TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Madis Männik 182516IVCM

SMART METER THREAT DETECTION BASED ON LOG ANALYSIS

Master's thesis

Supervisor: Gabor Visky

MSc in Information Engineering

Tallinn 2021

Acknowledgements

I would first like to thank my thesis advisor MSc Gabor Visky at The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). He provided more support than I asked. My supervisor made this possible by finding timeslots in the early morning or late in the evening, even if this stretched his days even longer and more exhausting than needed. He also consistently allowed this paper to be my work, guiding and pointing out thoughts and feedback related to this work.

I would also like to express my gratitude to Elektrilevi OÜ and Enefit Connect OÜ for providing me tools, support and time to concentrate on this research work. These companies also provided me with excellent knowledge and experience of the energy sector and the operation of the smart grid.

Additionally, I would like to thank my family and close friends for supporting this work with resources of time and knowledge.

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Madis Männik

14.05.2021

Abstract

Smart meters, which are connected to the network, are being installed all over the world as a system that will help to make the network more efficient and resilient. It is often overlooked that increasing numbers of devices connected to a network are also increasing potential cyber-attacks to be made.

This master's thesis discusses log collection methods from smart meters and data concentrators, smart meter log analysis and different attack vectors of smart meter network.

This paper will output recommendations for device manufacturer and utility, which events could be monitored and which should be monitored to provide integral visibility over smart meter network.

This thesis is written in English and is 83 pages long, including 8 chapters, 23 figures, and 4 tables.

Annotatsioon

Küberturbe sündmuste tuvastamine kaugloetavate arvestite logide abil

Võrku ühendatud kaugloetavaid arvesteid paigaldatakse ülemaailma kiire tempoga, eesmärgiga muuta elektrivõrgu teenust efektiivsemaks ning kerksamaks. Tihti jääb aga küberturvalisuse pool vajaliku tähelepanuta, kuna kasvava võrku ühendatud seadmete arvuga kasvab hüppeliselt ka potentsiaalsete rünnakute oht.

Antud magistri kraadi diplomitöö kirjeldab logide korjet kaugloetavatest arvestitest ning andme konsentraatoritest, kaugloetavate arvestite logi analüüsist ning erinevatest ründe vektoritest kaugloetavate arvestite võrgu vastu.

Antud töö väljundiks on soovitused seadme tootjale ning võrguteenuse pakkujale, milliseid sündmusi on võimalik jälgida ning milliseid sündmusi peaks jälgima, et tagada terviklik ülevaade võrgu toimivusest.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 83 leheküljel, 8 peatükki, 23 joonist, 4 tabelit.

List of abbreviations and terms

AMI	Advanced Meter Infrastructure
APN	Access Point Name
bps	Bits Per Second
CCD COE	The NATO Cooperative Cyber Defence Centre of Excellence
CPU	Central Processing Unit
ENCS	European Network for Cyber Security
EV	Electric Vehicle
GDPR	General Data Protection Regulation
GHz	Gigahertz
GSM	Global System for Mobile Communications
HAN	Home Area Network
HES	Head End System
IEC	The International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control Address
MHz	Megahertz
NIC	Network Interface Card
NID	Node Identification
NIS	Network and Information System
NTP	Network Time protocol
NV	Non-Volatile
OBIS	Object Identification System
OT	Operational Technology
PLC	Power Line Carrier
P2P	Point to Point
RAM	Random Access Memory

RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition
SEC	Simple Event Correlator
SMB	Server Message Block
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell Protocol
TLS	Transport Layer Security
TOU	Time of Use
WAN	Wide Area Network
WMI	Windows Management Instrumentation
VPN	Virtual Private Network
XML	Extensible Markup Language

Table of contents

List of figures

List of tables

1 Introduction

The energy sector, in technology advancement, is considered a slow-paced field compared to other more information technology (IT) dependant fields like robotics, automotive industry, etc. In IT, the average lifespan of a personal computer is four years [1]. The average age of the Estonian electricity grid and high voltage devices is 33 years, and the average age of the medium or low voltage device is 29 years. The optimal average age of electricity grid devices is rated at 20 years [2].

Network service providers, also referred to as utility, are rapidly implementing smart grid type networks, and one critical component is smart meters [3]. Smart meters are devices that monitor networks (including power consumption) and send monitoring information to service providers frequently instead of manual submission of power consumption required by older devices.

Smart meters have become a critical part of the electricity grid because these devices are helping to stabilize the network and providing essential data from the grid. If this information is altered or blocked, it could affect the network and possibly destabilize the electricity service [3] [4] [5].

