NTNU

Norwegian University of
Science and Technology

Cyber Security in Smart Meters: Vulnerability Investigation in the Home Area Network Port

Isa Agnete Halmøy Fredriksen

Master of Science in Communication Technology
Submission date: April 2018
Supervisor: Karin Bernsmed, IIK
Co-supervisor: Martin Gilje Jaatun, SINTEF

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title:	Cyber Security in Smart Meters: Vulnerability Investigation in the Home Area Network Port
Student:	Isa Agnete Halmøy Fredriksen

Problem description:

Up until now electricity usage in people's homes has been measured mechanically and read manually. The functionality of the conventional electricity meters has not allowed for fine grained measurement to learn exactly when how much energy is consumed. For a power generating company it is helpful to know when there is higher and lower consumption during a day in order to predict how much generated power is needed to match the demand. At the other end, the consumers should get more detailed feedback on their consumption to make it easier to keep an eye on and possibly lower their energy costs.

The new smart meters that are going to be installed in Norwegian homes within January 2019 will replace the conventional mechanical meters and produce more fine-grained information about energy usage. In contrast to the mechanical meter, the smart meter will provide a high-level information infrastructure to facilitate automatic monitoring and metering operations. To make some of this information available to the consumer, the smart meter will be connected to a Home Area Network (HAN) via a HAN-port that is built into the smart meter.

This thesis will investigate if the HAN-port has any vulnerabilities. It will consider the security of the smart meters and the smart home, and explore how vulnerabilities in HAN might influence or harm the smart metering system and users' privacy.

Responsible professor:	Karin Bernsmed, IIK, NTNU
Supervisor:	Martin Gilje Jaatun, SINTEF

Abstract

As a part of a modernized electric power system, mechanical electricity meters are being exchanged with smart meters. The smart meters are to be equipped with a communication interface that consumers may use to get a better overview of their energy consumption and control their smart electricity consuming devices. The chosen interface is the Home Area Network (HAN) port. This thesis investigates the HAN and the HAN port in search for potential vulnerabilities. Through a literature review and a stepwise vulnerability study and testing, the HAN and the HAN port are investigated for potential vulnerabilities. The steps in the vulnerability study consist of identifying the assets of the system, model the flow of the assets in the system, consider potential threats and attacks and develop multiple scenarios concerning these. With respect to a limited number of attack scenarios, the thesis identifies potential vulnerabilities. The investigation has not been exhaustive, thus there might be other potential vulnerabilities. The literature review revealed that the smart meters are being rolled out before the security solution to protect HAN port data is ready. This last remark has been discussed as a potential vulnerability in the sense that it is implemented after the rollout, and not included from an early stage.

Sammendrag

Den pågående moderniseringen av strømnettet er i gang med utbytting av mekaniske strømmålere med smartmålere. Smartmålere er utrustet med et grensesnitt som skal brukes av kundene. Det skal gjøre det mulig å holde en bedre oversikt over forbruket, og kan potensielt også brukes til å kontrollere smarte strømenheter i huset. Grensesnittet er valg til å være en Home Area Network (HAN)-port. Denne masteroppgaven undersøker om HAN og HAN-porten har potensielle sårbarheter. Gjennomomgang av eksisterende litteratur, utvikling av et sårberhetsstudie, samt testing, vil være bestanddelene for å undersøke om det finnes mulige sårbarheter. De fire stegene i sårbarhetsstudien inkluderer identifisering av verdideler som skal beskyttes, modellere flyten av de primære verdidelene, vudere flere trusler og angrep og utvikle scenarier der trusler og angrep betraktes. På bakgrunn av det begrensede antallet av scenarier, identifiserer masteroppgaven flere mulige sårbarheter. Gjennomgangen av eksisterende litteratur viser at smartmålere rulles ut før sikkerhetsløsningen som skal beskytte data som strømmen ut på HAN-porten er bestemt. Dette har blitt diskutert som en mulig sårbarhet med henvisning til at sikkerhet bør være inkludert i et utviklingsprosjekt fra en tidlig fase for å unngå flest mulig sårbarheter.

Acknowledgments

This master's thesis finalizes the five-year Master of Science in Communication Technology program at the Norwegian University of Science and Technology (NTNU), and is submitted to the Department of Information Security and Communication Technology (IIK).

There are several people that I would like to thank for their help and support during my studies.

First of all, I would like to give a humble thank you to my supervisor, Martin Gilje Jaatun, and my responsible professor, Karin Bernsmed, for their continuous guidance, feedback and motivation. They have been steadfast in their advising roles and their help has been invaluable and highly appreciated. Next I would like to thank my contact in Aidon, Rolf Pedersen, for having been very helpful with documentation and given immediate answers whenever I had any questions for him.

My family has always been there for me. I would therefore like to give a very special thank you to my mother and my father for their love, constant support and for believing in me. A big thank you goes to my brother Tor Andre Myrvoll for always inspiring me, for showing me that a challenging path is a good path and for many interesting conversations. I would also like to express my utmost gratitude to my sister, Anja Hennie Halmøy Fredriksen, to my brother, Stian Myrvoll, and to Jakob Dagsland Knutsen, for maintaining an unwavering faith in me.

For proofreading of the thesis I owe an extra thank you to Tor Andre Myrvoll, Anja Hennie Halmøy Fredriksen and Jakob Dagsland Knutsen.

Trondheim, April 24, 2018
I.A.H.F.

Preface

To work on this thesis has been both challenging and rewarding. Although I wished that the practical part of the thesis had been more extensive, I found great interest in the theoretical part in such a way that there was no disadvantage to the lack of practical testing.

Except the two borrowed figures, Figure 3.4 and Figure B.1, all illustrations are created or remodeled from others' work by the author of the thesis. In the cases where the illustrations have been inspired by others or have been remodeled, the sources to these illustrations have been referred to in the texts below the figures. The thesis has asked for and been granted permission to use the remodeled and the borrowed figures.

The smart meter that has been borrowed from Aidon to use for testing purpose in this thesis is not the exact same type that is going to be enrolled. The smart meters that are being enrolled are using a recommended standard solution and protocol, while the smart meter used for testing in this thesis is not.

Contents

List of Figures

List of Tables

List of Useful Words

asset	An asset can be a piece of data or anything else tangible within the hardware or the software that the system should be protecting. An asset can also be something intangible, like reputation. Since an asset is something of value to a person or an organization it needs to be protected [34, 35].
attack	An attack is an exploit that is being carried out. It might be successful or unsuccessful, but always in attempt to gain unauthorized access to destroy, disable, spread or steal an asset [35].
authentication	Authentication is the check a system does in order to make sure the user who wants access is who she claims to be [35].
authorization	Authorization is the check a system does in order to make sure the user is allowed to gain access to the particular asset she asks access to [35].
threat	A threat is a potential exploit and is directly connected to a a particular vulnerability [31].
vulnerability	A vulnerability is a weakness in a system that makes the system incapable of withstanding exploits [31].

List of Acronyms

AMI Advanced Metering Infrastructure.

AMR Automatic Meter Reading.

CIA Confidentiality, Integrity and Availability.

COSEM Companion Specification for Energy Metering.

DFD Data Flow Diagram.

DLMS Device Language Message Specification.

DSO Distribution System Operator.

ESD Electrostatic-Sensitive Device.

HAN Home Area Network.

HDLC High-Level Data Link Control.

HES Head End System.

IoT Internet of Things.

LDTI Local Data Transmission Interface.

M-Bus Meter-Bus.

MCD Mobile Computing Device.

MCI Modular Communications Interface.

MCU Microcontroller Unit.

NEK Norsk Elektroteknisk Komité.

NTNU Norwegian University of Science and Technology.

OBIS Object Identification System.

PLC Power Line Communication.

SCADA Supervisory Control And Data Acquisition.

SMI Smart Meter Infrastructure.

STRIDE Spoofing of identify, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privileges.

TRA Threat and Risk Assessment.

TSO Transmission System Operator.

UCM Universal Communications Module.

WSN Wireless Sensor Network.

Chapter 1
Introduction

1.1 The New Interface in Smart Meters

The Home Area Network (HAN) port is planned to raise awareness of electrical power consumption in households, motivate consumers to save electricity and thereof lessen the pressure on the power distribution network during peak hours. The HAN port will be implemented into smart meters that are being rolled out in Norway today, and elsewhere in the world, and is a part of the next generation power network, also called the smart grid. With the implementation of the above-mentioned features of the HAN port to the smart metering system, also called the Advanced Metering Interface (AMI) system, several new vulnerabilities will be added to the threat landscape of the AMI. An interface like the HAN port is an additional access point to the smart meter and the smart grid, hence it must be properly investigated to find or rule out any vulnerabilities before being deployed to the AMI system.

1.2 Motivation

With the expansion of Advanced Metering Infrastructure (AMI) systems, the power industry is facing a challenge regarding data security. Going from a fairly simple mechanical and manually handled system to a complex information system can lead to many unfortunate security incidents if not developed and managed in a proper way from the start. When detailed and sensitive data is gathered, transported and stored between multiple stakeholders the assets are historically more likely to be exposed due to improper system development. The reason is, more often than not, that development routines do not include security requirements from the beginning, but is implemented at the end of the development process [16].

This approach to information security shows a lack of awareness to its true importance. Even though security awareness, both by users and by developers, is increasing [43, 12], the focus on cyber security of AMI is falling behind [16]. Since AMI in the smart grid is a young topic and functionality is still being worked out, the

work on securing the system must be intense in order to keep up with development of AMI. A place to start is to analyse the system for threats and vulnerabilities in order to know the type and strength of proper security models for the AMI system [61].

Keeping in mind the challenges of cyber security in AMI, the motivation for this thesis is to contribute to a more secure AMI.

1.3 Aim of the Thesis

The aim of this thesis is to investigate whether there are any vulnerabilities in the Home Area Network (HAN) port. There will also be an investigation into vulnerabilities in the HAN. The theoretical and the practical part of the thesis are combined in order to have a thorough investigation into vulnerabilities.

1.4 Scope and Limitations

This thesis focuses on the smart meter and its communication through the HAN port to connected devices in the home. Area wise the scope is limited to the house where the HAN, smart meter and third-party equipment are going to be installed. Thus, any communication outside the house, for example the AMI channel from the smart meter to Head End System (HES) is out of scope.

As explained in the problem description, the thesis will be looking for vulnerabilities in the Home Area Network (HAN) port that may affect the security of the AMI system in the house. Nonetheless, this does not restrict the thesis from looking into the security of HAN in its entirety.

1.5 Challenges with Information Security Investigation

In the paper "Hunting for aardvarks: Can software security be measured?" (2012) [36] Jaatun examines different approaches to measure the strength of information security. On the matter of testing for security, he justifies that a flaw that has been found in a software means that the investigated software has flaws. On the contrary, if no flaws are found, one can not conclude that they do not exist, since flaws might exist elsewhere in the software. It is not possible to perform exhaustive testing to claim software to be perfectly secure, since a flaw might exist in a simple bug or be hidden behind bad design or improper implementation. Not everything can be tested for, since it would take too much time to go through all input combinations to the software. The same challenge is present within this thesis. To find a vulnerability reassures that a vulnerability exist in the system, while not finding any vulnerabilities does not guarantee that there are no vulnerabilities there at all.

In "Software Security – Building Security In" (2012) [41] McGraw stresses the importance of building in security from the beginning of a software development process. McGraw states that "there is no such thing as magic crypto fairy dust" that if added in the end makes the system secure, but that it should rather be included at the requirement level. He also emphasizes that a system can not be tested into security. Security testing should according to McGraw encompass both functionality testing and risk-based security testing based on attack models. Black-box testing is also useful. However, it is still not possible to cover all pressing security issues with testing.

Andersen [6] wrote an article in 2003 about the difficulties concerning the nonexistence of measuring techniques for information security. The well-known CIA (Confidentiality, Integrity, Availability) Triad has been the baseline for information security requirements, but measuring the strength or stability of the three elements of the CIA Triad is still lacking. Anderson suggests that a part of the problem is that estimates and statistical data regarding the matter of information security is all about the damage from undesired events. No estimates exist in regard to the assurance of the risks and control of the assets. With this knowledge, the results of this thesis will not be possible to measure the effect of. Hence, potentially discovered vulnerabilities can not be put on a scale to discuss how much less secure the system is.

1.6 Method

The thesis will be combining a theoretical approach towards the problem with a practical one through testing, as described in the following subsections.

1.6.1 Theoretical study

The theoretical part of the thesis is a literature review of existing documents, published articles and reports on AMI systems, HAN and the HAN port. Some of the documentation and reports have been provided by Aidon[1] under a non-disclosure agreement, and may contain confidential information. The thesis will still refer to some of these documents. A vulnerability study will be carried out in the theoretical part. This study has been planned and modeled by the author of the thesis based on a standard on risk analysis [34] and a SINTEF report to support risk analysis [39].

In a report on support for risk analysis from 2014 [39], SINTEF gives recommendations on how to go through with a stepwise risk analysis of AMI systems. They propose to start the analysis by identifying what they call "information values". Since a vulnerability study has to do with threats against values in a system, it is

[1] `https://www.aidon.com/nb/`

reasonable to start the vulnerability study in this thesis with the same task as in a risk analysis. Keeping in mind that because a risk analysis is much more rigorous and complex than a vulnerability study, the thesis will only make use of some of the recommendations in the report.

First, the assets of the system will be identified. The next step is to create an overview by drawing a Data Flow Diagram (DFD), to see where the assets go and what happens to them in the system. The DFD will be useful for the next step which is the vulnerability investigation. At this point several scenarios will be developed in order to give a tangible sense of what might go wrong and which vulnerabilities might exist.

Remark about the Information Gathered on Smart Meters

With respect to the information that has been studied to build the report, especially Chapter 3, the thesis will combine information that is generic for all smart meters together with information that is specific for the smart meter products from Aidon. The generic information has been gathered from standards, research papers, reports and other documents and applies to all smart meters in general. While on the other side, the information received from Aidon applies to their own smart meters and may differ from how other producers choose to implement their smart meters.

1.6.2 Testing

The practical part of the thesis will be concentrated around information retrieval from the smart meter and analysis thereof. A smart meter for testing purpose has been provided by Aidon. At first it will be useful to see which information is coming out of the HAN port. It will also be of interest to try to execute one or two attacks against the system.

The smart meter that has been provided by Aidon is a different type of smart meter, and has a different version, than the smart meters that are being enrolled. The smart meter that are being installed is implemented by the recommended standard and protocol from The Norwegian Water Resources and Energy Directorate (NVE).

1.7 Research Questions

Through the described method above, gathered information about smart meters and through testing, the thesis will try to answer the following research questions. The questions have been divided into umbrella questions, which are the main questions to be answered, and sub-questions.

Top questions:

1. What are the most significant threats and attacks against smart meters?
2. Which vulnerabilities may exist in the HAN and the smart meter's HAN port with respect to the most significant threats and attacks?

Sub-questions:

1. How is the HAN port and the HAN port data secured?
2. The smart meters are supposed to have a lot of functionalities, but only some of it is enabled. Technically, how are the rest of the functionalities disabled?
3. Which threats and attacks via the HAN or the HAN port against the smart meter are likely to occur? What is the motivation behind them and how may they be performed?
4. How may the attacks affect the assets that the system shall protect?

1.8 Outline

Chapter 2 will give the reader the necessary background information to understand how the several technologies existing in a smart grid belong together and which role the smart metering systems will have in the smart grid. Information security of smart metering will also be introduced. The last section will present previous research. Chapter 3 presents the HAN port, how it is planned to be implemented, and the security of the HAN port. In Chapter 4 the vulnerability study is demonstrated in a stepwise manner. Next, Chapter 5 will present the testing part of the method. Then, the discussion of the thesis will be presented in Chapter 6. Chapter 7 gives the conclusion of the thesis. The future work will also be presented here.

Chapter 2
Background

This chapter provides the reader with the necessary background information that will be essential throughout the discussion in the following chapters. The chapter introduces concepts and technologies that are used for the smart grid and smart meters to help the reader understand the connection between the technologies.

Smart metering is achievable thanks to several technologies and concepts. That is why this chapter will be introducing what lays the base for smart metering systems, which are often seen under the name Advanced Metering Interface (AMI). Both the Internet of Things (IoT), Wireless Sensor Network (WSN) and smart grids play a role in the AMI. IoT is not a technology in itself, rather an idea or a concept that is realized using e.g. WSNs. WSN is the key technology for IoT, especially when it comes to the smallest objects which are often called resource-constrained devices. The Smart Grid consist of many of these resource-constrained devices and IoT is the idea that interconnects these devices so that they can function on their own.

First, Chapter 2.1 and Chapter 2.2 give an introduction to WSN and IoT, followed by an overview of smart grids in Chapter 2.3. How smart meters work is explained in Chapter 2.4. Then, an introduction to key concepts of information security is given in Chapter 2.5 and finally Chapter 2.6 will present the reader with background knowledge on vulnerabilities and threats.

2.1 Wireless Sensor Networks

A WSN is a network of sensor nodes. These nodes are often considered to be resource-constrained objects since they are limited in battery, processing and memory capacity. A sensor node usually consists of a battery, a sensor, an antenna for wireless transceiving and a microcontroller, also called a Microcontroller Unit (MCU) [1]. The

[1] A microcontroller unit (MCU) is a small computer on a single chip. It consists of a processor, memory and has input/output possibilities. The MCUs are designed to be embedded into equipment such as smart phones, smart meters, washing machines, cameras and more [66].

sensor collects real-time data about the environment where it is located and sends the collected data to the microcontroller. The microcontroller collects and forwards the data using the transmitter, to for instance a website that the user of the sensor network has access to [74]. The user can interpret the information and react by sending messages to the microcontroller and tell it how to behave by e.g. lowering or turning off devices in order to save electricity.

