EU [Internet]. Dec 19, 2018. Available from: <http://ec.europa.eu/DocsRoom/documents/33162>
- [29] Chen ZN, Xianming Q, See T, Toh W. Antennas for WiFi Connectivity. 2012;100:2322–9.
- [30] Mäkinen S. Poliisi löysi GPS-taajuutta häirinneen laitteen – mies halusi esitellä naapurilleen laitteen toimintaa. 2016; Available from: <https://www.iltalehti.fi/uutiset/a/2016061021708589>
- [31] Gupta NC (Naresh C. Inside Bluetooth low energy. Boston: Artech House; 2013.
- [32] SIG. Bluetooth SIG, technology [Internet]. [cited 2019]. Available from: <https://www.bluetooth.com/bluetooth-technology>
- [33] SIG. Bluetooth 5. Available from: [https://3pl46c46ctx02p7rzdsvsg21-wpen-gine.netdna-ssl.com/wp-content/uploads/2019/03/Bluetooth\\_5-FINAL.pdf](https://3pl46c46ctx02p7rzdsvsg21-wpen-gine.netdna-ssl.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf)
- [34] De Morais Cordeiro C, Agrawal DP. Ad Hoc & Sensor Networks: Theory and Applications [Internet]. World Scientific Publishing Company; 2006. Available from: <https://books.google.fi/books?id=D24L4ygKFngC>
- [35] Vainio JT. Bluetooth Security. Helsinki University; 2000.
- [36] Pu D, Wyglinski AM. Digital communication systems engineering with software-defined radio. Boston: Artech House; 2013.
- [37] RACOM. RipEX – Radio modem [Internet]. [cited 2019]. Available from: [https://www.racom.eu/eng/products/radio-modem-ripex.html#features\\_ethernet](https://www.racom.eu/eng/products/radio-modem-ripex.html#features_ethernet)
- [38] Machado-Fernández JR. Software Defined Radio: Basic Principles and Applications. Universidad Pedagógica y Tecnológica de Colombia; 2015;24:79–96.
- [39] Forum W. WiMAX Mobile 4G [Internet]. [cited 2019]. Available from: <http://wimax-forum.org/Page/Initiatives/WiMAX-Advanced>
- [40] Penttinen JTJ. Wireless LAN and Evolution. 1st ed. Wiley; 2015.
- [41] Tonder T. Antenna system components, SATEL. SATEL; 2019.
- [42] Antenna MP. Omnidirectional Antenna Radiation Patterns Explained [Internet]. 2019. Available from: <https://www.mpantenna.com/omnidirectional-antenna-radiation-patterns/Stutzman WL>.
- [43] Antenna theory and design. 3rd ed. Hoboken (NJ): John Wiley & Sons; 2011.

- [44] Bartz R. Parabolic antenna [Internet]. 2008. Available from: [https://en.wikipedia.org/wiki/Parabolic\\_antenna](https://en.wikipedia.org/wiki/Parabolic_antenna)
- [45] Sähköturvallisuuden edistämiskeskus STEK ry. IP-luokitus [Internet]. [cited 2020]. Available from: <https://stek.fi/perustietoa-sahkosta/sahkojarjestelmat/ip-luokitus/>
- [46] Organization IM. International Convention for Safety of Life at Sea SOLAS Consolidated edition 2014 . 2014th ed. IMO.
- [47] Heikkinen S. Cross-cultural co-operation between Russian state authorities and a Finnish firm : the case study of ABB Marine and Ports and Russian classification society. Itä-Suomen yliopisto; 2017.
- [48] Lehto M, Kähkönen A. Kyberturvallisuuden kansallinen osaaminen. 2015;20:1–58. Available from: [https://www.jyu.fi/it/tutkimus/202015\\_Kyber\\_kansallinen\\_osaaminen\\_VERKKO.pdf/view](https://www.jyu.fi/it/tutkimus/202015_Kyber_kansallinen_osaaminen_VERKKO.pdf/view)
- [49] Jorgensen J. ABS CyberSafetyTM. 2016;1–19. Available from: [http://www.socp.us/images.html?file\\_id=40UY2UEI78k%3D](http://www.socp.us/images.html?file_id=40UY2UEI78k%3D)
- [50] Kumar., B Swapan .Debnath,Ajay. /z-wcorg/ [Internet]. San Diego: Elsevier Science & Technology; 2019. Available from: <https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5788502>
- [51] F-Secure Oyj. Back Orifice [Internet]. Available from: <https://www.f-secure.com/v-descs/backori.shtml>
- [52] Hassan SS, Bibon SD, Hossain MS, Atiquzzaman M. Security threats in Bluetooth technology. Elsevier Ltd; 2018;74:308–22.
- [53] De Pellegrini F, Miorandi D, Vitturi S, Zanella A. On the use of wireless networks at low level of factory automation systems. IEEE; 2006;2:129–43.
- [54] Journals I, Dhiman1 D. WLAN Security Issues and Solutions. Figshare; 2014.
- [55] Cabric M. Chapter 11 - Confidentiality, Integrity, and Availability. Elsevier Inc; 2015. p. 185–200.
- [56] Spill D, Bittau A. Bluetooth frequency hopping sequence [Internet]. [cited 2019]. Available from: [https://www.usenix.org/legacy/event/woot07/tech/full\\_papers/spill/spill\\_html/index.html](https://www.usenix.org/legacy/event/woot07/tech/full_papers/spill/spill_html/index.html)
- [57] Ristola P. Ensimmäisen kerran maailmassa maantielautta kulki ilman ihmisen ohjausta – katso videolta, miten matka Paraisilta Nauvoon sujui. [cited 2019]; Available from: <https://yle.fi/uutiset/3-10536482>
- [58] Wireless charger | Wärtsilä [Internet]. 2018. Available from: <https://www.youtube.com/watch?v=3p8y0bKvrz8>