Many industries and government reports have identified that cyber intruders have become a severe threat to the secure operation of a smart grid. Forty-six cyber-attack incidents were reported in the energy sector in 2015 [4]. This number is growing at a fast pace, and service providers must be ready for this.

"Security is ongoing. Continuous monitoring of the network is critical to catch intruders or infections, and monitoring should be performed at all levels of the network [6, p. 64]." Smart meters are rolled out all over the world [7] [8]. It is crucial to monitor all levels of the network, especially smart meters. Smart meter numbers are rapidly increasing, and as a result, the potential impact of cyber attack is growing.

Monitoring provides essential visibility over a network. Cyber-attacks will happen, and new vulnerabilities will also be detected, which need to be dealt with as these devices will be part of the network for over 20 years.

1.1 Problem statement

Smart meters connected to the network are installed worldwide to make the network more efficient and resilient [8]. It is often overlooked that increasing numbers of devices connected to a network also increases the potential for cyber-attack [9].

A cyberattack against the power grid is only a question of time. There are numerous examples of cyberattacks where a malicious actor targets the power grid and successfully penetrates security. Ukraine 2015-year attack is a remarkable one, where substations were switched through supervisory control and data acquisition (SCADA). After which workstations, master boot records were deleted, which essentially disabled those computers [10]. In 2017 powerful wave of ransomware hit Europe, including Ukraine, former Chernobyl nuclear plant systems were also hit by ransomware [11]. From 2017 to 2018, the number of "external hackers" number has increased by 9 per cent [12].

There are numerous works/reports done on this topic about security frameworks for implementing advanced metering infrastructure (AMI) in production or security vulnerabilities reports based on smart meter penetration testing [13] [14] [15].

To be prepared for cyber-attacks, it is strongly advised to have an overview and knowledge about network status. Event logging and monitoring are considered countermeasures for several smart meter threats, as shown in Figure 1 [16].

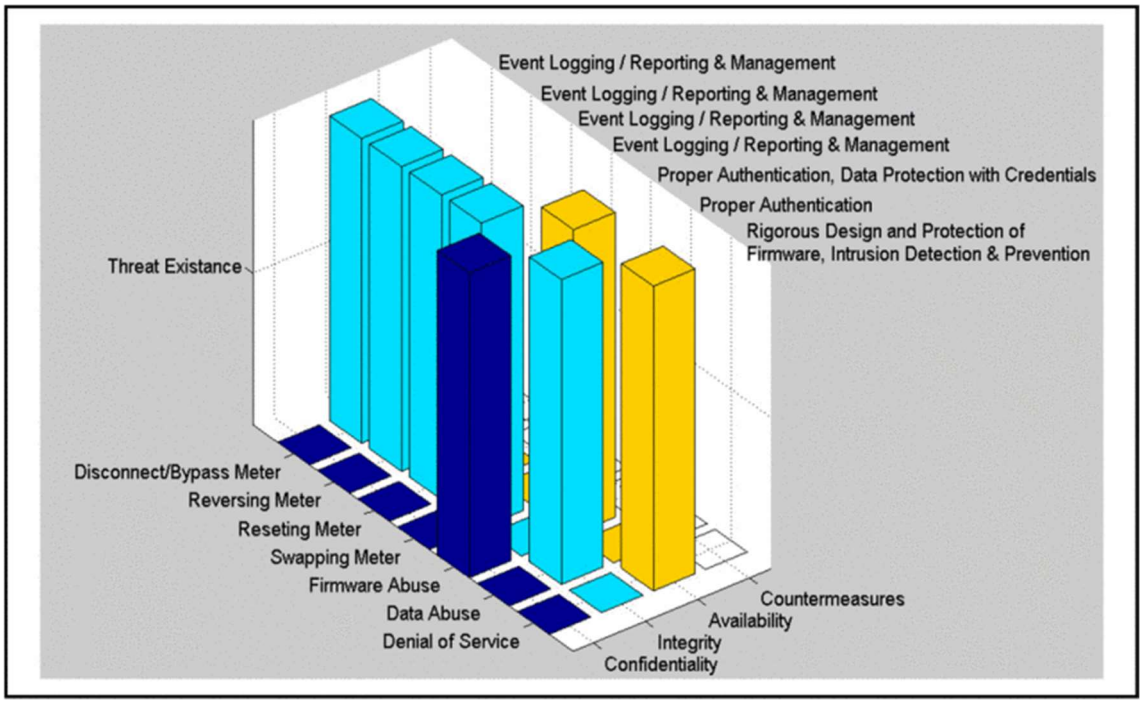


Figure 1 - Smart metering device attacks

Monitoring is the key in this part, and there exists no such research or information which could answer questions – which events of a smart meter should be monitored, what could be monitored and what are best practices to do it?