There are a wide range of usage areas for WSNs: Environmental monitoring like seismic or weather measurements, battlefield surveillance [40] and many more. Since 2014 [75], WSNs are also used for power management by the power industry [46]. In home automation WSNs are used for monitoring and control of power consumption in smart electrical equipment and automation.

2.2 Internet of Things

WSN can be considered as an enabling technology for IoT. The sensor nodes and the communication infrastructure create the network that IoT consist of. IoT is the enabler that lets any "thing" connect to the Internet.

IoT is a paradigm and a model of a system where the idea is that any object equipped with sensors and microprocessors should be able to connect to the Internet using existing Internet standards. Area wise, IoT is thought to exist everywhere. The domains range from large-scale monitoring of infrastructure to small-scale home-automation [24]. Whe narrowing it down to people's homes, the "things" in IoT are not only computers and smart phones, but objects like heaters, air conditioners, lamps, refrigerators, water heaters, cars and washing machines.

It is important to emphasize that IoT is not a technology by and of itself, but is rather an idea that brings several technologies together in order to connect everyday objects in a communicating-actuating network. IoT is meant to embed more intelligence in people's everyday objects and as a result many of the manual human-computer interactions become superfluous. Objects will become ubiquitous and easier to manage because of all the data that will be gathered, stored and processed on the Internet.

2.3 Smart Grid

The smart grid is being called the "next-generation power grid" [21, 73, 65]. It has features that in comparison to the traditional power grid makes it a disruptive

Table 2.1: An overview of the differences that come with the smart grid. Inspired by [21].

	Traditional Grid	**Smart Grid**
Infrastructure	Electromechanical	Digital
	Centralized power generation	Enables decentralized power generation in addition to centralized
	Few sensors	Many sensors
Functionality	One-way communication	Two-way communication
	Manual meter reading	Automatic meter reading
	Manual restoration	Self-recovering
	Only total consumption is monitored	More data provides the consumer with detailed insights into own consumption
	Hard for power suppliers to plan how much power to produce	Possible to make use of consumption data to create statistics on of how much to produce at what time.

technology[2] as it will change the power industry considerably. In Table 2.1 on page 9 differences between the traditional power grid and the smart grid are listed.

The smart grid is a more flexible power grid than the existing one. Both in regard to the flow of electricity and the flow of data. The traditional power grid was never designed to allow bi-directional flow of electricity. Only centralized power suppliers were able to generate and push power through the grid and out to the consumers. With the smart grid it is technically possible to allow for decentralized power generators to work together with the established suppliers. Wind turbines, solar panels and other generators may be connected to the grid and feed power into the grid. Ideally, if consumers take on a role as producers of energy in the future it might cause fewer blackouts, more sustainable energy production and lessen the pressure on power companies.

The traditional power grid is hierarchical and unidirectional. It is illustrated in Figure 2.1 on page 10. As the figure shows, there is only a physical infrastructure for the energy distribution. It does not have a digital communication infrastructure. The traditional power grid is all about power generation, transmission, distribution. Essentially, Transmission System Operators (TSOs) are responsible for high voltage

[2]A disruptive technology is a technology that "shakes up" the industry and forces a displacement or replacement of the previous technology. The term *disruptive innovation* was coined by professor Clayton M. Christensen in his book "The Innovator's Dilemma" in 1997 [14].

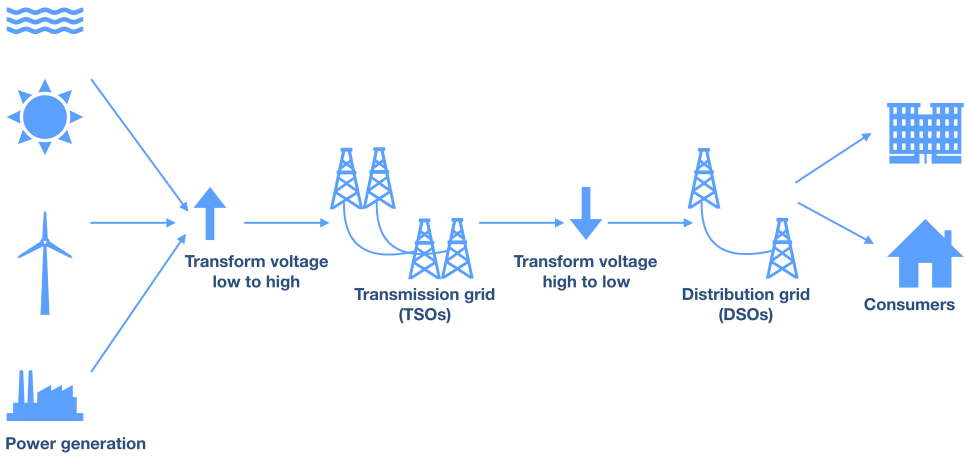

Figure 2.1: Illustration of the traditional power grid. Inspired by [21]

electricity transport from the generation plants to the distribution networks [59], while the Distribution System Operators (DSOs) are responsible for regional and local electricity transport to the consumers [56]. DSOs also provide consumers with energy meters and deal with billing of electricity consumption.

In contrast to the traditional power grid, the smart grid adds a communication grid upon the energy infrastructure. This is the essential point that separates the two types of grid; the fusion of the power network with the Internet. With the communication infrastructure comes many new functionalities and improvements. Sensors, processing nodes, meters, power generators and buildings are interconnected with the communication network. If a sensor detects for example a blackout or voltage error, it may send an alarm out on the grid and the processing nodes will be able to process the information from the sensors and handle the problem by informing the correct instances. The smart grid enables fast error handling and a safer power grid. Figure 2.2 on page 11 illustrates the interconnected smart grid.

In Figure 2.3 on page 12 the smart grid has been illustrated through different layers. At the bottom there is the physical infrastructure. Roughly put, the physical infrastructure of the smart grid is the traditional power grid. The other layers are put on top of the traditional power grid to create the smart grid. The communication layer consists of communication technology and protocols that interconnects entities in the physical layer. These entities range from sensors and meters in end points (houses, buildings), to transmission and distribution control centers, and Head End Systems (HES). The information layer represents data and information that is gathered, processed and communicated between entities in the system. The top layer, the

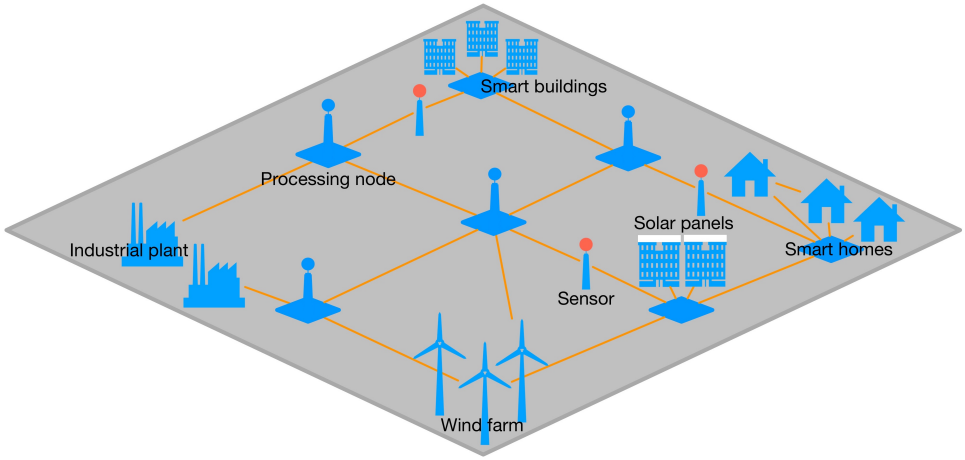

Figure 2.2: Overview of the smart grid. Inspired by [70].

function layer, decides what happens to the data and what it will be used for [70]. In this thesis we are especially interested in the layers that deal with communication, information and functions.

2.4 Smart Meter

At the time of writing, the smart meters are on the verge of being rolled out to every home in Norway and elsewhere in the world. In Norway, the installation is planned to be finished by January 2019 [39]. The new smart meters are going to replace the conventional mechanical energy meters to offer a high-level information infrastructure based on digital communication.

The base for the new metering system is the smart grid. Smart grid infrastructure and communication between the sensors, smart meters and data centers is the essence of the new metering system. Automatic real-time measurements are used to get a fine grained measurement of energy consumption [65].

The smart meter is connected to the HES via secured mobile communication. The communication flow is bidirectional [37]. Bidirectional flow implies that the smart meter and the HES both can send and receive data to each other. The connection between the smart meter and devices in the consumer's home is unidirectional, meaning the HAN port inside the smart meter shall be read only [1]. This restriction has been implemented to ensure data integrity of the HAN port data, and to secure the smart meter [51]. The read-only nature of the HAN port is also important for

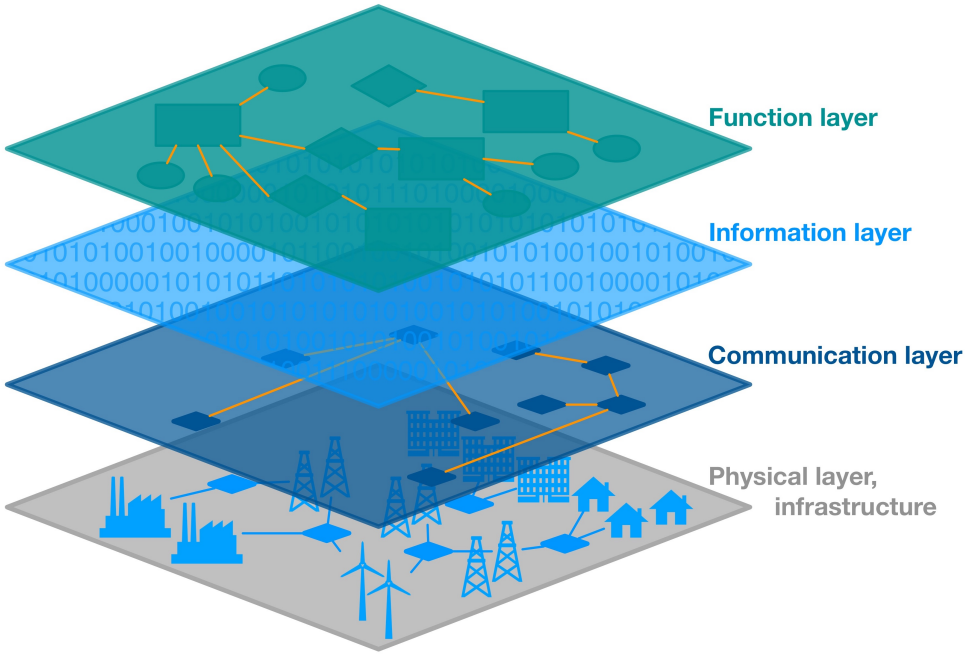

Figure 2.3: Illustration of the different layers that the smart grid consist of. Inspired by [70].

billing reasons [69].

Among the implemented functionalities, the smart meter will gather details about power usage which enables the consumers to pay better attention to their consumption in real time [17].

2.4.1 Mesh Topology

In certain areas where the density of consumers is high, such as residential areas and apartment buildings, the DSOs may choose a mesh topology for communication between smart meters and the HES. In a mesh topology, one of the smart meters that has been installed in a consumer's home is a master meter, while the other nearby smart meters are slave meters. The slaves transmit their meter data and status signals via short range radio frequency, for example 802.11, to the master meter. The master meter concatenates meter data from slaves as well as its own meter data and transmits the data to the HES via for example 2G or 3G. All communication from HES to the slave meters must go through the master meter [38, 4]. Figure 2.4 on page 13 depicts the mesh topology of smart meters.

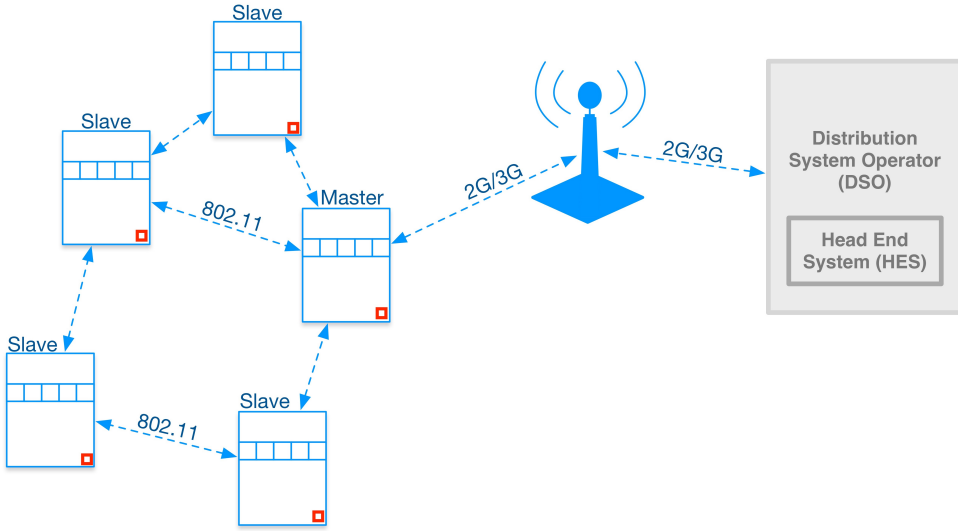

Figure 2.4: Illustration of the the mesh topology of smart meters. One of the meters is the master node that transmits and receives signals from slave nodes to the HES and the other way around. Inspired by [4].

2.4.2 Overview of the Smart Metering System

The architecture of the communication interface between the smart meter and the DSOs is a matter of optimization of the billing system. The DSOs are obliged to protect consumers' data according to Norwegian law while they also need to take into account their own financial budget limitations. Norsk Elektroteknisk Komité (NEK), that is The Norwegian Electrotechnical Committee[3], has delivered a report where they recommend how the architecture of the smart meter interface should be assembled [48]. The communication channel between the smart meter and the energy supplier can be implemented in several ways, either by Internet, mobile communication, radio link or over Power Line Communication (PLC). If meter data are transmitted over PLC, the data is sent simultaneously together with the electric power. The communication require an IP base to be able to carry logical functionality and a dedicated infrastructure in the distribution network. At some point in the PLC, the meter data will have to split from the electricity transmission and leave the PLC to be carried further to the HES via ordinary data networks [30]. Figure 2.5 on page 14 illustrates the smart metering communication system.

At the consumer's side the interface between the smart meter and the local network is planned to be arranged as follows:

[3] `https://www.nek.no/english/`

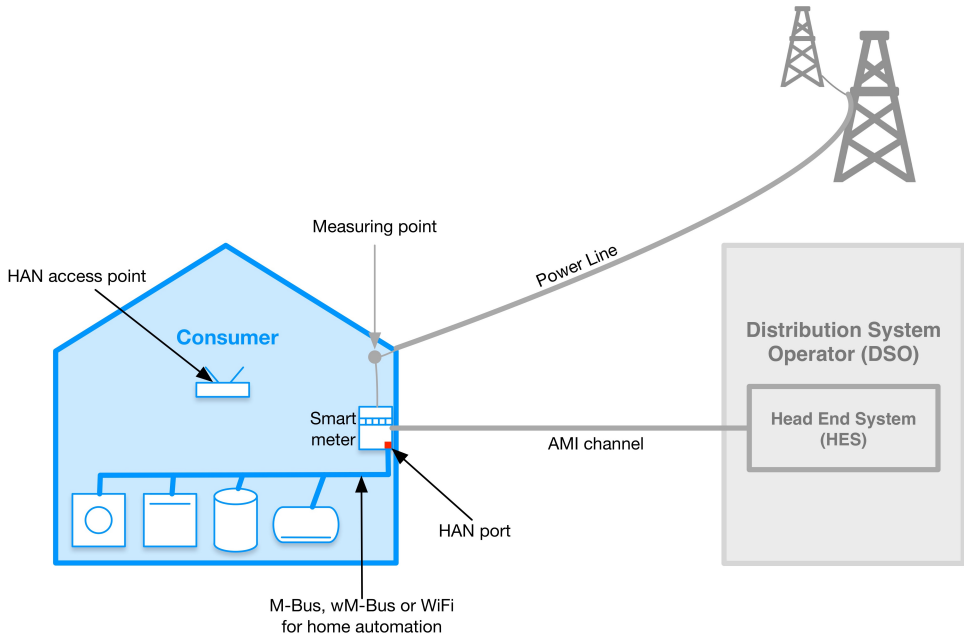

Figure 2.5: Illustration of the Smart Metering System.

- HAN will be the local network at the consumer's side,
- The interface between the local network (HAN) and the smart meter will be the HAN port
- The physical contact to make the HAN port available to the consumer will be a RJ45 connector. This is the contact that a wireless adapter may be connected to.
- Transportation of data between smart meter and HAN is arranged via Meter-Bus (M-Bus).

This is illustrated in Figure 2.6 on page 15.

2.4.3 Functionality of the Smart Meter

The main task for the smart meter is to measure consumption and the quality of the electricity in the house and send this information to the DSO, automatically, at given intervals. If there is a blackout an alarm is sent to the DSO [30].