- [59] ABB. ABB toteutti uraauurtavan etäohjatun matkustaja-aluksen testiajon Helsingissä [Internet]. 2018 [cited 2019]. Available from: <https://new.abb.com/news/fi/detail/11652/abb-toteutti-uraaurtavan-etaohjatun-matkustaja-aluksen-testiajon-helsingissa>
- [60] ABB. ForSea - Zero Emission operation [Internet]. [cited 2019]. Available from: <https://new.abb.com/marine/marine-references/forsea>
- [61] Rolls-Royce. Rolls-Royce and Finferries demonstrate world's first Fully Autonomous Ferry [Internet]. 2018 [cited 2019]. Available from: <https://www.rolls-royce.com/media/press-releases/2018/03-12-2018-rr-and-finferries-demonstrate-worlds-first-fully-autonomous-ferry.aspx>
- [62] Kongsberg. AUTONOMOUS SHIP PROJECT, KEY FACTS ABOUT YARA BIRKELAND [Internet]. [cited 2019]. Available from: <https://www.kongsberg.com/maritime/support/themes/autonomous-ship-project-key-facts-about-yara-birkeland/>
- [63] Aittokoski H. Tässä on liikenteen vallankumous: Norjan rannikolla seilaa pian "aavelaiva". 2018 [cited 2019]; Available from: <https://www.hs.fi/ulkomaat/art-2000005832922.html>
- [64] MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b [Internet]. Available from: [http://www.modbus.org/docs/Modbus\\_Application\\_Protocol\\_V1\\_1b.pdf](http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf)

## APPENDIX A: MASTER STATION CODE

The code produced with Compact Control Builder AC 800M for master station represented under in appendix A.

### Master Station

*Table 7: Parameters of the master station.*

	Name	Data Type	Direction	FD Port	Initial value	Description
1	pSlaveChannel1	string[40]	unspecified	yes	'1'	Place number in order of device tree.
2	pSlaveChannel2	string[40]	unspecified	yes	'2'	
3	pStartAddressRead	string[40]	unspecified	yes	'%MW0'	Refer to the Access Variables

*Table 8: Variables of the master station.*

	Name	Data Type	Attributes	Initial value	Description
1	vFirstScan	bool	retain	true	
2	vEnableCommand	bool	retain		
3	vWifi_ip	bool	retain		
4	vRedundancy	bool	retain	false	
5	vConnectAll	bool	retain		
6	vMBTCPValid1	bool	retain		
7	vMBTCPValid2	bool	retain		
8	vMBTCPError1	bool	retain		Connecting error
9	vMBTCPError2	bool	retain		Connecting error
10	vMBTCPStatus1	dint	retain		
11	vMBTCPStatus2	dint	retain		
12	vID1	Comm_Channel_MBTCP	nosort		
13	vID2	Comm_Channel_MBTCP	nosort		
14	vReqRead	bool	retain	true	
15	vSlaveAddress1	string[4]	retain	'1.41'	
16	vSlaveAddress2	string[4]	retain	'1.42'	
17	vReadNdr1	bool	retain		
18	vReadNdr2	bool	retain		
19	vReadMBTCPReadError1	bool	retain		
20	vReadMBTCPReadError2	bool	retain		
21	vReadStatus1	dint	retain		
22	vReadStatus2	dint	retain		
23	vReply	Modbus_read_type	retain		
24	vWrite	Modbus_write_type	retain		
25	vRedundancyTimer	Timer	retain		
26	vRedundancyTime	time	retain	t#5s	Change communication tech
27	vReadError	bool	retain	false	Reading error from both
28	vWriteReq	bool	retain	true	
29	vWriteDone1	bool	retain		
30	vWriteDone2	bool	retain		
31	vWriteMBTCPError1	bool	retain		
32	vWriteMBTCPError2	bool	retain		
33	vWriteStatus1	dint	retain	1	

	Name	Data Type	Attributes	Initial value	Description
34	vWriteStatus2	dint	retain	1	
35	vWriteEnable1	bool	retain	true	