1.2 Scope and goal

This thesis focuses on smart grid networks, specifically smart metering devices, a critical part of the smart grid and modern electricity grid.

This thesis aims to examine the log files available from smart meters and figure out the most effective way of processing them to raise cyber awareness by detecting known attack scenarios. The most effective method to optimize the cyber threat indication's performance will also be determined.

Experiments will be conducted to generate and gather log data in a laboratory environment where a smart meter network is available. Different actions will be taken on the smart meters during this phase, resulting in log files enhanced with additional information.

As a result, the best practices for smart meter monitoring, log analysis, and smart meter log file-based automated alert creation will be introduced. The author will shed light on the actions that a grid service provider can take to ensure network stability.

Although the poor-quality household devices, like power supplies, LED lights, computer parts, may affect the smart meter communication network, this issue is out of the scope of the thesis; therefore, it will not be tested nor analysed in this paper.

Validation of the recommended solution will not be part of this work as it is challenging, which must be carried out using actual data. Using real data from devices introduces several problems, e.g. GDPR related issues, vast amounts of data, which are not easily solvable; therefore, it will not be in the scope of this work and will be carried out as a

1.3 Novelty

This paper will concentrate on smart meter log analysis in the electricity grid network and will set basic recommendations for smart meter monitoring to identify cyber events as quickly as possible using available tools. These recommendations will help minimize downtime of a network and improve the overall resilience of the network. This recommendation framework should be used by network service providers who are using smart meters.

This paper outcome is unique and has not been researched publicly before. The output of this work will help network service providers to raise cybersecurity awareness to a basic level in terms of smart meter attack detection. This framework will also set standard smart grid monitoring requirements.

1.4 Contribution

The motivation for this research is a dire need for security among utilities providing life vital services for every household. This paper will conclude different known and possible attacks against the smart grid and provide essential monitoring recommendation for utilities. This work will contribute to the more secure grid service and provide us with a more resilient tomorrow.

During the writing of this thesis, there is an ongoing project called CyberSEAS, funded by the European Commission within the H2020 program. This project starts in 2021 October and lasts 36 months. From 8 countries, 26 European organizations are included in this work. The projects' goal is to improve the resilience of energy supply chains. The purpose is to analyse and provide a method or toolset for the smart grid communication channel securing [17]. The information gathered into this thesis, analytical work, and output will be used as a data source in the project and results of this work will be validated in the H2020 project.

1.5 Methodology

The author will collect logs from the network of smart meters in a laboratory environment, which will be a downscaled model of an actual electricity grid. This solution will be close to the real-life version and provide a platform for experimenting with different scenarios without interrupting the service provider's service, meantime providing sufficient and relevant information for the research. Logs will be analysed to determine what information could be extracted from smart meters, what values need to be monitored, and which events could be automatically mitigated.

1.6 Outcomes

This paper will output a framework with recommendations for grid operators which events could and should be monitored. Recommended methods of data collection will also be included to have a good picture of AMI. Analytical work will also output recommendations on which risks could be mitigated automatically by automatic alert generation or active monitoring.

2 Background information

This paragraph will briefly explain what a smart grid is and how it works, which elements it usually consists of and how the Estonian electricity grid operates.

2.1 Smart Grid

The smart grid does not have an exact definition; hence it can only be described: "Smart Grid can be described as a transparent, seamless and instantaneous two-way delivery of energy, information and enabling the electricity industry to better manage energy delivery and transmission and empowering consumers to have more control over energy decisions [18, p. 2591]."

A smart grid is a type of network which combines modern communication technologies with physical network capabilities. Smart grid makes the power distribution network more effective, provides bi-directional communications and power flow between household and service providers.

The load on the power distribution network can vary depending on several conditions, like the period of the day and the year's season, the actual temperature, and many more. For example, most people arrive home from work simultaneously and connect high current drawing devices like heating systems or electric vehicles; therefore, households' summarised power consumption exceeds the average consumption for a short period. This period is called a peak and leads to the question of over dimensioning. To provide stable, uninterrupted electricity, the network providers must handle these peaks, so the networks are not dimensioned for the average consumer but the peaks.

This problem is getting more severe today because of the growing number of electric vehicles. The network in some urban areas is not designed to withstand the increased load that overloads network components in particular distribution areas, which can cause damage or activate the protection that leads to dropping out of the service.