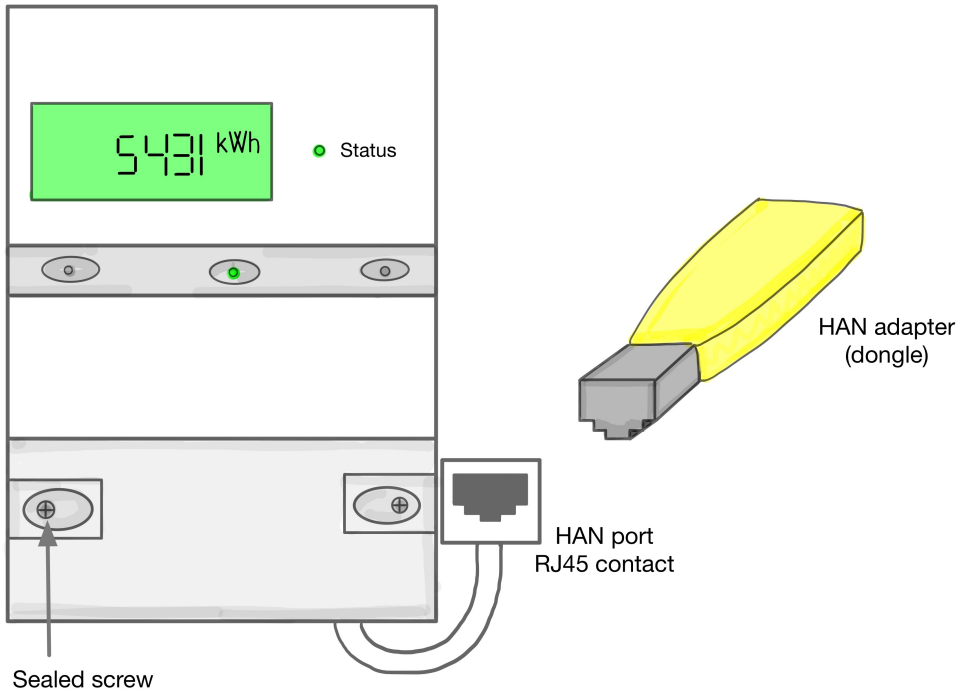

Figure 2.6: Illustration of the smart meter, the RJ45 physical contact and a HAN adapter to connect the home automation devices to smart meter. Inspired by [50].

The smart meter has three modes of communication:

1. A communication channel between the smart meter and the DSO, called the AMI channel.
2. A HAN port used to share consumption data gathered by the smart meter with the consumer's smart home equipment that is connected to the HAN.
3. An RS (Recommended Standard) port used for configuration of the smart meter

The communication channel between the smart meter and the DSO is the main communication of the AMI and is called the AMI channel. All other communication is additional functionality [30].

The RS port is located beneath the sealed cover on the smart meter, thus it is unavailable for the consumer. This port is a local service port that is exclusively

used for the purpose of testing, configuration and development of the smart meter. Only technicians from the smart meter producer are permitted to use this port [49]. The RS port will assumably be used in situations where the meter is not able to be configured remotely from the HES, for example due to hardware errors. In such cases, a technician may visit the consumer's home to inspect and debug the meter via the service port.

The HAN port is at the time of installation closed. Only if requested by the consumer may technicians from the DSO open the port remotely from the HES for communication through the HAN port. When the HAN port is opened, the consumer is free to connect any smart home technology equipment to it. The idea behind this functionality at the consumer's end is to provide a more detailed overview and control of the energy consumption [71]. This functionality is realized through HAN. As explained in Section 2.4.2 on page 13, the smart meter may be connected to smart objects around the house via the HAN port. When the smart devices are connected, the smart meter will push information about electric power usage (kW), energy consumption (kWh), current (A) and voltage (V) to all connected devices through the HAN port [49, 7]. This is where the control part of the functionality comes in; depending on the total consumption, the devices will be able to react by turning themselves off or switch to a saving mode [55, 57].

There are certain times of the day where the price of electricity[4] is higher. The reason is often that consumption peaks and results in higher demand. If the heaviest power consuming devices in the home can react logically to information from the HAN port, this can even out the peaks and lead to reduced costs. The interoperability between smart devices lessens the intensity of the power demand at peak hours, and is necessary in order not to stress the power distribution network too much [53, 42]. Being able to control the power consumption of the consumer is beneficial both for the consumer, the DSO, the physical infrastructure and leads to socioeconomic benefits in general [30].

In order to make metering data available to the consumer, the DSO may offer the consumer a display that the consumer must pay for himself. The display would show the real-time consumption, but would not be able to connect to a service to get pricing data. Since most people today own a smart phone, tablet or PC, these personal devices might be better suited to provide the consumer with meter data [30]. This thesis then assumes that the chosen device to have meter data available on will be connected to the M-Bus. Making meter data easily available to the consumers, the idea is that they will become more motivated to save electricity and lower their

[4]The prices and statistics about price variation will be available to the consumer via a web site and not via the HAN port. However, the service to make the pricing data on the web site available is still being worked out [27].

consumption at peak hours [57].

The smart meters are equipped with other functionality that is by default disabled, in addition to the sealed HAN port. Among the functionalities is the 'breaker'. In the SINTEF report "Evaluering av NVEs veileder til sikkerhet i AMS" [60] the authors emphasize the risk of wide-area power outage in case of unauthorized access to the mentioned functionality. This functionality is planned to be used by the DSO as a kill switch in case the consumers fail to pay their electricity bills. However, if this functionality is misused, great consequences follow. For instance, if someone were to gain widespread unauthorized access to smart meters they may trigger remotely controlled blackouts. Based on SINTEF's evaluation report, NVE states in their guide to security in smart metering systems that switching off the power is considered a high risk [63].

2.5 Information Security

This section will give an overview of one of the thesis' main concerns; the information security issues regarding smart metering systems. It is then natural to start with the CIA Triad, which concerns confidentiality, integrity and availability, three security concepts widely known as the heart of information security. When developing a new information technology system, it is important to focus on security from the beginning. This way fewer errors occur and the system security becomes more effective [16].

Norsk Elektroteknisk Komité (NEK) carried out an examination on how the smart metering interface and the measuring data should be handled in [48]. This document is based on a philosophy that claims to rely as much as possible on global, already existing, standards when designing the physical architecture. Standardization is already a step in the right direction in regard to system security, since standards are based on the idea of optimizing reliability, safety and quality [23, 9]. The philosophy already mentioned also states that the data gathered by the smart meter and the smart metering interface should be secured with respect to the CIA Triad.

2.5.1 CIA Triad

A system that is considered to be secure should support the three CIA principles [33]:

- **Confidentiality** says that information shall be prevented from falling into the wrong hands. This concept is closely related to privacy. Proper access control mechanisms must restrict the data to only be accessible by those who are authorized.

- **Integrity** means that data shall not be tampered with in order to keep its trustworthiness. Access and usage control prohibits unauthorized people from making changes to the data.
- **Availability** is directed to having information available to those who needs it and are authorized to have it. Availability is also the maintenance word of the Triad. It consists of upgrading of the system, recovery and backup mechanisms during and after unwanted events and keeping the system in fit shape in general, and downtime low.

In addition to the CIA Triad, there are two more security requirements that are valuable for a system to be secure. One of them is called **non-repudiation** and means that the system must prove that the integrity and origin of the data is valid [62]. The other security requirement is **authenticity** which shall make sure that the sender of the information really is who he claims to be [72].

2.6 Vulnerabilities, Threats and Attacks

The IoT, the smart grids and the AMI are enablers for smarter energy utilization, incidence responses and more. However, the more connected entities are and the more data is gathered and transported, the higher the chances are for weaknesses to emerge in a system. When a system becomes more diverse, complex and heterogeneous, the probability for new vulnerabilities to appear and threats to take advantage of them increases [67]. There is also a higher chance of smart grid components getting infected or compromised due to several external access possibilities. A smart grid gives opportunities to many more attack paths compared to a traditional power transmission system [45].

To make sure the reader understands the concepts used in this section they will briefly be explained, as they are often seen to be mixed up. No system is perfect, so minor mistakes or hot fixes might create a weakness in the system. This is not necessarily a major issue, depending on where the weakness is located and how hard it is to make advantage of. Generally, if weakness is possible to take advantage of it, then it is called a vulnerability. A vulnerability can be exploited by a threat in order to get unauthorized access to an asset the system is trying to protect, whereas an attack is the actual exploit [34].

2.7 AMI Security by Aidon

Each smart meter is secured against physical tampering. At several places the meter is sealed with metal wire around the screws. If the screws are loosened, the metal wire will be broken and a tampering alarm will be sent to the HES [5, 52].

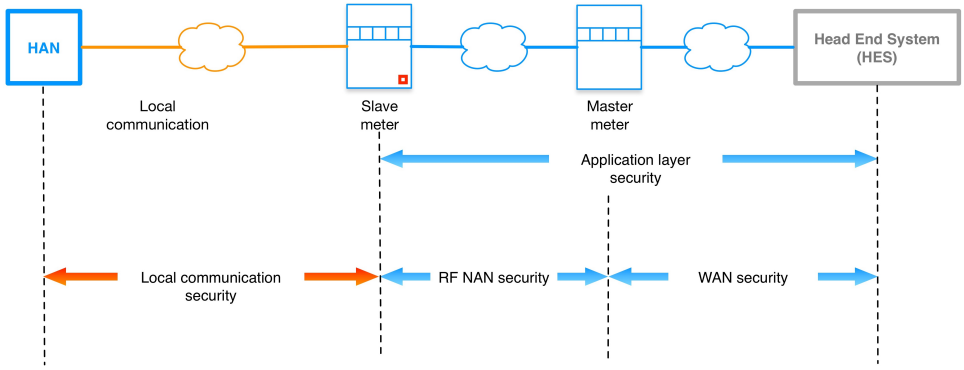

Figure 2.7: Overview of Aidon's security solution of the AMI system. Inspired by [5].

Figure 2.7 on page 19 shows an overview of the security of the AMI system. There is going to be end-to-end encryption between the smart meter devices (slaves and masters) and the HES. The security provided will be at the application layer. Communication between meters in the case of mesh networks where there are both master and slave meters will additionally be secured under "RF NAN Security", which is short for "radio-frequency neighbor area network security" [5]. The application layer security ends at the HAN port in the smart meter [52, 47]. Between the HAN port and HAN the communication must be secured locally [5].

2.8 Suggested Local Security Solutions

The DSO has the responsibility to inform the consumer about how one may gain a sufficiently secure solution between the HAN port and the HAN. When the HAN port is opened, there are two options to secure the information coming out of the local HAN port:

- Information security by encryption of HAN port data.
- Physical security by placing the smart meter inside an approved and locked cabinet.

The simplest solution is to place the box inside a cabinet, and it is most likely that this solution is chosen [52]. In case this solution is chosen, the DSO will secure the cabinets with physical locks. The thesis assumes that the reason for this solution to be considered is that it is likely that few consumers are going to build complex smart homes right away. Perhaps only one or two devices is thought to be connected to the HAN port, in which case a wired solution is the easiest one.

The encryption option requires that connected devices that will read data from the HAN port must be trusted and provided with correct decryption algorithms and decryption keys. Then, the devices are able to decrypt the encrypted data from the HAN port. Since the security solution is not going to be ready and implemented until after the smart meters have been rolled out, the smart meters must be equipped with hardware and software that are going to handle the chosen encryption scheme. The three smart meter producers in Norway, Kamstrup, Kaifa and Aidon, all claim that their meters are equipped with the necessary mechanisms in case the HAN port stream will be encrypted [47].

If the encryption solution is the one that is chosen in the end, the data available through HAN will be encrypted with an encryption key. There will be a website where the consumer can log in with a secure ID and ask for the decryption key from the DSO. The consumer places this key in the third-party devices that are going to read data from the HAN port [47, 51].

2.9 Smart Meter Security Faults in Other Markets

In 2016, The Financial Times published an article [15] describing a serious loophole in the new smart meters. The smart meter encryption scheme shared the same encryption key for every single meter that had been installed. This means that if a hacker was able to decrypt the key to get information from one smart meter, he could use the same key to get information from all other installed smart meters.

2.10 Previous Work

In a study published in 2008 [67], Ten et al. present a systematic vulnerability assessment framework for Supervisory Control And Data Acquisition (SCADA) systems. The vulnerabilities were evaluated at three different levels: System, scenarios and access points, using a framework composed of a cyber-net model and power-flow model. The cyber-net model is used for analysis of passwords and firewalls, models an overview of access points and draws potential attack models and attack paths through the SCADA system. Combining the power-flow model with the cyber-net model, the attack scenarios get numerically weighted by calculated probabilities for the different attacks. The power-flow model can also evaluate the impact of an attack through an access point, thus giving the vulnerability of the access point a value. This vulnerability assessment is quite rigorous and mathematical. Although the thesis will not get into such depth of the vulnerability assessment as this study has done, it can still be used as a confirmation that the focus on access points and attack paths are central in the anticipation of the new threat landscape. The authors of the proposed framework also stresses the challenge that was mentioned in Chapter 1.4, about the lack of statistical information on intrusion attempts in the modern

power infrastructure. Vulnerability investigation in SCADA systems need specialized models, hence the future assessment models should be based on more intrusion data.

Tøndel et al. [69] conducted a study in 2013 on threat modeling of AMI. In the study they combine several methods to identify and deal with threats. Data Flow Diagrams (DFDs) are used to make an overview of where data travel, STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges) classification is used to identify threats and attack trees highlights attacker goals and their potential path to the assets. The aim of this study was to make it easier for the power industry to perform threat modeling in AMI systems. The approach they concluded with is inspiring for this thesis' aim at investigating the HAN port for vulnerabilities, since threats and vulnerabilities are closely connected.

In 2015, Dougherty and Saitoh [18] published a paper that discusses several potential threats against the distribution of AMI systems. In the paper, the authors conclude that risk analysis and security testing of AMI systems should exist at the beginning of the design cycle and throughout the entire life span of the AMI systems. The paper emphasizes that the AMI consists not only of the smart meter, but all interfaces spanning from the DSO and all the way to the home automation system. One potential vulnerability that was mentioned in the paper, was the case of a flawed implementation of the HAN port. A case that is highly relevant to this thesis. The authors have, through the conduction of several Threat and Risk Assessment (TRA) workshops across business units and stakeholders, rated the HAN port as a "likely and major threat" to the AMI system. In order to better secure a flawless implementation of the HAN port, the results from the TRA workshops highlights among others, these requirements: 1) Third-party equipment that may be connected to the HAN port must be authenticated before connection takes place. 2) Before functions of the HAN port can be used, the third-party equipment must be authorized to use them. 3) There must be a way to change or remove authorization of third-party equipment from the HES. The thesis agrees with the first two requirements. The last requirement sounds like a violation of the consumer's rights, since the third-party equipment is the consumer's possession and the HAN port is not supposed to be used from HES.

Chapter 3
The Home Area Network (HAN) Port

In Chapter 2 the reader learned the economical reasons to why the HAN port and the extra functionality is implemented in the smart meter. This chapter will explain the technology in more detail, and dig deeper into information security in the Home Area Network (HAN) and the HAN port.

3.1 System Module

Figure 3.1 on page 24 shows an overview of the different components that the Aidon AMI system consists of. The HAN port is located on the system module [1]. It can be connected to adapters which again are connected to external devices (HAN), as the figure shows. The system module is a component with the following responsibily areas [26, 49]:

- Store meter data
- Process meter data
- Send meter data to the Distribution System Operator's (DSO) Head End System (HES)
- Send status reports to HES about network statistics such as current, voltage, harmonic
- Send alarms in case anything happens, e.g. attempts to break the seal on the smart meter box, ground faults, interruptions and blackouts

The smart meter has two microcontroller units (MCU). This technology was briefly explained in Chapter 2.1. One of the MCUs is placed inside the metering unit and the other is placed inside the system module. The MCU inside the system module is controlling everything the system module does, including the communication through

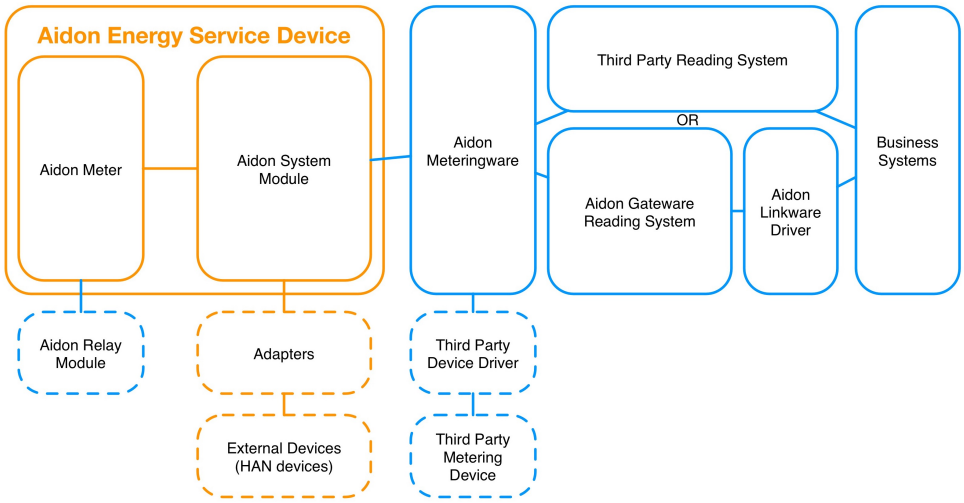

Figure 3.1: Overview of Aidon's Advanced Metering System which has been remodeled, inspired by [1, 4]. The thesis is concentrated around the Aidon Energy Service device (the smart meter) and the communication interface it has between adapters and external devices. This has been marked in orange.

the HAN port [50]. Figure 3.2 on page 25 shows the interior of the system module and the metering unit.

3.2 HAN Port

According to NVE the HAN port will not be opened until some time in 2018. The delay has to do with the security mechanisms of the data stream from the HAN port; it has still not been decided how the HAN port will be secured. Until a decision is made the HAN port will not provide any data to the HAN [58, 25]. Nevertheless, in Trondheim, among the 33000 installed meters per February 21, 2018, 30 consumers had gotten their HAN ports opened for communication. These consumers are free to start using the HAN port before the final the security solution has been decided, as long as the communication between the meter and third-party device is wired and inside the house [7].