**Table 9:** Used Function blocks in the application of master station.

	Name	Function Block Type	Task Connection	Description
1	TestStatusRead1SR	SR		
2	TestStatusRead2SR	SR		
3	MTRRead1	MBTCPRead[1]		
4	MTRRead2	MBTCPRead[1]		
5	MBTCPConnect1	MBTCPConnect		
6	MBTCPConnect2	MBTCPConnect		
7	MTWrite1	MBTCPWrite[1]		
8	MTWrite2	MBTCPWrite[1]		

**Start\_Code:**

```
(*
29.11.2019
Atte Suutari
Master's thesis
Start code
*)
IF (vFirstScan) then
    vFirstScan :=false;
    MBTCPConnect1.Channel := pSlaveChannel1;
    MBTCPConnect1.Partner := vSlaveAddress1 ;
    MBTCPConnect2.Channel := pSlaveChannel2;
    MBTCPConnect2.Partner := vSlaveAddress2;
END_IF;
```

**Connect:**

```
(*
MODBUS TCP Connect:
*)

vConnectAll := NOT vFirstScan;

MBTCPConnect1( En_C := vConnectAll,
```

```

Channel := MBTCPConnect1.Channel,
Partner := MBTCPConnect1.Partner,
Valid => vMBTCPValid1,
Error => vMBTCPError1,
Status => vMBTCPStatus1,
Id := vID1 );

```

```

MBTCPConnect2( En_C := vConnectAll,
Channel := MBTCPConnect2.Channel,
Partner := MBTCPConnect2.Partner,
Valid => vMBTCPValid2,
Error => vMBTCPError2,
Status => vMBTCPStatus2,
Id := vID2 );

```

**Read:**

```

(*
MODBUS TCP Read
*)

```

```

vReqRead := NOT vReqRead;
TimerStart(vRedundancyTimer);

```

```

IF vRedundancy = FALSE THEN

```

```

MTRed1( Req := vReqRead,
Id := vID1,
StartAddr := pStartAddressRead,
Ndr => vReadNdr1,
Error => vReadMBTCPReadError1,
Status => vReadStatus1,
Rd[1] := vReply);

```

```

TestStatusRead1SR( S1 := vReadStatus1 < 0, Reset := vReadStatus1 = 1 );

```

```

IF TestStatusRead1SR.Q1 THEN

```

```

IF TimerElapsed(vRedundancyTimer) > vRedundancyTime THEN

```

```

TimerReset(vRedundancyTimer);

```

```

TimerStart(vRedundancyTimer);

```

```

vRedundancy := true;

```

```

END_IF;

```

```

END_IF;

```

```

ELSE
MTRed2( Req := vReqRead,
        Id := vID2,
        StartAddr := pStartAddressRead,
        Ndr => vReadNdr2,
        Error => vReadMBTCPReadError2,
        Status => vReadStatus2,
        Rd[1] := vReply);

TestStatusRead2SR( S1 := vReadStatus2 < 0, Reset := vReadStatus2 = 1 );
IF TestStatusRead2SR.Q1 THEN
    IF TimerElapsed(vRedundancyTimer) > vRedundancyTime THEN
        TimerReset(vRedundancyTimer);
        TimerStart(vRedundancyTimer);
        vRedundancy := false;
    END_IF;
END_IF;
END_IF;

```

(\*Error until read is possible.\*)

```

IF TestStatusRead1SR.Q1 AND TestStatusRead2SR.Q1 THEN
    vReadError := true;
ELSE
    vReadError := false;
END_IF;

```

### **Write:**

```

(*
MODBUS TCP Write
*)

```

```

vWriteReq := NOT vWriteReq;

```

```

IF vWriteEnable1 THEN
    MTWrite1( Req := vWriteReq,
             Id := vID1,
             StartAddr := pStartAddressRead,
             Done => vWriteDone1,
             Error => vWriteMBTCPError1,
             Status => vWriteStatus1,
             Sd[1] := vWrite);
ELSE

```

```

MTWrite2( Req := vWriteReq,
          Id := vID2,
          StartAddr := pStartAddressRead,
          Done => vWriteDone2,
          Error => vWriteMBTCPError2,
          Status => vWriteStatus2,
          Sd[1] := vWrite);
END_IF;

```

## Slave Station

**Table 10: Parameters of the slave station**

	Name	Data Type	Direction	FD Port	Initial value	Description
1	pEnable	int	unspecified	yes	11	

**Table 11: Variables of the slave stations**

	Name	Data Type	Attributes	Initial value	Description
1	vEnable	int	retain	1	This can be seen on the 'Access Variables'
2	vEnable2	int	retain	2	
3	vEnable3	int	retain	3	
4	vEnable4	int	retain	4	

### **StartSlaveCode:**

```

(*)
29.11.2019
Atte Suutari
Master's thesis
Slave
*)
vEnable := pEnable;

```