A smart grid could utilize different accumulators to stabilize the network during high workload periods, for example, electric vehicles. Using accumulators or other types of service could help network service providers lower costs by over-dimensioning the network.

To overcome the network over dimensioning issue, the smart grid could use electric vehicles or smaller electricity manufacturers (solar panels, wind generators, etc.) to stabilize a network. There are many small energy-producing individuals in Estonia who have built solar panels on their land, or even some have constructed wind generators. This could help by providing capacity in the same region of the network. This means that service providers can build smaller magistral electricity lines between distribution areas and power plants.

As service providers need to invest less money by using smaller cross-section cables for electricity network, the cost of electricity service would be more affordable [5]. Smart grid network is also known as Advanced Meter Infrastructure (AMI).

A typical example of a smart grid can be seen in Figure 2 [19].

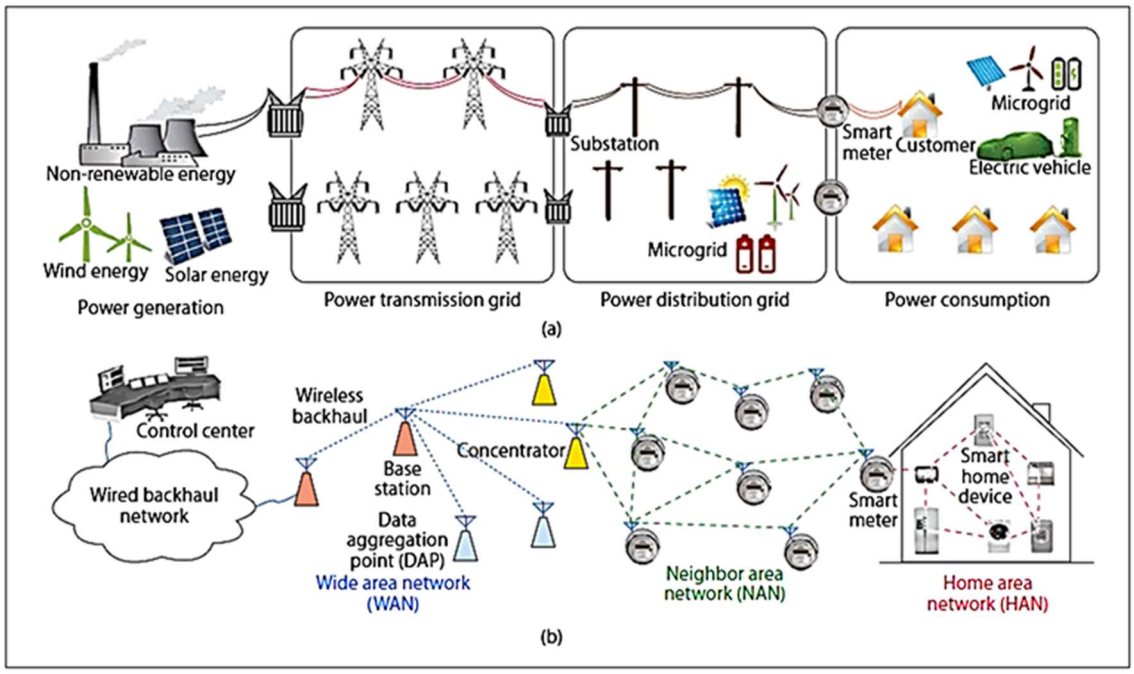


Figure 2 - Typical smart grid network

Devices connected to the network in-household can be called Home Area Network (HAN). Smart meters are considered as a device part of the Neighbour Area Network. Smart meters provide a communication link between HAN and NAN network [14], illustrated in Figure 2.

Smart meters have become a critical part of the grid because these devices help to stabilize the network by providing critical data from the electricity grid. If this information were altered or blocked, it could affect the grid and possibly destabilize the network.

2.2 About Estonian electricity grid

The Estonian Electricity grid is separated between several companies - Enefit, Elering, Enefit Connect, and Elektrilevi. This paragraph will briefly describe the Estonian electricity grid and what is the role of these companies.

Estonian electricity network begins from Enefit's power plants in Auvere or Narva. Electricity is transferred over longer distances by a high voltage grid, which Elering operates. High voltage is needed to transmit electricity over long distances with lower losses of energy. There are few medium to low voltage grid service providers in Estonia; the biggest is Elektrilevi.