The HAN port is illustrated in Figure 3.3 on page 26, where the magnifying glass is circling the HAN port. In this picture the sealed meter cover is removed. The port consists of four pins that will be connected to a 4-pin connector of the type Molex[1] to a RJ45 adapter at the time of installation [51]. Figure 3.4 on page 27 shows a picture of what the 4-pin connector looks like. The reason to why there will be an

[1] `https://www.molex.com/molex/products/group?key=connectors&channel=products`

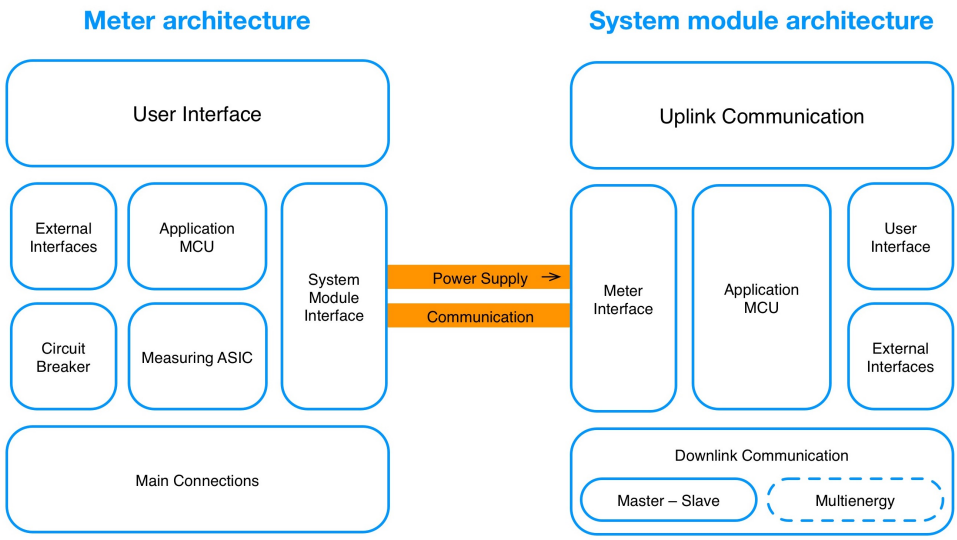

Figure 3.2: The architecture of the meter and the system module inside the smart meter. The figure is remade from an illustration received from Rolf Pedersen in Aidon [50].

external RJ45 connector and not one that is built directly into the system module is that the meter must be sealed, thus the HAN port becomes unavailable. The HAN port is going to be opened for data retrieval from the DSO's side, logically, therefore the HAN port should be available outside the seal through a RJ45 connector [52, 2].

The HAN port communication channel should support real time computing[2]. An example to why real-time computing is a requirement could be that the smart meter must be able to respond to the current market price, for example by lowering consumption when the price is high. As stated in Aidon's document description "Local HAN Interface" [1], HAN supports real-time computing.

3.3 M-Bus

In Norway the HAN port is chosen to be an M-Bus master in the bus technology in the consumer's home, thus the HAN port is the one driving the communication. The devices attached to the meter via the HAN port will function as slaves [50]. These devices are then going to react to the signals from the master, but are not allowed to

[2] "Real-time systems are defined as those systems in which the correctness of the system depends not only on the logical result of computation but also on the time at which the results are produced [64]." In practice it could mean that a system only has a limited amount of time to react on an event that has occurred, and that the reaction must be precise.

Figure 3.3: The smart meter borrowed from Aidon. The magnifying glass is circling the HAN port.

Figure 3.4: A 4-pin-to-RJ45 connector of this type will be inserted into the HAN port. The RJ45 contact will be outside the seal that is covering the smart meter. Photo: Aidon Ltd.

send any signals back to the master since the HAN port is designed to be read only. The M-Bus technology is not the technology that makes the HAN port read-only. Slaves in the M-Bus architecture are designed such that they are able to transmit signals to the master according to the international standard EN 13737-2 regarding the M-Bus [19]. The read-only nature of the HAN port is created at the link layer, and is explained in chapter 3.4.1.

Among the four pins on the HAN port, only two are used for the HAN port communication in Norway, which is the M-Bus technology. In other markets all four pins are in use, due to other requirements for the HAN port [50], thus the thesis assumes that the remaining two pins are not used at all in the Norwegian market and can be ignored. The pins that are used for communication through the HAN port carry the following signals:

- PIN1 is used for ground, GND
- PIN2 is used for +24V M-Bus TXD

The RJ45 connector, also called the HAN adapter, also uses the first two pins for the same purpose [1].

In order to make use of the information coming from the HAN port, the consumer may either choose a wired or a wireless solution. A wired solution is very cumbersome

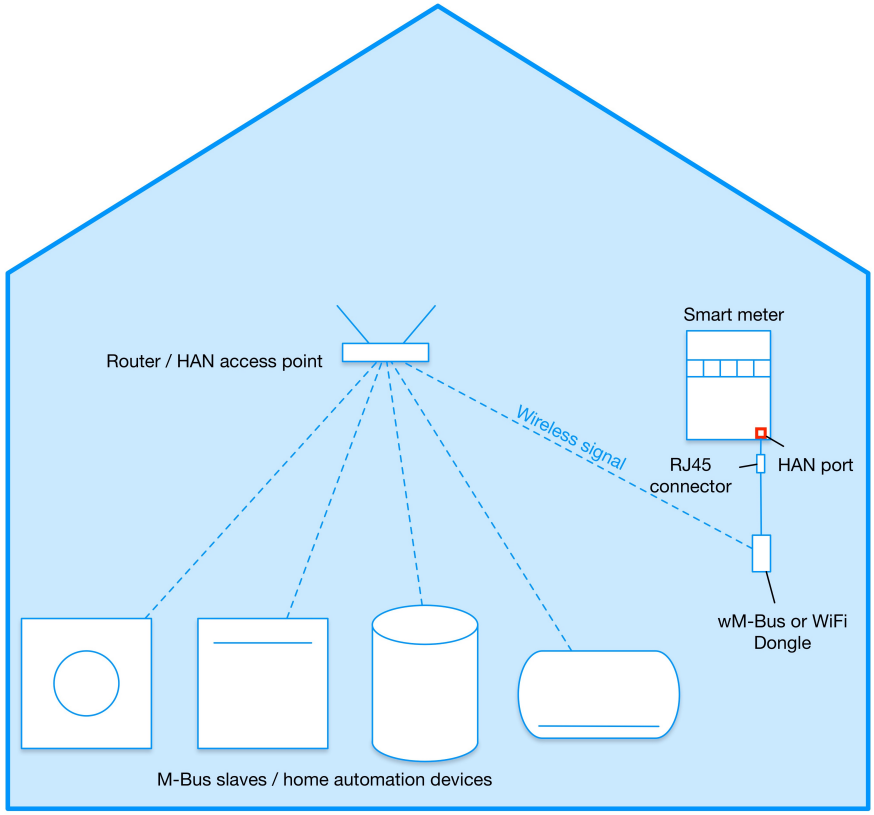

Figure 3.5: Getting data out of the HAN port with a M-Bus converter.

if many devices shall be added to the M-Bus, while a wireless solution is both easier and tidier. In the case of a wireless solution, a dongle may be connected to the RJ45 connector at the HAN port and send this signal to the router via a wireless networking protocol, for example using a wireless M-Bus (wM-Bus), WiFi or Zigbee. The router then forwards this signal to any device that speaks with the same protocol as the HAN port [52].

Figure 3.5 on page 28 shows an illustration of the described setup of a consumer's smart home with a wireless solution. Information coming out of the HAN port is made available to the consumer via a RJ45 contact and a connected HAN adapter (dongle) transmits the information to the smart devices in the home via the HAN access point.

3.4 Communication protocol

The communication protocol used on the M-Bus is DLMS/COSEM. Device Language Message Specification (DLMS) is a protocol that is used for metering data exchange [20]. Companion Specification for Energy Metering (COSEM) is the communication interface or object model that models the functions of the smart meter together with smart meter data using an object-oriented approach [10, 20].

3.4.1 Unidirectional Protocol Interface

"The Local HAN Interface - Product Description" from Aidon [1] states that the HAN port is unidirectional based on the standard EN 62056-7-5 (DLMS/COSEM suite) in combination with the standards EN 13757-2 (M-Bus physical layer), EN 62056-6-1 (Obis codes) and EN 62056-6-2 (Interface classes). Studying the M-Bus standard EN 13757-2 [19] one learns that the M-Bus is designed to support a bidirectional data transmission flow. Taking a closer look at standard EN 62056-7-5 it becomes clear that it is a special mode of the DLMS/COSEM communication profile that creates the unidirectional nature of the HAN port. This mode is realized with the modeling of COSEM objects through Local Data Transmission Interface (LDTI). The LDTI is a transmission interface at the data link layer that is unidirectional and acts as an M-Bus master [20]. Thus, the LDTI is the read-only interface that in the smart metering context is called the HAN port.

The COSEM server in the smart meter context will be the central software inside the smart meter. The thesis assumes that the central software must be the system module. The LDTI COSEM client will according to the standard IEC 62056-7-5 either be a part of the third-party device or an adapter in the HAN port that will function as a medium between the meter and the HAN devices. If the LDTI COSEM client is a part of the third-party device, it means that the third-party device is directly compatible with the LDTI communication. If not, a gateway must translate the signal from the HAN port and transmit the translated signal to the third-party device. In practice, this means that the data from the HAN port may be decrypted by the gateway before transmitted to the HAN devices. Further, it means that what protects the meter data between the HAN port and the third-party devices is the consumer's local communication network, in this case the HAN. However, the gateway may also just function as a translator of signals, and let the decryption be done in the third-party device [20]. Figure 3.6 on page 30 shows an example of how the security environment may look like when using encryption on the HAN port data.

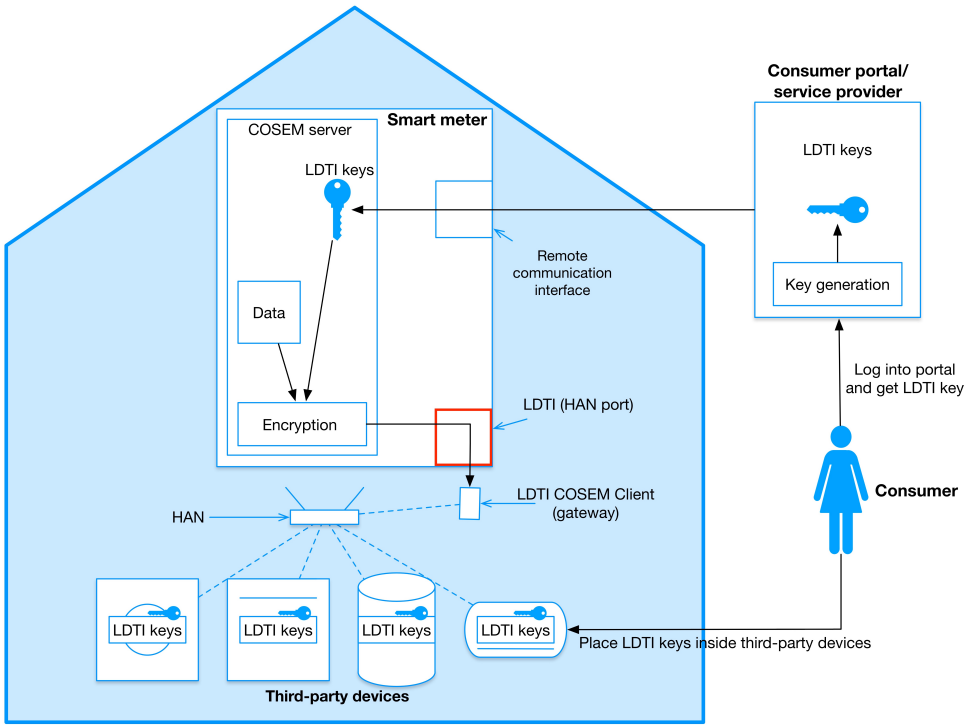

Figure 3.6: This illustration of the security environment using encryption has been inspired by [20, 51].

3.4.2 Security of the HAN Port

As this is written, the HAN port is not secured other than that it is read only and electrically secured. It is electrically secured in a way such that no electricity goes to the HAN port before it has been activated by the DSO. It is also electrically secured such that if something with conductive properties, e.g. a screw driver, is stuck inside the HAN port, the meter will not be shortened or broken. When the security solution has been finalized, it will be added to the smart metering system at the consumer's end [49].

As already discussed in the Chapter 2.5, waiting with security until the end of the installation process is not ideal. Cleveland [16], McGraw [41] and Potter and McGraw [54] all defend the idea that security should be a concern from the design process and onwards.

The following quote is from "Product description: Local HAN Interface" from Aidon [1]:

> Future functionality includes data encryption for data security and channel enabling and disabling possibilities. This functionality is managed from the business systems via the system integration interface.

Thus, the security solution regarding the data that will be available through the HAN interface is not present yet. This is not solely concerning Aidon, but all smart meter producers. The security solution will not be ready until the DSOs have decided which security solution they want to use. In the meantime, the HAN port will be closed until Jan 2019 due to privacy requirements from Datatilsynet[3], the Data Protection Authority in Norway. [47]. The fact that smart meters are being rolled out before the security solution is ready is in conflict with the claims by Cleveland, Potter and McGraw, mentioned above, that security should be kept in mind from the beginning of a design process, not postponed.

3.4.3 Encryption Algorithm

In case the choice of security solution will be encryption of HAN data, NEK has decided that the chosen encryption algorithm will be the AES-128 [47], which is the Advanced Encryption Standard (AES) with a block size of 128 bits. AES-128 is a block cipher. Since the data packets sent on the HAN port have a fixed length, the AES-128 encryption algorithm is a reasonable choice [32]. The smart meter producers and the producers of third-party equipment both must build their devices such that the chosen algorithm will be possible to implement into them [47].

[3] `https://www.datatilsynet.no`

Chapter 4
Vulnerability Study

This chapter will present the results from the applied methodology. Figure 4.1 on page 34 illustrates the steps of the vulnerability study.

First, the assets of the system will be identified. In Advanced Metering Interface (AMI) systems, **assets** include meter data especially, but they might also include information about pricing and time. However, today's solution will be to get the price information from an external service [51]. The international standard ISO/IEC 27005:2011 also uses the word 'assets' to describe values in a system [34]. The next step will be to look at where assets are saved, processed and sent. This will be the data flow analysis. After investigating where the assets are moving around in the system, the thesis will investigate attacks and threats where the motivation behind is, for example, to destroy or steal the assets. Possible attacks and threats will be presented with the attacker framework model STRIDE[1] that has been developed by Microsoft[2]. The last step will be closely connected to the previous step in order to identify the potential vulnerabilities that are revealed after the investigation.

4.1 Assets

This section identifies the assets in the AMI system within this thesis' scope, and is the first step in the vulnerability investigation. The assets are split into two groups: Primary assets and supporting assets, according to [34]. The primary assets are the information that the system shall protect. The supporting assets are assets that must be working correctly in order to protect the primary assets. Thus, the supporting assets must also be protected, and consists of hardware, software and communication (network). Table 4.1 on page 34 presents an overview of the identified assets in the AMI system.

[1] Spoofing of identify, Tampering with data, Repudiation, Information disclosure, Denial of Service, Elevation of Privileges.

[2] `https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx`

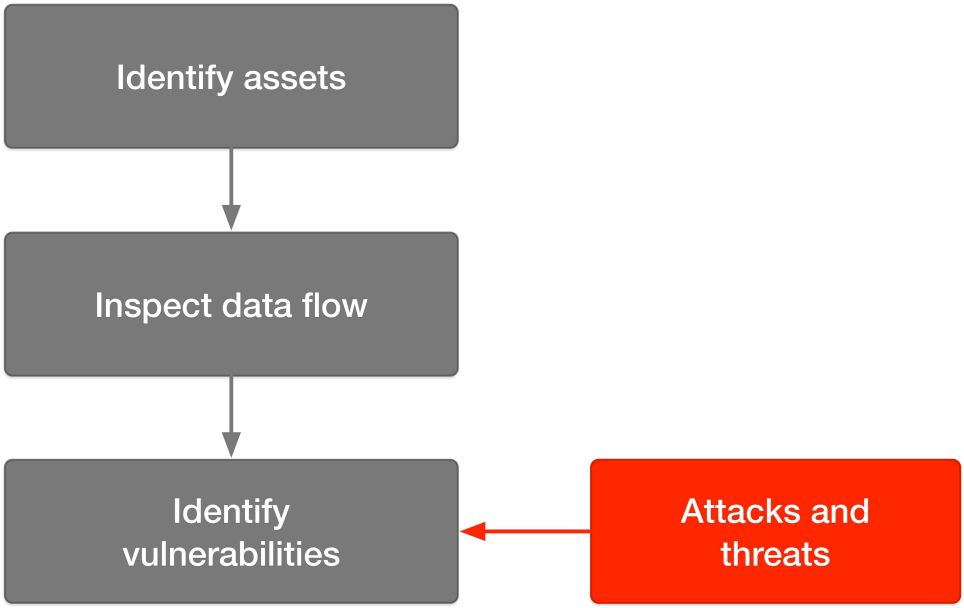

Figure 4.1: The four steps of the vulnerability study.

Table 4.1: Assets in the AMI system.

Primary assets	**Supporting assets**
Meter data	HAN port
Time of consumption	Home Area Network
Breaker functionality	

4.1.1 The Different Components of Meter Data

The meter data is the primary asset that has been given focus in this thesis. Meter data are not considered as sensitive information, but personal information that suggest something about the individual consumer, for example at which time she usually is at home or away [47]. These data have been modeled into the data flow analysis in Section 4.2. In Appendix B is the example data profile from Aidon describing what each packet of data coming out of the HAN port consist of. This profile is not the one that has been implemented into the smart meters that are being rolled out to consumers, since those meters are using OBIS codes and not this data profile. Nevertheless, the data packets will assumably contain much of the same information in both types of meters even though the data profiles are different.