2.2.1 Elektrilevi OÜ

Elektrilevi OÜ is the biggest electricity grid operator in Estonia, whose ambition is to provide electricity to almost every Estonian customer. Elektrilevi has more than half-million customers, about 60 000 km of electricity line and 24 000 substations in Estonia. The company is responsible for the medium to low voltage network used for the distribution network, for transporting electricity from substation to customer point aka metering device on customer's land.

2.2.2 Enefit AS

Enefit is also known in Estonia as Eesti Energia, is a publicly limited energy company in Estonia, which the Estonian government owns shares. Enefit was founded in 1939. Enefit is used mainly for international operations as Enefit is operating currently in Estonia, Latvia, Lithuania, Finland, Jordan and Utah and the United States. Enefit owns several powerplants, including one in Narva and one in Auvere near Tallinn. Enefit's powerplants are using oil-shale as a raw material which is being mined primarily on Narva. Enefit also owns 17 wind parks total in Estonia and Lithuania [20].

2.2.3 Enefit Connect OÜ

Enefit Connect is a part of the Enefit group and is responsible for the network management of Estonian electricity, fibre-optics and Electric Vehicle (EV) charging. Additionally, Enefit Connect offers indoor and outdoor lighting, off-grid electricity solutions, solar solutions etc.

2.2.4 Elering AS

Elering provides a high voltage transmission network from power plants to distribution network. Elering is providing grid service between Enefit and Elektrilevis. Elering operates more than 5000 km of electricity line operation, which can be seen in Figure 3 [21]:

- 1697 km of 330 kV lines
- 158 km of 220 kV lines
- 3493 km of 110kV lines
- 58 km of 35kV lines

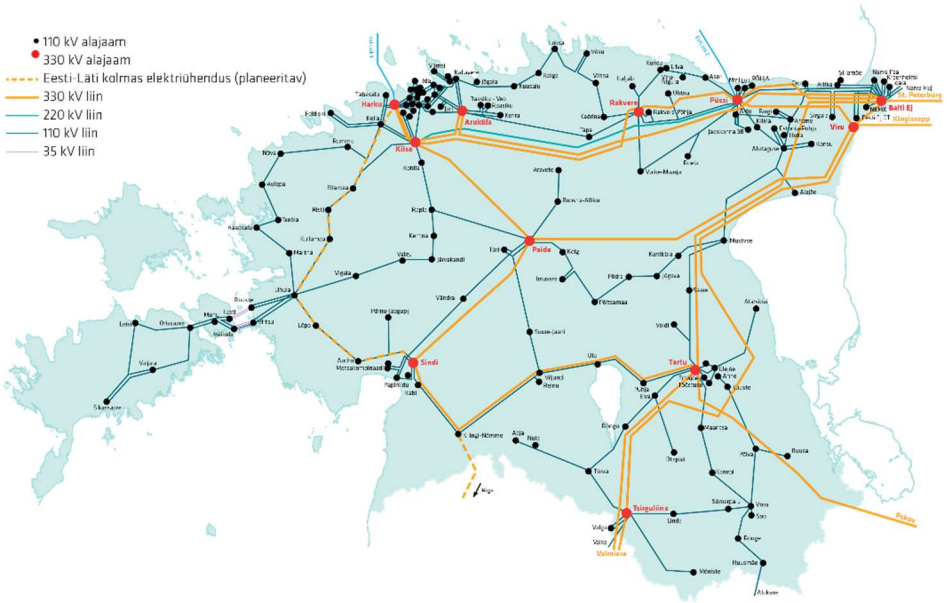


Figure 3 - Elering high voltage grid in Estonia

2.3 The cyber situation in the energy sector

Cybersecurity has been overlooked for some time in the energy sector as with rapid development, new risk vectors formed. These unmitigated risks and lack of processes resulted in cyberattacks against systems, which happened against Ukraine as a part of political conflict from 2015 to 2017. This drew new light to the cybersecurity part and resulted in much-needed carefulness in the IT world.

"Smart meters (…) fail to comply to the Open Web Application Security Project (OWASP) standards such as injection, authentication, cross site scripting (XSS), insecure direct object references, security misconfiguration, sensitive data exposure and missing function level access control [22]."

2.3.1 Cybersecurity overview

Cybersecurity can be described as three primary pillars which can be presented using the CIA model [23]:

- Confidentiality – Information should be available only to authorized people. Unauthorized people should be kept from viewing information. This usually should be done by restricting access to data, files, information, or systems using access control methods.

- Integrity – Information should be kept in original form and should not be modified in any way, either intentionally or accidentally. Integrity means that original data needs to remain original and unmodified. For example, message transferred between parties should not be intercepted and changed in a third party favour. A message should not be corrupted and be always readable.

- Availability – Information should be accessible and available to authorized personnel. Information can be in any forms - files, documents, information system, processes etc [23, p. 1].

In 2012, a non-profit member organization, the European Network for Cyber Security (ENCS), was founded, which helps critical energy sector companies battling against cybersecurity threats and actors. ENCS has dedicated researchers and test specialists who

work with the members. ENCS provides training, end-to-end testing, research capability and defining technical security requirements [24].

In 2016 European Commission proposed the European Union Network and Information Security directive (called NIS directive), which European Union adopted in 2016. NIS directive's purpose is to enhance cybersecurity by bringing a minimum level of requirements into the picture for every European Union member state. The national transposition deadline for every member state was 09.05.2018 [25].

2.3.2 Energy sector

Electricity infrastructure in most countries has been emerging since the 1930s, when the first power plants were built. The centralised energy production raised the question of energy transportation and distribution to customers. After a long time, the currently used high, medium, and low voltage network become the standard solution. Up to date, the metering devices at customer points were just physical devices, which recorded electricity consumption [13].

As European Parliament mandated replacing electricity metering devices with a new type of meters called smart meters, the AMI system will become an essential part of the electricity grid [13].

AMI changed the electricity grid by adding smart meters into the equation. Since these devices are bi-directionally connected to a server or a data concentrator and send metering data periodically (which is sensitive personal information), the importance of cybersecurity is considerably higher than ever before [13].

Smart meter manufacturers and network service providers considered the encryption of data storage and transmission as a solution to the cyber security challenges. The method solves only a portion of the puzzle - confidentiality [26]; on the contrary, it omits integrity and availability. This implies that security and privacy are not adequately addressed because of low awareness in the cybersecurity field among network service providers [13].

The first politically motivated, publicly documented cyber-attack against the power grid took place in 2015 against Ukraine's power system. This act shed new light on cybersecurity in the energy sector. The political conflict was the motivation of this act.

Inadequate security measures were leveraged in Ukraine's power grid system, which resulted in over 225 000 outages. Attack was carried out by spear-phishing emails, which contained malware that gained access to the SCADA system and switched off substations [4] [10].

From 2008 to date, numerous reports published describing frameworks that could be applied to AMI and conferences were organised where different attack vectors were discussed, and mitigation techniques were proposed [27].

2.3.3 AMI security

As energy sector companies are implementing AMI systems and previous attacks against power grid are good examples of poor security in a highly volatile environment, better security measures need to be applied by energy sector companies to keep resilience. To support resilience and make energy transmission more secure, the CIA model could be applied to the AMI system:

- Confidentiality – Data should be protected from being disclosed by unauthorised entities as consumption data can reveal the life pattern of individuals. Additionally, access to management systems should be kept only available to authorized people.

- Integrity – Information from the smart meter must be transferred to the server unaltered or modified without authorization. Additionally, loss of information could cause disruptions in network stability and billing.

- Availability – Consumption data must be available because the utility supplier is balancing network, ordering capacity from plant and invoicing based on this data [28].

There are multiple proposed technical methods of securing a smart meter network, either using a trust model [29] or a secure communication framework [30]. While this trust model is a good idea with proof, it seems to be more a method that device manufacturers should implement.

Smart meters are part of a network paradigm called the Internet of things (IoT) [30]. There is a monitoring system developed for IoT devices, which theoretically could be applied

for smart meters as well [31]. Most smart meter manufacturers tend to restrict access to smart meter system by only providing tools for firmware updating, device configuration and access to logging data to authorized companies or people.

There is ongoing research about using the 5G network as the communication platform of the smart grid. The solution is going to be implemented in smart meter's next generation. 5G will support massive broadband that offers sufficiently enough bandwidth and the possibility to connect billions of devices. With 5G implementation arises new security threats, which need to be addressed [32].

Systematic management of authentication information and a stable mass injection method has also been proposed to be applied on the AMI network to secure against unauthorized eavesdropping and forgery. The method is a service for certificate-based AMI device authentication centre for injecting AMI authentication information into devices. This information is injected into data concentration units and PLC modems [33].

There exists an archetypal attack tree for penetration testing AMI devices with several actual attacks on commercially available systems: energy fraud, denial of service and targeted disconnect [15].

2.3.4 Estonian power grid cybersecurity

In Estonia, Enefit, Elering, Enefit Connect and Elektrilevi have a strong collaboration in cyber security.