The meter data contains information about the ID of the meter, the energy consumption, power, voltage, current, network frequency and the type of the meter.

4.1.2 CIA Breach on Meter Data Components

In case there is a confidentiality, an integrity or an availability breach on one or more of the components of the meter data, one can expect several results. If the network frequency is tampered with, the service might not be available as expected. If the energy consumption data (Wh) is tampered with, the integrity of the data is lost and false data are sent out from the HAN port. In case the meter data is not secured by encryption or secured within home using wired data transfer, the confidentiality of the meter data is vulnerable and can not be promised to be private only for the consumer. Potential attackers and threats are described in Section 4.3.1.

4.2 Data Flow Diagram

A DFD gives an overview of what happens to the assets in the system; how are they gathered, saved, processed and communicated. With a DFD one might easier locate where in the system there are potential vulnerabilities. The following list describes the different symbols of a DFD:

- Rectangles represent systems that receive or send data.
- Circles represent functions that processes data.
- Horizontal lines represent data storages.
- Arrows represent data flow.
- Dashed lines represent trust borders, where data flows from one zone to another zone.

Figure 4.2 on page 36 shows the data flow diagram of the smart metering system based on documentation from Aidon [4]. There is a communication interface between the smart meter's system module and the HES, another between the system module and the HAN and a third between the system module and the meter inside the smart meter. The three communication interfaces can also be observed in Figure 3.1 on page 24. With regard to the three communication interfaces, it is reasonable to think that the DFD must have three trust boundaries: one between the meter and the system module, one for the communication to the Home Area Network and that last one for communication to the Head End System.

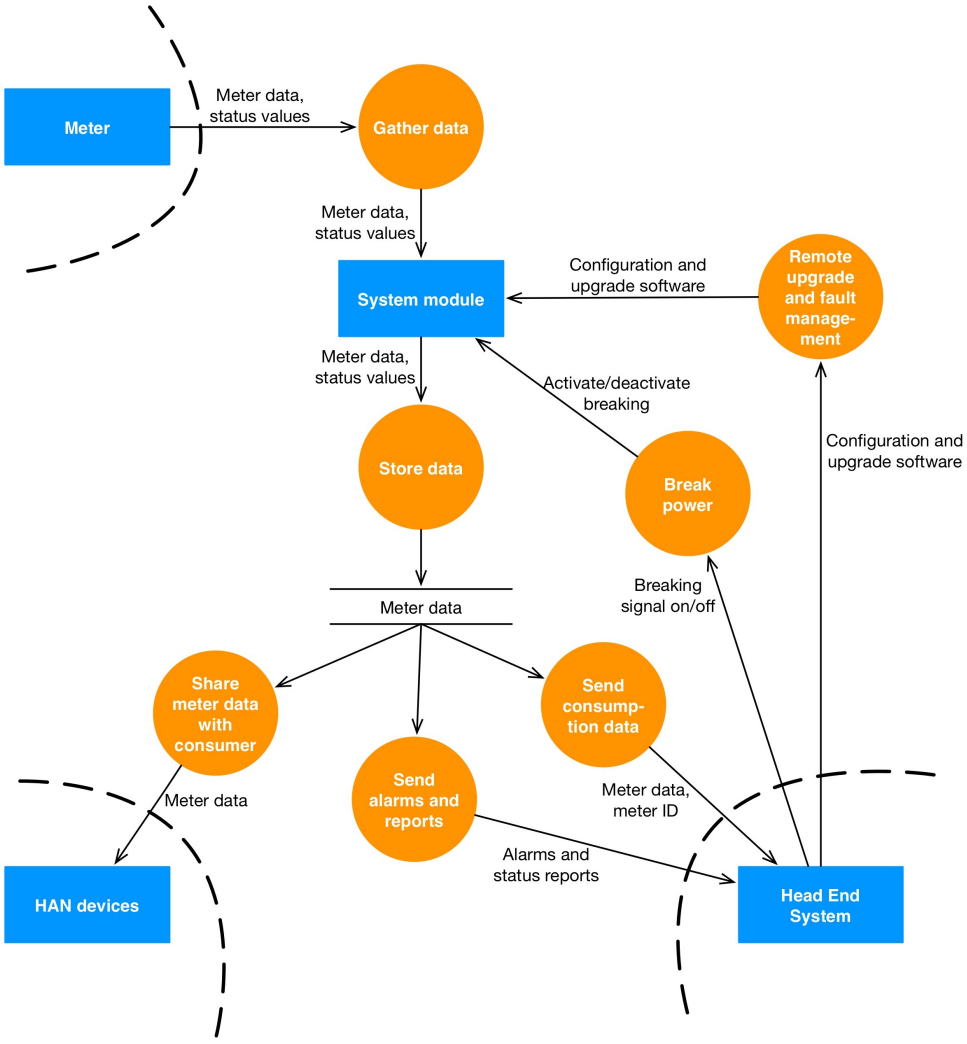

Figure 4.2: A Data Flow Digram presenting actors and processes in the smart metering system.

4.3 Attacks and Threats

Based on the identified assets in Section 4.1 and where they may be found in the system as depicted in the DFD in Section 4.2, this section will look into potential unwanted events that threatens the assets. The DFD will be used to show where the threats and attacks may occur. Looking into potential attacks and threats is useful to gain an understanding of an attacker's capabilities to carry out an attack, the motivation behind an attack and whether the attack is targeted or non-targeted.

The section will first present the different types of attackers that have motivation and capabilities to attack the AMI system through the HAN or the HAN port, and threaten the assets. Next, the attacker framework model STRIDE will be used in order to obtain a systematic process to identify the different threats to the system. Last, as a part of the motivation for this thesis and in order to highlight the potential attacks and threats, the thesis will present the attacks and threats through scenarios. The scenarios are also meant to support the scientific research with a tangible example and invite the reader to take a closer look at the problem. The scenarios will be classified according to the STRIDE framework.

4.3.1 Attacker Types

There are several people that are possible attackers for the AMI system. A brainstorming resulted in the following potential attacker types. There might be several others, so the thesis does not limit the number of attacker types and variations to the mentioned ones.

The Consumer

The consumer herself could be an attacker with the motivation to save money. In such a case, she would be interested in tampering with her own meter data that will be sent from the smart meter to the HES.

The Neighbor

In the case where the smart meters in an area has been connected to a mesh network, the neighbors could become potential attackers. If the consumer who has a master meter is able to hack her meter in some way, she could manipulate her neighbors data before they are transmitted to the HES. The motivation for such an attacker could be personal conflicts between neighbors or interest in spying.

The Angry Ex-Spouse

Domestic conflicts are not unusual and is therefore included as a potential threat. The motivation could be revenge. This attacker often has access to the house and HAN and could carry out attacks from the inside.

The Skilled Hacker

The skilled hacker could be well-educated and part of an organized criminal network anywhere in the world. These are motivatied by money. An attack could result in meter data theft, where they ask for money in return. Or worse, they could find an attacker path from HAN to HES, hijacking the breaker functionality and create a blackout. The motivation could be money or to show a political statement, like saving the environment.

The Script Kiddies

Script kiddies are individuals, kids and adults, who are uneducated when it comes to hacking and security, but have still learned hacking techniques and toolkits made by others, often through online tutorials. The script kiddies are not aware of the consequences that their scripting might lead to, and that the outcome can be harmful even if it was not intended to be harmful. Dropping a fork bomb[3] would, for a script kiddie, be a matter of curiosity where she wants to see what happens if she drops it. For instance, the bash command `:() :|:& ;:` is a fork bomb. Not knowing what it is, but still trying it out, could damage a system. In the AMI scenario, this attack could cause downtime which affects the availability of the system.

In any system, not just within the AMI systems, these attackers are not known to the users of the system and they are therefore considered as outsiders [8, 11]. The attacks are usually non-targeted.

The Social Engineer

In general, an attacker could also be a socially intelligent person who, through social engineering, would be able to trick people into sharing secret information. This information could for example be passwords, sensitive or private data. Social engineering is the act of using psychological manipulation in order to make people with authorization give away confidential information [29]. This technique does not demand any technical skills.

[3] A fork bomb is a denial of service attack where a system process is being replicated an infinite number of times, making the system run out of memory and crash [22].

4.3.2 The STRIDE Attacker Framework Model

The STRIDE framework gives an overview of several potential threats and attacks. Although the framework is not exhaustive, such that every possible threat can be covered by it, it is useful in order to brainstorm and make use of the framework to start thinking about what could go wrong in a system.

Spoofing of Identity

Spoofing of a user's identity is a masquerading attack where an adversary successfully got the user's authentication information, like her username and password. Once the attack has succeeded the adversary gains access to assets that he is normally not authorized to have access to. Such an attack may be carried out technically, for example by forging, or through a fraud scheme like social engineering [44].

Tampering

Tampering with data is a malicious modification of data, such that the data loses its integrity. The integrity of data in AMI systems is essential for, among others, billing reasons and to have correct responses to signals that steer functionality. For example, meter data must not be tampered with because the result may lead to a consumer paying more or less than her actual energy consumption. As for the correct responses to signals, the functionality must not be tampered with since it may lead to serious situations like blackouts [44, 68]

Repudiation

Repudiation has to do with attackers who deny to have performed a malicious activity when the system has insufficient recordkeeping of actions that are being executed in the system. Thus, the system lacks controls to prove that the activity in fact happened. These controls are called non-repudiation controls and they keep information about, for example, payments [44, 16].

Information Disclosure

Information disclosure is a threat that involves the exposure of data to an individual that is otherwise not supposed to have access to the data. This attack could for example occur at the HAN port, reading the meter data that is streaming from it [44].

Denial of Service

Denial of service is an attack that results in a service becoming unavailable to its users. The attack could consist of spamming an application that handles requests, so

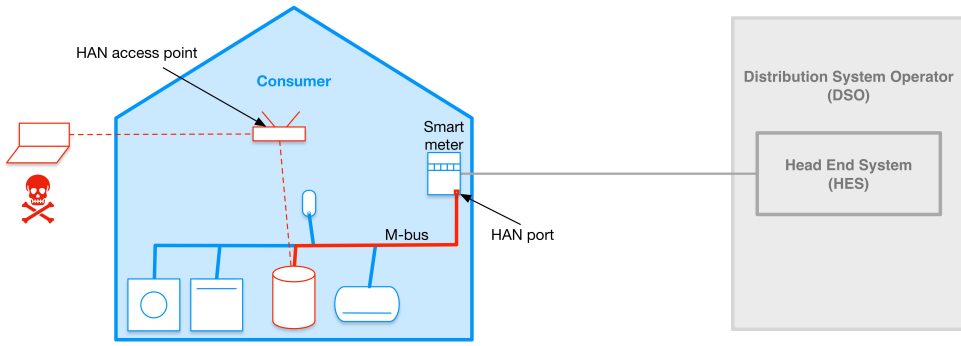

Figure 4.3: An attack via a third-party device by exploiting the operating systems in order to carry out an buffer overflow attack to make the system unavailable.

that it eventually crashes [44]. Having a look af the DFD, this attack could occur at every orange bubble, which represent functions. Spamming a function will eventually create downtime because it is overloaded.

Elevation of Privilege

Elevation of privilege is an attack where an adversary uses tools to maliciously give himself privileges to access the system. This is a hazardous attack in which the attacker becomes a part of the system and is therefore able to do much damage [44]. This includes execution of commands in the system that normally takes more than one person to carry out. In the AMI system, the breaker functionality is a capability of the system that has been decided to be carried out by at least to separate actors from the HES. Elevation of privilege is a relevant threat to this functionality.

4.3.3 Scenarios

The scenarios are based on threats and attacks that have been described in this chapter.

Scenario 1: Buffer Overflow Attack via Third-Party Equipment

The third-party equipment runs on the same network (the HAN) as the smart meter. Because of this, an attacker can potentially attack the backend over the network, via a third-party equipment. If the third-party equipment application is running on the same operative system as the smart meter does, the attacker might be able to run an arbitrary piece of code in the smart meter, and thereby manipulate data and attack the backend. Figure 4.3 on page 40 illustrates this scenario.

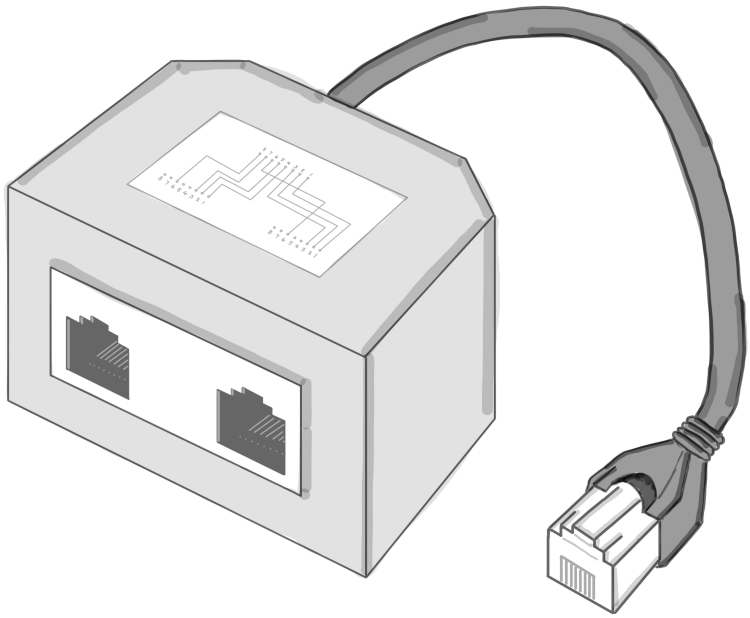

Figure 4.4: Y-splitter to split the signal that is coming from the HAN port.

- Potential attacker: Skilled hacker
- Type of attack: Denial of Service
- Location in the data flow diagram: HAN devices

Scenario 2: The Angry Ex-Spouse

This scenario considers the angry ex-spouse attacker and is based on communication with the HAN port. This type of attacker is motivated and willing to tamper with the meter data in order to enlarge the electricity bills. The way she could do this is to split the signal coming from the HAN port into one signal that goes into a computer and one that goes to the home automation system. An RJ45 Y-splitter could be used for this purpose. Figure 4.4 on page 41 shows a picture of a Y-splitter. The splitter is connected to the HAN port (RJ45 contact). A computer is connected to one of the RJ45 connectors in the Y-splitter, and a HAN adapter (dongle) to the home automation system is connected to the other.

On the computer the attacker could try to flip some of the bits coming out of the HAN port. In order to do so she must understand the output; mapping the bits with the corresponding information. If she succeeds in flipping bits, she could trick her home automation system by sending it a lower total consumption number. The result would be that the saving mode would never be used. In Appendix B there is

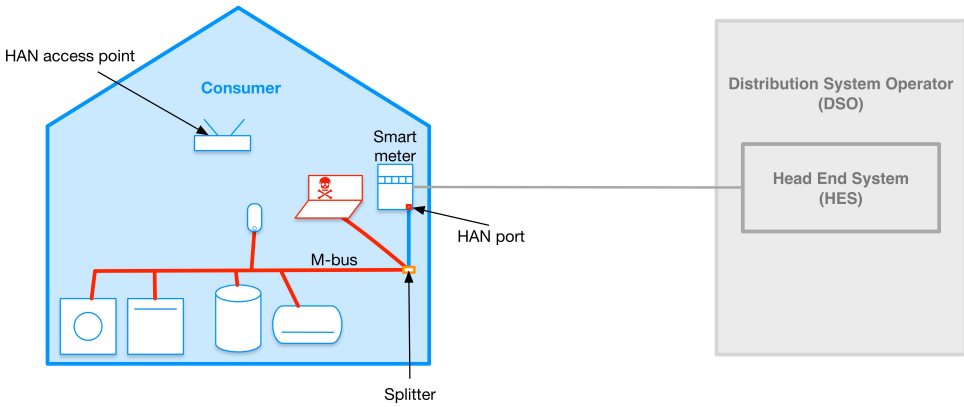

Figure 4.5: An attacker attempts to tamper with metering data that she receives from the HAN port.

an example data profile of how data packets from the smart meter borrowed from Aidon looks like. Data bits that represent information like "Active Energy Import" could be useful to flip in order to reach the attacker goal.

The scenario is illustrated in Figure 4.5 on page 42.

- Potential attacker: The angry ex-spouse
- Type of attack: Tampering
- Location in the data flow diagram: HAN port

Scenario 3: Insert False Device

This scenario considers an attacker who makes an effort to gain access to the smart meter through the HAN or the HAN port. Once he is inside the network he can place a false device onto the M-Bus that acts like any other power consuming device on the M-Bus. Since the thesis does not know what kind of protection the smart metering system has against malware, nor about the self-healing of the system, the thesis will assume that any attack like this will go through the HAN. A loophole could be a fault in the firewall implementation or a weak password to connect to the HAN. The scenario is illustrated in Figure 4.6 on page 43.

- Potential attacker: A skilled attacker
- Type of attack: Tampering
- Location in the data flow diagram: HAN devices, HAN

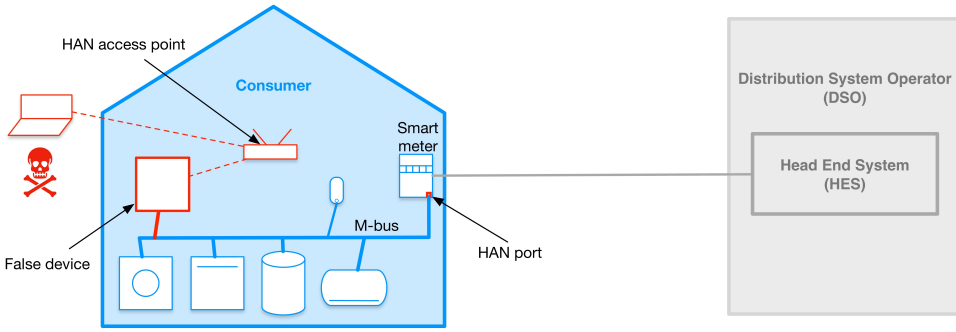

Figure 4.6: An attacker hacks into HAN and adds a virtual and malicious device to the M-Bus.

Scenario 4: Compromising the Breaker Functionality

This scenario illustrates an unwanted event where someone who is unauthorized to use the breaker functionality finds a way to compromise this functionality. This is an unwanted event that has been mentioned in [39]. It has been suggested that the breaker functionality should be controlled by two or more people to lower the risk of human error. In theory, one may always find a way to get around solutions like this by attacking a lower layer in the architecture. In case there are two people who together control the breaker functionality, an attacker can theoretically send falsified messages directly on the network, and thereby avoid the two-person check.

Figure 4.7 on page 44 shows an illustration of the attack path that an attacker may use in order to take control over the breaker signal, starting by getting access to the HAN and from there hack the smart meter. The HES and connection between the HES and the smart meter has been marked with a red dashed line to highlight that these are the actor and the communication channel that are being circumvented in this scenario.

- Potential attacker: A skilled attacker, the social engineer
- Type of attack: Elevation of privilege
- Location in the data flow diagram: System module

Scenario 5: System Module with a General Mictrocontroller Unit

At first sight, the system module inside the smart meter seems to be a candidate for hosting vulnerabilities. It has several responsibilities and controls communication with the HAN, the Distribution System Operator (DSO) and the testing communication port. If the microcontroller unit (MCU) inside the system module is not implemented

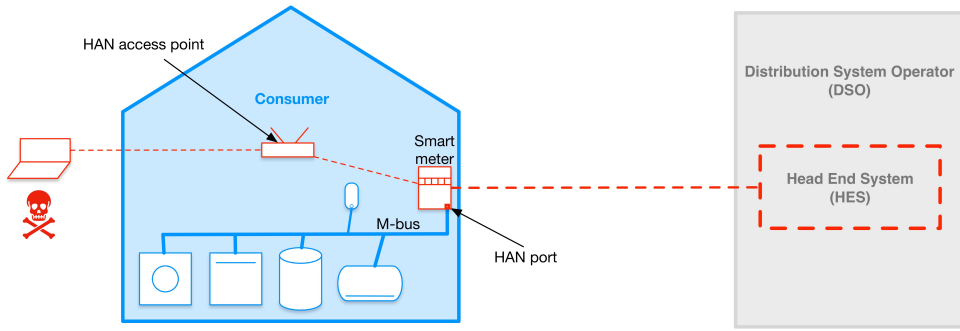

Figure 4.7: An attacker gains access to the smart meter via the HAN and is skilled enough to operate on a low layer, for example the data link layer, to get around the two-person check in order to turn on the breaker functionality.

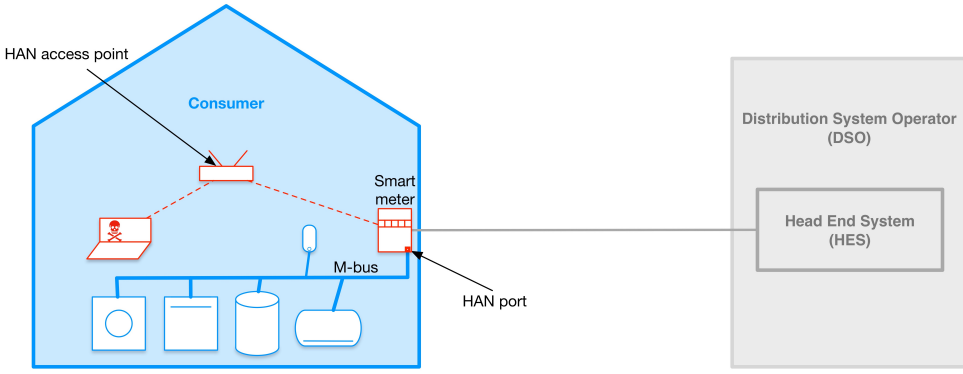

Figure 4.8: An attacker gains access to the smart meter via the HAN. The ping attack is aimed to overload the microcontroller unit (MCU) so that the smart metering system stops working.

correctly, it could be vulnerable against threats that aim at exhausting the MCU capacity. This is especially a challenge in resource-constrained IoT devices which have a small amount of processing power. Figure 4.8 on page 44 shows an illustration of this scenario.

- Potential attacker: A skilled attacker or a script kiddie
- Type of attack: Denial of service
- Location in the data flow diagram: System module

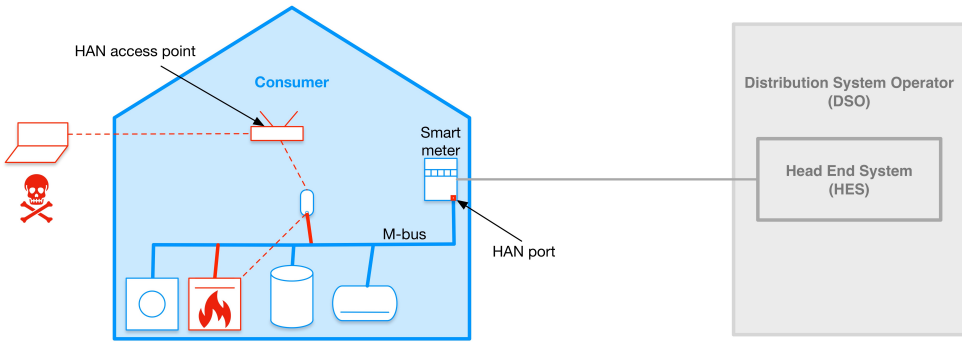

Figure 4.9: An attacker gains access to the third-party equipment via HAN and a controlling device. The attack could cause a fire if the electrical equipment is manipulated to be always on.

Scenario 6: Gain Control over Third-Party Equipment

The intruder's goal is to obtain control of the smart meter and pursue this control by taking over other devices in the Smart Home. There are numerous unwanted consequences that this attack can lead to. One of the motivations behind this attack could be to cause fire.

Third-party equipment that could be affected are for example washing machines, dishwashers, heaters, air conditioners, coffee machines, if they are connected to the M-Bus. In Figure 4.9 on page 45 this scenario is illustrated. The dish washer is the attacked device.

- Potential attacker: A skilled attacker
- Type of attack: Denial of service
- Location in the data flow diagram: System module

4.4 Identify Vulnerabilities

The six scenarios in the previous section shows that the primary assets in the system may be vulnerable towards tampering attacks. These attacks may be allowed to occur if the system components are not implemented correctly or the supporting assets are not secured properly. Thus, potential vulnerabilities may include a wrong implementation of smart meter and home automation components.

The supporting assets may be vulnerable towards denial of service attacks. Attacks that affect the supporting assets also affect the primary assets, thus indirectly the primary assets are also vulnerable to denial of service attacks in cases where there are

vulnerabilities in the HAN or the HAN port. Potential vulnerabilities in supporting assets may also include wrong implementation of components, and weak HAN protection, for example a weak password or firewall.

Chapter 5
Testing

The practical part of this thesis will be explained in this chapter. All configurations and practical setup is depicted in Appendix A.

The first section will describe the primary test setup of communication between the smart meter and a computer. This communication was established with an 4-pin connector to RS232 serial cable that was handed out together with the borrowed meter from Aidon. The next section deals with second test setup communication which was established with an M-Bus converter.

5.1 Primary Setup of Communication: RS232-to-USB Adapter

When the meter was handed out, a 4-pin connector with an RS232 plug was handed out as well. The 4-pin connector had only implemented three pins to it: PIN1, PIN3 and PIN4. Thus, one of the holes was missing a metal pin. As already explained in Chapter 3, in Norway the HAN port will only be using 2 pins, PIN1 for ground and PIN2 for M-Bus. According to [50], Aidon has been using the HAN port in other markets already. These markets needed more than two pins for the HAN port. This is why the form of the port still has 4 connection points, even though only two of them will be used in smart meters in Norway. The thesis assumes that the connector that was handed out with the thesis had either been used for communication through the HAN port in other markets or used for testing of the smart meters in Norway, at an early stage.

Figure 5.1 on page 48 shows the cable that was handed out with the meter. It shows how the 4-pin connector looks like, with one pin missing. The other end of the cable is a RS232 serial connector. This is where the RS232-to-USB adapter is connected between the serial cable and the computer.

The RS232 end of the cable needed an RS232-to-USB adapter connected to it

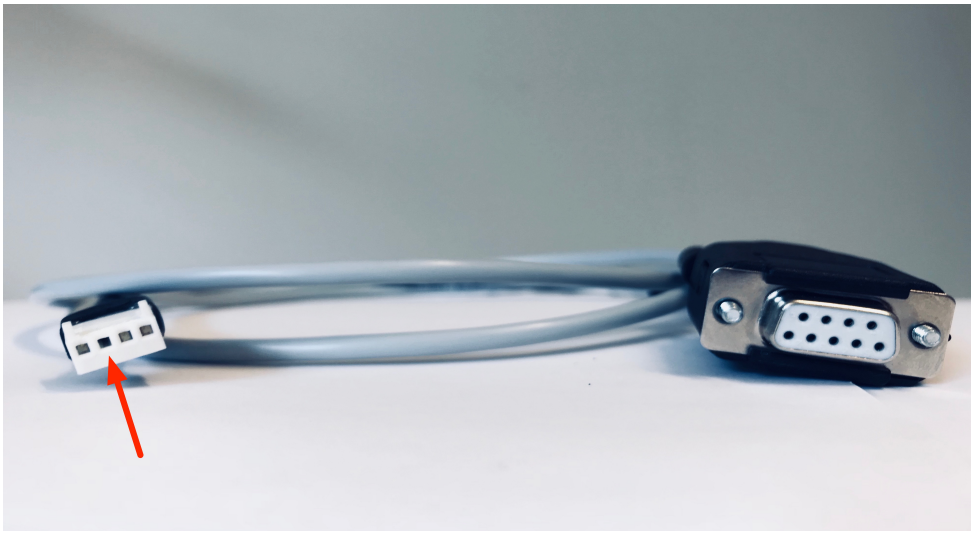

Figure 5.1: This picture shows a 4-pin connector where the missing pin is marked with the red arrow. The other end of the cable has a RS232 connector.

in order for a computer to receive the serial signal. Inside the adapter there is a little chip that needs a corresponding software driver so that the computer can read the output from it. The driver is placed between the computer's hardware and the computer program that is used to read the data. A Terminal program called Minicom was used to look at the output.

Two different adapters were tried out. The first one is depicted in Figure 5.2 on page 49. The two most common chips that are used inside RS232-to-USB adapters are the Prolific and the FTDI [13], but the corresponding drivers for these did not work for the first adapter. Numerous other drivers were installed one by one without any further luck.

Figure 5.3 on page 49 is a picture of the second RS232-to-USB adapter that was tried out in the primary testing setup. This adapter worked perfectly with the correct driver and communication was established between the computer and the smart meter. The configuration is explained in Appendix B.

Using the second RS232-to-USB adapter and the correct configurations, data from the smart meter started coming out to the Terminal. The data looked like log data and could not be understood intuitively. Through personal communication with Rolf Pedersen in Aidon the log data was established as "mysterious". The 4-pin connector used for the HAN port in Norway shall only have two pins implemented: PIN1 and PIN2. These will be used for communication over the M-Bus. This was

Figure 5.2: This picture shows the first RS232-to-USB adapter that was tried out in the primary test setup. This adapter was not possible to use.

Figure 5.3: This picture shows the second RS232-to-USB adapter that was tried out in the primary test setup.

explained in Chapter 3.3. Since only PIN1 and PIN2 are going to be used, and then only for metering data via the M-Bus, the log data was a surprising result. Based on the lack of answers found, the thesis can not present a proper explanation to these log data.

Instead, a different communication setup is needed, and it will be described in the next section. This communication setup is the one that will be implemented into the consumers' homes.

5.2 Secondary Setup of Communication: M-Bus Adapter

A problem with the communication explained in the previous section was that the pin for M-Bus was missing: PIN2. This problem could not be fixed simply by creating a new cable with 4 pins, so that data could flow out on the M-Bus to the computer. If going through with such a solution, the computer might have been damaged due to hight voltage. The M-Bus require +24V which is too high for the computer to handle as input voltage through USB[1].

In order not to ruin any hardware, an M-Bus to USB adapter is necessary. The adapter converts the signal to a lower voltage and makes it readable by the computer. The chosen adapter for this thesis is a "CP210x USB to UART Bridge Controller" from Silicom Labs. With the adapter it is possible to get the information from the HAN port that it would be sending to its slaves. Since the M-Bus is the one carrying the meter data, it is more useful than the simple log data that came out from the previous connection. Figure 5.4 on page 51 shows a picture of the M-Bus adapter.

5.3 M-Bus Output

The smart meter borrowed from Aidon has a one minute interval on the output from M-Bus. Without any load, the output looks like Figure 5.5 on page 52 shows. With load, the output looks like Figure 5.6 page 52 shows. The difference between the two outputs is that some hexadecimal numbers that first were zeros, are in the output with load not zeros anymore, due to the energy flow.

In the document "Product Description – Local HAN Interface" [1] there is one page describing the data profile of a data packet sent out from the HAN port. The data profile is included in this thesis in Appendix B. The data packets from the borrowed smart meter are coded with a data profile that is preliminary to the OBIS coding that is going to be the standard for each smart meter in Norway [50], thus it is called an "Example Data Profile".

[1] `https://support.apple.com/en-us/HT204377`

Figure 5.4: The green box is the M-Bus adapter that is connected to the HAN port. The white wire is used for ground, while the black wire is used for M-Bus. The other end of the adapter has a USB connector that goes to the computer.

To start the communication with the smart meter using Minicom, it is best to use the -H flag in order to get the output in hexadecimals.

The first 16 hexadecimals shown in each output packet is the smart meter's serial number. In the case of the meter from Aidon, the first 16 hexadecimals are "37 33 35 39 39 39 32 38 39 30 36 35 36 35 31 36" and they represent the smart meter with serial number "7359992890656516". This correlates to the serial number on the smart meter borrowed from Aidon. The marked numbers (light gray shade) in Figure 5.5 on page 52 represent one data packet sent from the HAN port on M-Bus.

5.3.1 Endianness of the Output Data

The output data of the borrowed smart meter were not straightforward to understand, even with the example data profile from Aidon in possession. Converting the numbers from hexadecimal to decimal did not give results that made sense. With time to help, eventually the code was broken. In each data packet, the first 16 hexadecimal

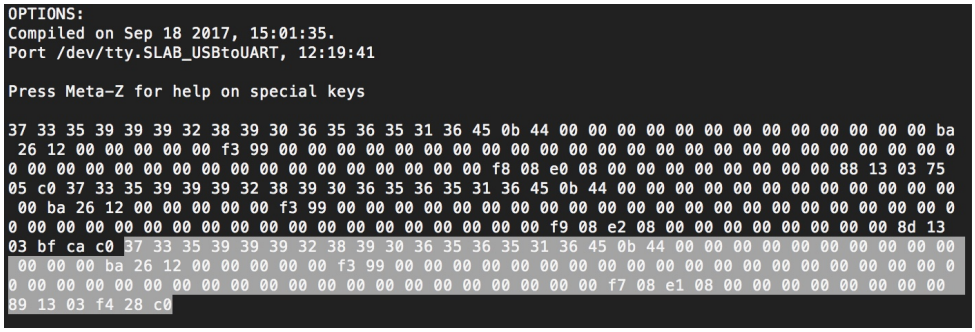

Figure 5.5: Minicom screenshot: Output from M-Bus without load.

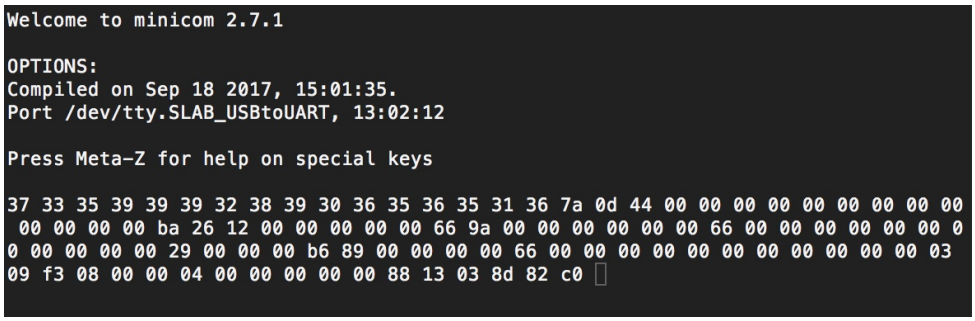

Figure 5.6: Minicom screenshot: Output from M-Bus with a Macbook and a computer screen for charging as load.

numbers that represent the serial number is stored as a string that is fixed for each transmission. These numbers must be converted in the order they are sent, from hexadecimal to ASCII.

The rest of the data packet is represented in a different manner. Each part of the data representing a single information is stored in a special byte order, also called endianness. The endianness that has been used is the little endian[2]. The next section will use the knowledge of endianness to deconstruct and convert the different parts of the data packets from the HAN port.

5.4 Deconstruction of HAN Port Data Packets

Figure 5.7 on page 55 shows the data packet that was depicted in Figure 5.3 split into blocks of hexadecimals of various sizes that each represent meter data components.

[2]When bytes are stored with little endian byte ordering, the least significant byte of the octet pair is stored in the lower order memory address and the most significant byte is stored in the higher order memory address [28].

The figure shows two versions of the splitting, called (a) and (b).

The leftmost figure, Figure (a), shows a deconstruction starting from top to bottom. Everything looks fine, the number of data blocks and their respective lengths match the example data profile. However, there is a problem. Looking at the bottom-most number, c0, this can not represent the phase of the smart meter. According to the example data profile, the phase will be 1, 2 or 3 in decimal number and must thereby be represented by hexadecimal number 01, 02 or 03.