There is an ongoing cybersecurity awareness program in Enefit Connect to raise the company's overall cybersecurity awareness by training employees from every structural unit of the company. The courses' audience like 'ambassadors' should distribute their new knowledge and experience all over the company. The program creates an IT-related cultural shift and improves user's cybersecurity awareness drastically. From the technical side of view, Eesti Energia, aka Enefit, has defined critical business processes where the company will concentrate more, and a bigger portion of investments will be made. [34].

IT and industrial automation, constantly growing industry-related cases, pointed out the necessity of attention raising to cybersecurity at Elektrilevi. As a result, in 2016, the company joined European Network for Cyber Security.

Also, Estonia was the first of countries from the eastern Baltic region who joined ENCS [33]. Elektrilevi started installing smart meters in 2013, and by the end of 2016, all client metering devices had to be replaced with smart meters [35].

2.4 Related works

AMI security issues have been researched thoroughly, and different scenarios are proposed, out of which many of these are also analysed in this work. Multiple methods are proposed to secure the AMI network, using either potential process mining for intrusion detection in smart metering [36] or intrusion detection system using an online sequence extreme learning machine [37].

Apart from AMI security issues, there is no specific work related to smart meter log analysis or detection from a cybersecurity perspective. There is a paper with a design of privacy that could enhance smart meter architecture [38].

There is a data traffic analysis work, which reflects data sizes and possibilities of different data transfer methods [39]. Many devices in-network means that even small changes in data amounts could affect data gathering speeds and availability of devices. For example, even a small increase of data amount, 5 kilobytes per device, on a network consisting 150 000 devices causes over 0,75GB increase of traffic per polling time.

There is no academic work on smart meter log analysis from a cybersecurity perspective that outputs any actual conclusion to which events could be gathered, monitored or react to.

2.4.1 Log collection methods and tools

There are different logging protocols available, which can be used for centralized logging. The most common logging protocol for Unix-like operating system is called syslog. Syslog is widely used for various applications, e.g. switches, printers etc. On a single device, syslogs purpose is to include device-wide logs into one single point for easier parsing [40].

There are several tools for syslog information collection, which can be divided into two categories – User agent style and agentless style [41].

User-agent style log collection usually leverages a program called an agent. An agent is installed on a remote device from which logs are collected. The agent collects metrics from the device and transmits incorrect information structure to a centralized server. Either community or a software manufacturer usually develops software agents. Software manufactured agents effectiveness heavily depends on the software manufacturer. A commonly used modern log collection and parsing stack is called Elastic stack, which uses beat type agents (filebeat, metricbeat) for log collection from systems.

Agentless style usually uses different preinstalled or configured methods available on devices for accessing device. This kind of solutions usually uses operating system native protocols like Simple Network Management Protocol (SNMP), Windows Management Instrument (WMI) or Syslog. There is also a possibility to use methods to store information in remote databases or acquire information using remote management protocols like Secure Shell Protocol (SSH) or Server Message Block (SMB) protocol to access files.

2.4.2 Log analysis methods

Different log analysis methods are available for a systematic approach. These methods provide a way for data amount reduction and sometimes give a better understanding of information in logs.

It is also possible to use intrusion detection methods based on density, cluster centres and nearest neighbours. This method uses each sample point to cluster centre and distance to the nearest neighbour [42].

For quicker log analysis, it is possible to use clustering methods. It is possible to filter out all the known and expected log messages from a log file resulting in a dataset that could give hints of the reason for an event. This can remove clutter from a dataset and help discover more quickly related information to the event [40]. This method would help to parse big data amounts and extract only relevant from these files. Unfortunately, this solution still requires lots of data to be inputted into the application, which could be difficult due to PLC throughput and manufacturer limitations.

Event correlation is also a method for combining multiple alarms with additional information present in a log file. Event correlation will create a message with reason. This

helps to reduce data amounts by combining multiple messages and gives a better understanding of event by adding reason [40]. Simple Event Correlator (SEC) is a lightweight platform-independent tool written in Perl by Risto Vaarandi, which can be leveraged for event correlation [43].

Artificial intelligence and machine learning are commonly heard terms in every IT sector in 2021. Machine learning is usually leveraged by supervised or unsupervised methods. The supervised method means that the data model is built by "training" - learning correct and incorrect answers to find different paths and solutions. The supervised method needs considerable amounts of labelled data (correct answers or anomalies). The unsupervised method is leveraging data which can leverage data without given true answers. There is proof of concept, which tests different machine learning models and outputs the five best methods applicable to parsing [44].

3 Research environment and limitations

This paragraph describes this field's overall environment, including the production electricity grid, lab setup, and other environmental aspects that affect this work.