The other prominent problem is the next to last data block with the numbers "8d 82". Remembering little endian, the byte pair will be "82 8d" which in decimal is 33421. This data block is supposed to represent the network frequency and differs extensively compared to the network frequency listed in the smart meter specification document from Aidon [3]. In the specification it says that the frequency shall be 50 Hz +/- 1 Hz. Based on this fact, the byte pair 82 8d can not represent the frequency.

Later it was learned that the last byte pair represent the stop bit, while the two next to last byte pairs represent the checksum [27].

Keeping in mind the stop bit and checksum, the data packet was split according to Figure (b). The data blocks make more sense to what they represent. In Figure (b), the data packet was split from top to bottom, except the last two blocks, which are colored yellow, that knowingly represent the stop bit and the checksum. The example data profile shows that the last 8 blocks shall be 7 double octets and finally one single octet. With the new splitting, the number that is representing the frequency is now showing a reasonable value; 50.01 Hz. This can be seen in Table 5.1 on page 54.

Since the new splitting results in a lack of hexadecimals, red question marks has been added as placeholders. It is not certain if the question marks are representing the missing hexadecimals, or if they should be placed elsewhere.

The thesis assumes that the missing bytes may have occurred when data was written to the Minicom terminal. On the other hand, writing to a file did not solve the problem either. It might also be possible that the smart meter does not always transmit full data packets, but sometimes omits three pairs of the hexadecimals.

In Table 5.1 on page 54 the data packet in Figure 5.3 on page 50 has been deconstructed according to the data profile in Appendix B, the knowledge of endianness in Section 5.3.1 and knowledge of data packet deconstruction in Section 5.4 .

Table 5.1: The output from minicom divided into blocks using the data profile from Aidon. Each block contains a piece of information that is shared with the consumer from the HAN port.

Description	**Output, raw**	**Output, converted**
Serial number of the meter	37 33 35 39 39 39 32 38 39 30 36 35 36 35 31 36	7359992890656516
Active energy import, with resolution of Wh	7a 0d 44 00 00 00 00 00	4459898
Active energy import, with resolution of Wh	00 00 00 00 00 00 00 00	0
Reactive energy import, with resolution of Varh	ba 26 12 00 00 00 00 00	1189562
Reactive energy export, with resolution of Varh	66 9a 00 00 00 00 00 00	39526
Active import power, with resolution of W	66 00 00 00	102
Active export power, with resolution of W	00 00 00 00	0
Reactive import power, with resolution of Var	00 00 00 00	0
Reactive export power, with resolution of Var	29 00 00 00	41
Angle between voltage and current L1, with resolution of 0.01 deg	b6 89 00	35254
Angle between voltage and current L2, with resolution of 0.01 deg	00 00 00	0
Angle between voltage and current L3, with resolution of 0.01 deg	66 00 00	102
Active power L1, with resolution of W	00 00 00 00	0
Active power L2, with resolution of W	00 00 00 00	0
Active power L3, with resolution of W	00 03 09 f3	4077454080
Voltage L1, with resolution of 0.1V	08 00	8
Voltage L2, with resolution of 0.1V	00 04	1024
Voltage L3, with resolution of 0.1V	00 00	0
Current L1, with resolution 0.1A	00 00	0
Current L2, with resolution 0.1A	00 ??	
Current L3, with resolution 0.1A	?? ??	
Network frequency, with resolution of 0.1A	88 13	5000
Phase	03	3
Check sum	8d 82	33421
Stop bit	c0	192

Figure 5.7: The output from Minicom depicted in Figure 5.6 deconstructed according to the example data profile in Appendix B.

5.5 Testing the Unidirectional Nature of the HAN port

Knowing that the HAN port is read only, based on standard IEC 62056-7-5, it would still be useful to test that this restriction really exist with a few commands on the command line. The serial communication with the smart meter is available through a simple file in the /dev directory. If it is possible to change this file, by writing to it, then we know for sure that there is something wrong with the read only restriction.

The following command was tested:

```
$ echo '\033' > /dev/tty.SLAB_USBtoUART
$ printf '\033' > /dev/tty.SLAB_USBtoUART
```

`\033` is the C-style octet for the escape character and removes all content in a file. When trying this command on the file where the serial connection is, the command line froze and nothing happened to the file. Both `echo` and `printf` are commands that write to files.

5.6 Results

Setting up Minicom with the M-Bus converter connected to the smart meter gave the output that is exactly what this thesis is interesting in: The meter data. The output shows that the data packets are not encrypted, but transmitted out of the HAN port in clear text. When meter data is not encrypted, its confidentiality is threatened.

In order to see with own eyes if the HAN port was read only, two write commands was sent to the HAN port. The results strengthened the fact that the HAN port is read only.

Chapter 6
Discussion

In this chapter, the findings from Chapter 4 and Chapter 5 are going to be discussed, also referring to findings in the theory in Chapter 2 and Chapter 3. The research questions that were listed in Chapter 1.7 will be used to systemize the discussion.

6.1 Research Questions Revisited

The four sub-questions among the research questions are questions that are helpful to present and discuss the results of the thesis, thus they belong to this chapter. The top questions are better fitted to present a conclusion and answers to them have therefore been included in the text in Chapter 7.

RQ1: How is the HAN port and the HAN port data secured?

The thesis confirms that the HAN port is read-only based on findings in the literature review and the testing part. The nature of the

The literature review revealed that the solution to secure the data that will be available through the HAN port has not yet been decided. Two possible solutions have been suggested, presented in Chapter 2.8. Later, in Chapter 3.4.2, it was mentioned that the solution will be ready after installation of the smart meters. This is conflicting with research-based knowledge [16, 41, 54] saying that a system's security solution should be developed from the beginning of the design process in order to better secure the system against threats and attacks.

The speed at which the smart meters are being rolled out suggests that there is a matter of urgency in the process. One might wonder if enough attention has been given to the security aspects of the product. Regarding the size of the smart meter project and how many consumers that will be affected, there also seems to be a lack of will to secure peoples data responsibly. The best practice is to include security prospects into the brainstorming and design processes. Several potential threats and

attacks might otherwise never be thought of, if not proposed as likely to happen at an early stage of development. If a developer does not think about which threats and attacks that may occur in a system, the security solution he makes will not be designed especially against these unwanted events. In this way, vulnerabilities in the system may occur.

RQ2: The smart meters have several functionalities, but only some of them are enabled. Technically, how are the rest of the functionalities disabled?

The HAN port is physically, electrically and logically secured, as this thesis has described. The results from the testing part implied it is not possible to write to the HAN, thus the logical security of the HAN port appears to be working. However, the testing was far from exhaustive. The thesis does not exclude that other commands, for example on a lower level, would yield different results.

The latter also applies to the breaker functionality. An attack against the smart meter to take control over this functionality has been presented as theoretically possible by attacking at a lower layer in the architecture. This was depicted in **Scenario 4** in Chapter 4.3.3. The thesis regards this as a serious threat if it occurs, as the result directly affects the daily life of the consumer. However, an attack like this may be technically demanding in terms of knowledge as described in Chapter 4.3.3. Therefore, the thesis considers this attack to be a less likely threat. On the other hand, using social engineering to deceive or bribe controllers at the HES in order to compromise the breaker functionality is perhaps a more likely scenario.

Due to the lack of information about possible functionalities of the meter, it is challenging to find the full answer to this research question. This problem has been mentioned in Chapter 6.2.

RQ3: Which threats and attacks via the HAN or the HAN port against the smart meter are likely to occur? What is the motivation behind them and how may they be performed?

The threat towards the breaker functionality has already been discussed in the previous research question. Other potential threats and attacks are likely to be denial of service (DoS) attacks and tampering attacks, which were the results from the vulnerability study.

Scenario 1 is a DoS attack that may be a threat if the security at the operating system layer has vulnerabilities. This threat could be related to weaknesses in code as a result of wrong approach towards best practice. With that in mind, the attack is likely to happen. However, the attacker should have experience in order to carry

out this attack. The attacker's motivation may not be strong enough to match the amount of effort behind the attack. The thesis suggests that best practice should be considered as a supporting asset in itself, by hardware and software developers, in order to protect important functions in a system.

Scenario 2 describes an attacker who has a strong motivation and access to the house. The scenario is likely to happen in a house where the involved parties are enthusiastic about home automation and have enough knowledge of how the system works. In case the HAN data is encrypted, the consumer will get the decryption key from a portal on the web. The attacker could use social engineering to try to get the password to the portal, or even the decryption key, from the consumer. This is not unlikely to happen, since most people who live together trust each other. The attack is not impossible to carry out for a person with no hacking experience, if enough information on the attack is available. There are often ready-to-use attacks available on the Internet, or information about how they may be carried out.

Scenario 3 depends on the security of the HAN and how the M-Bus works when new devices are added to it. If a new device is suddenly added, by an unauthorized person, there should be an alarm. If the attacker masquerades himself, it is harder to prevent. The thesis regards the motivation behind this attack to be low, since the attempt to attack might produce little gains. It all depends on what the attacker can gain through the false device he added to the M-Bus. He could potentially make the electricity bills bigger in a similar way as the attacker in Scenario 2 did. However, the attacker in Scenario 2 is personally involved, with a targeted motivation, and the attacker described in Scenario 3 is not.

Scenario 5 has two potential attackers. The skilled attacker who knows what he is doing and the script kiddie who got into the system by chance and may try to ping the microcontroller (MCU) an arbitrary amount of times without thinking about the consequences. Again, this is a matter of security from the design process and onwards and best practice during implementation. An implementation fault could result in a vulnerability in the MCU where it fails to manage its processes. The attack demands either time and luck, or a to be carried out by a skilled attacker. It is not the biggest threat against the smart meter.

Scenario 6 is a DoS attack that could result in a fire. In general, fuses would turn off the electricity in case the electrical system is stressed. However, if considering a case where the fuses in the house do not work correctly, this attack is realistic.

RQ4: How may the attacks affect the assets that the system shall protect?

Primary assets may be tampered with and supporting assets may be suffering from DoS attacks. As have been explained in Chapter 4.1, the supporting assets are significant assets in the system in order to protect the primary assets. Several of the potential attacks and threats in the scenarios deliberated in this thesis affects the availability of the system. A smart meter system that has been affected by a DoS attack may not provide the consumer with the meter data, the primary assets, that has been promised.

An improper implementation of the HAN or HAN port could also create vulnerabilities that may directly jeopardize the security of the primary assets and leave the assets vulnerable to tampering attacks.

6.2 Challenges with the Thesis

There have been several challenges during the work on this thesis. The smart meters are being rolled out in parallel with this thesis being written. Since the smart meters are currently a trending topic, the newspapers watch the actors of the smart meters intently. Thus, there is little interest from the DSOs in sharing documentation on architecture and functionality on a detailed and lower level with anyone. This resulted in a black box situation, where the thesis had to make several assumptions where the documentation was lacking.

The other challenge was about the testing part. Ideally there would have been a lot more testing during the thesis, but the HAN port showed to be well-secured due to its read-only implementation. Since the thesis' scope was limited to the HAN and the HAN port, looking at other ports on the smart meter was out of scope. The fact that the HAN port was proven to be read only resulted in a limited practical part of the thesis. This made the theoretical part even more important to do thoroughly.

Chapter 7
Conclusion and Future Work

In this thesis, the functionality and the security of the Home Area Network (HAN) port in smart meters have been discussed. The main focus has been to investigate the HAN and the HAN port in order to identify potential vulnerabilities. Both a theoretical and a practical approach to the problem were brought about through literature reviews, a vulnerability study and a testing part. The results from the testing part and the literature review confirmed that the HAN port is read-only. The threats and attack scenarios that were developed during the vulnerability study have given the potential vulnerabilities a tangible form. Attacks that appears to be the most prominent ones to the HAN and HAN port are denial of service (DoS) and tampering attacks. Vulnerabilities that may occur in the HAN and the HAN port are improper implementation of different components that the smart metering system consists of, weak network password or weaknesses in the firewall. The smart meter may also be vulnerable to social engineering. The vulnerabilities' likelihood of occurrence varies depending on the motivation behind the attacks, the technical complexity of the attacks and whether the components in the smart meter and devices in the smart home have been implemented correctly.

The thesis can be regarded as a study that explores what to expect from attacks and threats towards the Home Area Network (HAN) and the HAN port, as well as thoughts on what to expect from a security solution. It has been discussed that awareness of threats, attacks and designing a security solution should be included from the beginning of a development process. This way, the number of potential vulnerabilities that may occur in the system will decrease. Since the security of smart meter depends on how its components have been implemented, not only the anticipated encryption solution, this must also be taken into account during the early stage of the development of smart metering systems.

The vulnerability investigation in the HAN and HAN port can be further worked on by planning the attacks in more detail, set up a network to work as HAN, attach devices onto a wireless M-Bus or a similar technology. Then the attacks may be

executed in order to see how the system reacts and if the assets will be affected.

To investigate the smart metering system for vulnerabilities on a larger scale, the other two ports of the smart meter, the testing port and the one that communicates with the Head End System may be studied. The AMI channel is especially important for billing and safety reasons. Metering data must not lose its integrity before transmitted onto the AMI channel. A scenario about "sneaky consumers" could be developed in order to investigate if consumers are able to tamper with their metering data with the motivation to get smaller electricity bills. Another important asset is the breaker functionality. In future work, one may look into detail of how this functionality is secured on higher and lower levels. The breaker functionality should be protected extensively to withstand attacks that aim to create large-area blackouts.

References

[1] Aidon Ltd. Product description: Local HAN Interface. 2005.

[2] Aidon Ltd. Aidon HAN Adapter – Installasjonsveiledning. (Versjon 1.1 A):1–5, 2015.

[3] Aidon Ltd. Aidon 6530 series 4-wire polyphase dc meters. pages 1–8, 2016.

[4] Aidon Ltd. Aidon RF2 System Modules – Product Description – Version 1.5 A – Public. pages 1–18, 2017.

[5] Aidon Ltd. Aidon Security Solution – Product Management – Confidential. 2017.

[6] James M. Anderson. Why we need a new definition of information security. *Computers & Security*, 22(4):308–313, 2003.

[7] Rolf Andresen. Personal communication, February 2018. TrønderEnergi Nett AS.

[8] William A. Arbaugh, William L. Fithen, and John McHugh. Windows of vulnerability: A case study analysis. *Computer*, 33(12):52–58, 2000.

[9] Standard Online AS. Standardisering. `https://www.standard.no/standardisering/`, March 2018.

[10] DLMS User Association. What is COSEM? `http://www.dlms.com/faqanswers/generalquestions/whatiscosem.php`, March 2018.

[11] Richard Barber. Hackers Profiled — Who Are They and What Are Their Motivations? *Computer Fraud & Security*, 2001(2):14–17, 2001.

[12] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3):523–548, 2010.

[13] Jacob Davis Campbell Scientific. How to handle common issues with USB to rs-232 adapter cables. `https://www.campbellsci.com/blog/usb-rs-232-adapter-cable-issues`, March 2018.

[14] Clayton M Christensen. *The Innovator's Dilemma*, volume 24. 1997.

[15] Pilita Clark and Sam Jones. GCHQ intervenes to secure smart meters against hackers, March 2016. [Accessed: April 9, 2018].

[16] Frances M. Cleveland. Cyber security issues for Advanced Metering Infrastructure (AMI). *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–5, 2008.

[17] Ilhami Colak, Seref Sagiroglu, Gianluca Fulli, Mehmet Yesilbudak, and Catalin Felix Covrig. A survey on the critical issues in smart grid technologies. *Renewable and Sustainable Energy Reviews*, 54:396–405, 2016.

[18] Steven Dougherty and Takaki Saitoh. Smart Meter Deployment Threat and Vulnerability Analysis and Response. 9:199–213, 2015.

[19] EN 13757-2 Communication systems for and remote reading of meters - Part 2: Physical and link layer. Standard, International Organization for Standardization, Geneva, CH, February 2005.

[20] EN 62056-7-5:2016 Electricity metering data exchange - The DLMS/COSEM suite - Part 7-5: Local data transmission profiles for Local Networks (LN). Standard, International Organization for Standardization, Geneva, CH, December 2016.

[21] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, 14(4):944–980, 2012.

[22] GeeksforGeeks A Computer Science Portal for Geeks. Fork() bomb. `https://www.geeksforgeeks.org/fork-bomb/`, March 2018.

[23] International Organization for Standardization. The main benefits of iso standards. `https://www.iso.org/benefits-of-standards.html`, March 2018.

[24] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 2013.

[25] Hafslund. Informasjon om automatisk strømmåler (AMS-måler). `https://www.hafslundnett.no/kunde/info_om_amsmaaler/15522`, March 2018.

[26] Hafslund. Slik fungerer den nye strømmåleren. `https://www.hafslundnett.no/kunde/veiledning/15478`, March 2018.

[27] Joar Harkestad. Personal communication, April 2018. Hark Technologies.

[28] Paul Hoffman and Francois Yergaeau. UTF-16, an encoding of ISO 10646. Rfc, Network Working Group, February 2000.

[29] Interpol. Social engineering fraud. `https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud`, April 2018.

[30] Offentlig Isbn and Prosjektnr Nve. *AMS — Tilleggstjenester . Tredjepartsadgang Utarbeidet for NVE*. Number 978. 2011.

[31] ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management. Standard, International Organization for Standardization, Geneva, CH, June 2005.

[32] ISO/IEC 18033-3:2010 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. Standard, International Organization for Standardization, Geneva, CH, December 2010.

[33] ISO/IEC 27002:2017 Information technology - Security techniques - Code of practice for information security controls . Standard, International Organization for Standardization, Geneva, CH, March 2017.

[34] ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management. Standard, International Organization for Standardization, Geneva, CH, March 2011.

[35] ISO/IEC/IEEE 24765:2017 Systems and software engineering — Vocabulary. Standard, International Organization for Standardization, Geneva, CH, June 2017.

[36] Martin Gilje Jaatun. Hunting for aardvarks: Can software security be measured? *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7465 LNCS:85–92, 2012.

[37] Yasin Kabalci. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews*, 57:302–318, 2016.

[38] Bill Lichtensteig, Branko Bjelajac, Christian Mueller, and Christian Wietfeld. RF Mesh Systems for Smart Metering: System Architecture and Performance. *2010 First IEEE International Conference on Smart Grid Communications*, pages 379–384, 2010.

[39] Maria Bartnes Line, Inger Anne Tøndel, Gorm Johansen, and Hanne Sæle. Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer. 2014.

[40] Enrico Lovat and Florian Kelbert. Structure matters - A new approach for data flow tracking. *Proceedings - IEEE Symposium on Security and Privacy*, 2014-Janua:39–43, 2014.

[41] Gary McGraw. Software Security: Building Security In. *Addison-Wesley Professional*, 1(9):662–665, 2012.

[42] Tiago Mendes, Radu Godina, Eduardo Rodrigues, João Matias, and João Catalão. *Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources*, volume 8. 2015.

[43] Mark S Merkow and Jim Breithaupt. *Information Security: Principles and Practices*. 2014.

[44] Microsoft. The STRIDE threat model. `https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx`, March 2018.

[45] Yilin Mo, Tiffany Hyun Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[46] S. P. S. Gill N. K. Suryadevara, S. C. Mukhopadhyay, S. D. T. Kelly. WSN-based smart sensors and actuator for power management in intelligent buildings. *IEEE/ASME Transaction on Mechatronics*, 20(2):564 – 571, 2014.

[47] NEK and Lars Ihler. Vedlegg 1 – HAN Personvern – et tillegg til utredningen « AMS + HAN – om å gjøre sanntid måledata tilgjengelig for forbruker ». pages 1–10, 2017.

[48] Norsk Elektroteknisk komite. AMS + HAN, om å gjøre sanntid måledata tilgjengelig for forbruker. Technical report, 2015.

[49] Rolf Pedersen. Personal communication, November 2017. Aidon.

[50] Rolf Pedersen. Personal communication, March 2018. Aidon.

[51] Rolf Pedersen. Personal communication, April 2018. Aidon.

[52] Rolf Pedersen. Personal communication, February 2018. Aidon.

[53] Margherita Peruzzini, Michele Germani, Alessandra Papetti, and Andrea Capitanelli. Smart home information management system for energy-efficient networks. *IFIP Advances in Information and Communication Technology*, 408:393–401, 2013.

[54] Bruce Potter and Gary McGraw. Software security testing. *Security & Privacy, IEEE*, 2(5):81–85, 2004.

[55] The Norwegian Water Resources and Energy Directorate (NVE). Ams. `https://www.nve.no/reguleringsmyndigheten-for-energi-rme-marked-og-monopol/sluttbrukermarkedet/ams/`, March 2018.

[56] The Norwegian Water Resources and Energy Directorate (NVE). Network regulation. `https://www.nve.no/energy-market-and-regulation/network-regulation/`, April 2018.

[57] The Norwegian Water Resources and Energy Directorate (NVE). Ny teknologi og forbrukerfleksibilitet. `https://www.nve.no/reguleringsmyndigheten-for-energi-rme-marked-og-monopol/sluttbrukermarkedet/ny-teknologi-og-forbrukerfleksibilitet/`, March 2018.

[58] The Norwegian Water Resources and Energy Directorate (NVE). Smarte strømmålere (ams). `https://www.nve.no/stromkunde/smarte-strommalere-ams`, March 2018.

[59] The Norwegian Water Resources and Energy Directorate (NVE). System operation in the norwegian power system. https://www.nve.no/energy-market-and-regulation/system-operation-in-the-norwegian-power-system/, April 2018.

[60] Hanne Sæle, Maria Bartnes, Boye A. Høverstad, and Martin Gilje Jaatun. *Evaluering av NVEs veileder til sikkerhet i AMS Konsulentrapport utarbeidet for NVE.* 2017.

[61] SINTEF for Norges vassdrags- og energidirektorat (NVE). Risikovurdering av AMS. 2012.

[62] Mikko T Siponen and Harri Oinas-kukkonen. A Review of Information Security Issues and Respective Contributions. *The Data Base for Advances in Information Systems*, 38(1):60–80, 2007.

[63] Frank Skapalen. Veileder til sikkerhet i avanserte måle- og styringssystem. 2012.

[64] John A. Stankovic. Real-time computing. *Wikipedia*, (Figure 1):1–19, 1992.

[65] S Tan, D De, W Z Song, J Yang, and S K Das. Survey of Security Advances in Smart Grid: A Data Driven Approach. *IEEE Communications Surveys & Tutorials*, 19(1):397–422, 2017.

[66] Techopedia. Microcontroller. https://www.techopedia.com/definition/3641/microcontroller, March 2018.

[67] C W Ten, C C Liu, and G Manimaran. Vulnerability assessment of cybersecurity for SCADA systems. *Power Systems, IEEE ...*, 23(4):1836–1846, 2008.

[68] Inger Anne Tøndel, Martin Gilje Jaatun, and Maria Bartnes. Security Threats in Demo Steinkjer; Report from the Telenor-SINTEF collaboration project on Smart Grids. 2012.

[69] Inger Anne Tøndel, Martin Gilje Jaatun, and Maria Bartnes Line. Threat modeling of AMI. *Lecture Notes in Computer Science*, 7722 LNCS(Section 6):264–275, 2013.

[70] Joern Trefke, Sebastian Rohjans, Mathias Uslar, Sebastian Lehnhoff, Lars Nordström, and Arshad Saleem. Smart Grid Architecture Model use case management in a large European Smart Grid project. *4th IEEE PES Innovative Smart Grid Technologies Europe*, (978):1–5, 2013.

[71] Arne Venjum. Informasjon til kundene via HAN-grensesnittet i AMS-måleren. OBIS-koder. *18.03*, pages 1–4, 2016.

[72] Rossouw Von Solms and Johan Van Niekerk. From information security to cyber security. *Computers and Security*, 38:97–102, 2013.

[73] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys and Tutorials*, 15(1):5–20, 2013.

[74] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292–2330, 2008.

[75] Shu Yinbiao, Kang Lee, Peter Lanctot, Fan Juanbin, Hu Hao, Bruce Chow, Jean-Pierre Desbenoit, Guido Stephan, Li Hui, Xue Guodong, Simon Chen, Daniel Faulk, Tomas Kaiser, Hiroki Satoh, Ouyang Jinsong, Wang Shou, Zhen Yan, Sun Junping, Yo Haibin, Zeng Peng, Ling Dong, and Wang Qui. Internet of Things: Wireless Sensor Networks. *Internation Electronic Commision*, (December):1–78, 2014.

Appendix A
Configuration

A.1 Setup of smart meter-computer connection

The RS232 serial cable is an old standard for serial communication transmission. Most computers nowadays do not have a port for RS232 anymore, which also goes for the MacBook Pro used in this thesis. To solve this problem, a RS232-to-USB adapter is attached to the serial cable. The adapter converts the serial data signals into USB data signals. In practice this conversion is carried out by a chip inside the converter that translates serial data signals to USB data signals by applying the correct voltages on the incoming serial signals.

The next step is to install a driver that can process and understand the data signals coming from the serial-to-usb converter. The choice of driver depends on the chip inside the adapter[1]. The adapter used in this thesis is a ST Lab USB to Serial Port Adapter with a Prolific PL-2303 chipset. The installed driver is also called Prolific PL-2303.

The only thing missing after installing the correct driver is to find a good terminal software for the serial port communication. There are several good programs to choose among. One example is Serial[2] for macOS which have a nice GUI and intuitive use. Unfortunately it cost some money. Then there is Terminal[3], compatible with Windows and is easy to use. This thesis prefers to use Minicom[4] as much as possible. It is text-based and used from the terminal emulator. It is both easy and free to use.

To be able to get understandable information from the connection with the smart meter, the correct baud rate, parity bits and stop bits for the smart meter needs to be configured in Minicom. Type `minicom -s` and go to "Serial port setup". Figure A.1 on page 70 shows a screenshot of these settings in Minicom. As depicted by setting

[1] `https://pbxbook.com/other/mac-tty.html`
[2] `https://www.decisivetactics.com/products/serial/`
[3] `https://sites.google.com/site/terminalbpp/`
[4] `https://help.ubuntu.com/community/Minicom`

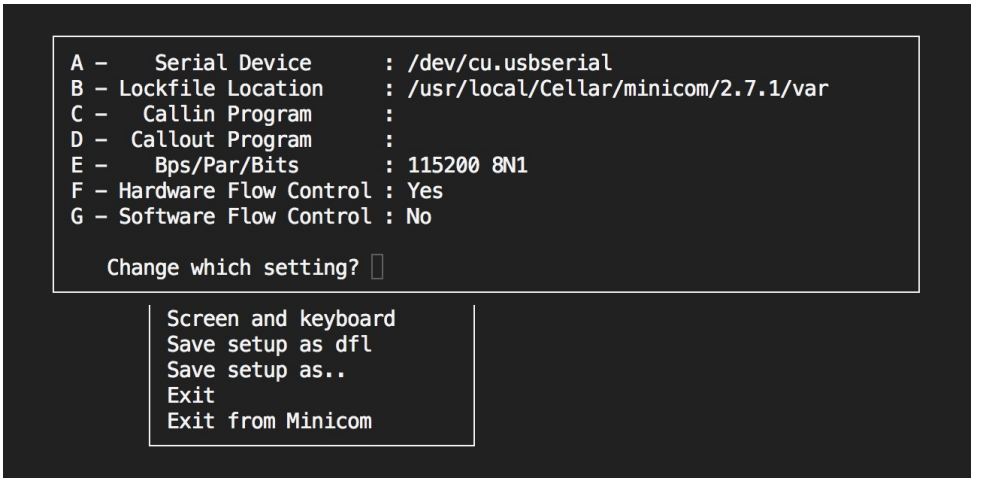

Figure A.1: Serial port setup in Minicom.

E, the baud rate is 115200 pits per second (bps), the parity bit is 0 and the stop bit is 1. This information exist in the smart meter documentation. For the smart meter Aidon provided, the baud rate was supposed to be 9600 bps [1], but this setting only gave gibberish as output. 9600 bps and 115200 bps are the two most common baud rates. When testing the communication with 115200 bps as baud rate setting, the output that came out was understandable log data. It could be that someone who had borrowed the meter before had changed the baud rate.

The RS232 serial cable has a Molex/4WAY 4-pin connector in the end that connects to the HAN port. Only had 3 out of 4 possible pins in the contact point. With a little investigation it turned out the missing pin belonged to the +24V M-Bus TXD [1].

A.2 Setup of Communication With a CP210x USB to UART Bridge Connector

In order to get more useful information from the HAN port, it is necessary to make use of the M-Bus connection. To work out the problem with a +24V M-Bus connected to the computer, a device to do voltage regulation is needed. The CP210x USB to UART Bridge Controller from Silicon Labs is the M-Bus adapter used in this thesis. A suitable driver can be downloaded from Silicon Labs webpages[5].

[5] `https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers`

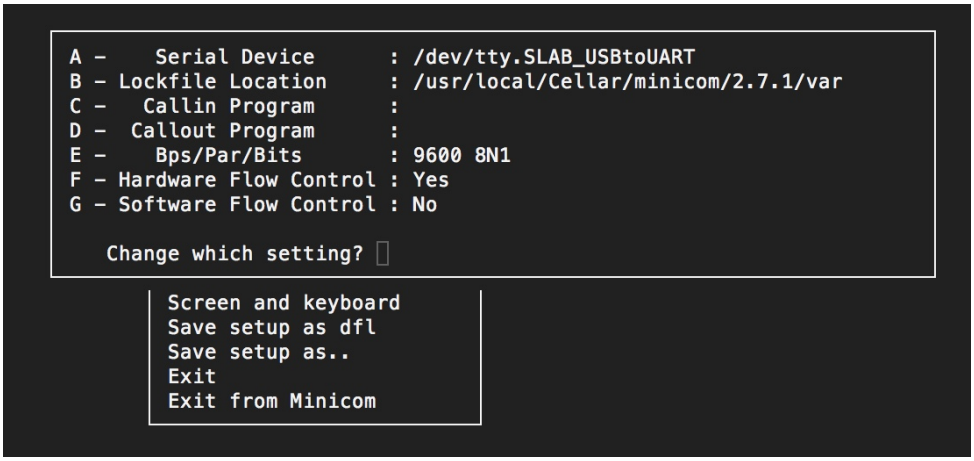

Figure A.2: Serial port setup in Minicom, when using the M-Bus adapter

The USB device was at first not listed in /dev as a virtual serial port, but as soon as the driver was installed, it appeared in the /dev directory. The same problem is explained on this Stack Overflow webpage[6]. Once the path to the correct serial device is found, Minicom can be configured to the correct settings. See Figure A.2 on page 71 for how it looks like in this case.

When all settings are done, run Minicom with the command `minicom -H` to get output in hexadecimal. If no argument is given, the output is in ASCII and only the smart meter serial number is shown in clear text, the rest is just garbage. Hexadecimal gives useful output.

Minicom defaults to no line wrap, so the output is only on one line and exceeds the Terminal windows. The line wrap setting can be changed to yes as shown in Figure A.3 on page 72.

[6] `https://stackoverflow.com/questions/47109036/cp2102-device-is-not-listed-in-dev-on-macos-10-13`

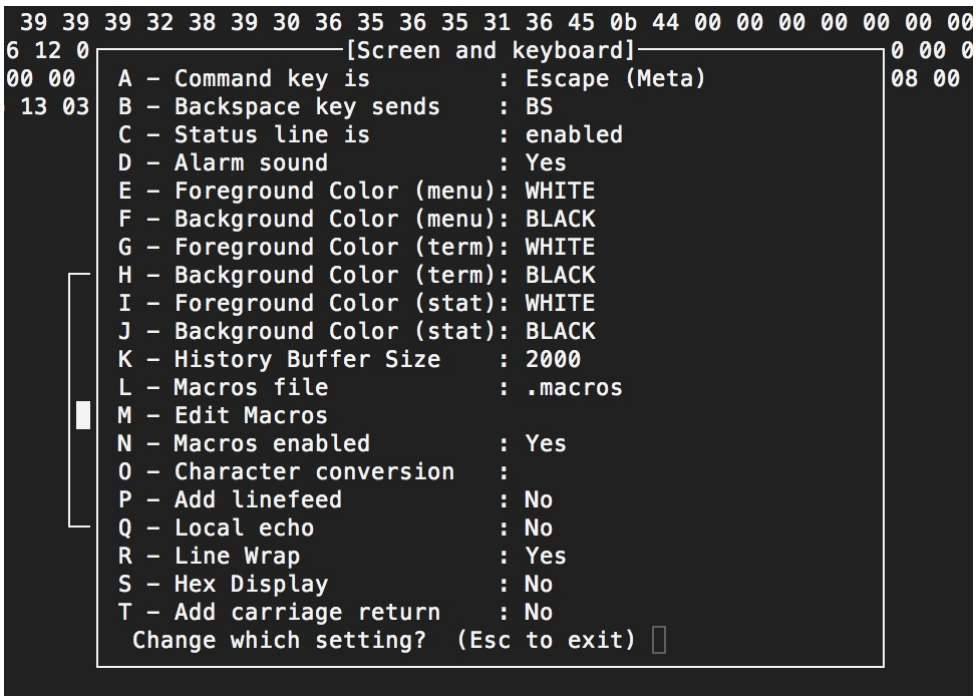

Figure A.3: Minicom settings, set linewrap to yes.

Appendix B
Example Data Profile

In the document "Product Description – Local HAN Interface" from Aidon, the authors have listed a description of the output data packets from the HAN port. This is called the "Example Data Profile" and is the predecessor of the OBIS codes. The smart meters that are being installed in the consumers' homes will not use this data profile, but the OBIS codes. Figure B.1 on page 74 shows this data profile.

Field	Data type	Description
METERID	U8[16]	Serial number of the meter
A+	U64	Active Energy import, with resolution of Wh
A-	U64	Active Energy export, with resolution of Wh
R+	U64	Reactive Energy import, with resolution of Varh
R-	U64	Reactive Energy export, with resolution of Varh
P+	U32	Active import power, with resolution of W
P-	U32	Active export power, with resolution of W
Q+	U32	Reactive import power, with resolution of Var
Q-	U32	Reactive export power, with resolution of Var
Phi1	U16	Angle between voltage and current L1, with resolution of 0.01 deg
Phi2	U16	Angle between voltage and current L2, with resolution of 0.01 deg
Phi3	U16	Angle between voltage and current L3, with resolution of 0.01 deg
P1	U32	Active power L1, with resolution of W
P2	U32	Active power L2, with resolution of W
P3	U32	Active power L3, with resolution of W
U1	U16	Voltage L1, with resolution of 0.1V
U2	U16	Voltage L2, with resolution of 0.1V
U3	U16	Voltage L3, with resolution of 0.1V
I1	U16	Current L1, with resolution of 0.1A
I2	U16	Current L2, with resolution of 0.1A
I3	U16	Current L3, with resolution of 0.1A
F	U16	Network frequency, with resolution of 0.01Hz
PHASES	U8	Type of the meter 1 = single phase meter 2 = three wire meter (phases 1 and 3) 3 = four wire meter (phases 1, 2 and 3)

Figure B.1: The example data profile from Aidon that describes the contents of each data packet sent from the HAN port. A new packet arrives once every minute from the borrowed smart meter. The table is taken from [1].