3.1 Environment

Electricity grid service is considered a life vital service, which means this service must be operational with minimal downtime. Life vital service also means that the biggest priority is providing electricity to every customer, even if this sometimes means less security or reduced functionality. All in all, the electricity grid service's primary focus and goal is to transport electricity.

3.1.1 Production

The electricity grid in production consists of different type of devices and lines for electricity transmission. As this thesis mainly focuses on smart meters, these devices will be introduced here. The smart meters deployed in Estonia can be divided into two major groups by connection type:

Power Line Communication (PLC) means that operational data from a smart meter is obtained by communication over power lines. This method is usually used with data concentrators, a device that collects logs from multiple smart meters and transfers a batch of this data to a centralized server [3].

If the data is transferred over Radio Frequency (RF), the communication structure can be Point to Point (P2P) and Mesh type. Smart meters with RF communication are usually used in places where using PLC is impossible because of lack of connectivity, like off-grid solutions or unstable connection, such as cheap electronics disruptions.

There are also smart meters that communicate over mesh type connection, which means devices are connected over RF frequency in 900 MHz or 2,4 GHz bands, forming a LAN network. Information from the LAN network is transferred to a centralized server over WAN technology [3].

There are also methods for manual network alteration due to the nature of electricity service – critical service, which is also considered life vital service. Manual alteration

means that there is a physical switch on the network device to switch it off in the worst-case scenario or by the landlord's need. This method has been used for network operation before remotely controlled network devices became available.

In Estonia, the RF type network is based on cellular data transfer because the cellular connection has proven to be more stable in terms of disruptions caused by cheap electronic devices, which tend to create disturbances in the PLC system. However, this type of communication depends heavily on the external service provider and cellular connection stability and quality. The cellular connection also tends to be expensive because of higher fixed costs related to the telecommunication service provider; therefore, Elektrilevi considers cellular-based communication a second choice.

3.1.2 Research Environment

Since the experimental research in particular cases would harm the production, the Enefit Connect's laboratory will be used for this research. This environment is isolated and utilizes the same devices and similar configuration as the production network. The analysis of the structure, the devices, and the applied communication methods in the laboratory offers a sufficiently good environment to experiment and test different scenarios.

3.1.3 Devices and lab setup

Devices, management, and monitoring solutions used in the lab are similar to those with a similar configuration in the production network. The following type of devices are installed in the research environment:

- PLC type network
    - Landis+Gyr E450
    - Landis+Gyr E350
    - Landis+Gyr DC450 v2 (Data concentrator)
- Cellular type network
    - Landis+Gyr E450
    - Landis+Gyr E350
    - Landis+Gyr S650

Landis+Gyr devices will only be used as these devices are used in the company and northern Europe. These devices are used because they are accessible to the author.

Acquiring different manufacturer devices would prove difficult as vendors usually don't give out their devices for this kind of testing, requiring additional competencies related to electrotechnology.

Although the research environment follows the real network, several differences take place as follows:

The research environment accommodates only 11 smart meters and one PLC concentrator; contrary, the production network contains approximately 150 000 devices.

There are physical differences, like the distance between the smart meters and their distance from the data concentrator. In the production environment, these distances are between 100 and 900 meters, averaging at 200m. In the research environment distance between smart meters is 0,4 m on average.

There is a significant difference in network usage as well. Unlike in the production environment, there are no real customers in the laboratory, and it is "sterile"; all the installed components meet the quality requirements. There is no electrical noise that might influence communication.

PLC smart meter lab setup is visualized in Figure 4.

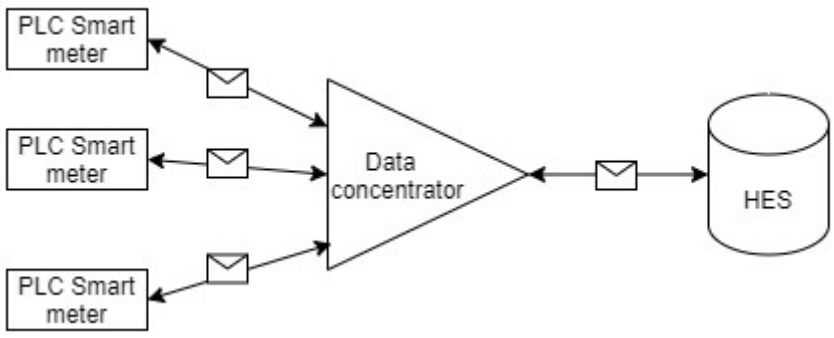


Figure 4 – PLC smart meter lab setup

The cellular lab setup is visualized in Figure 5.

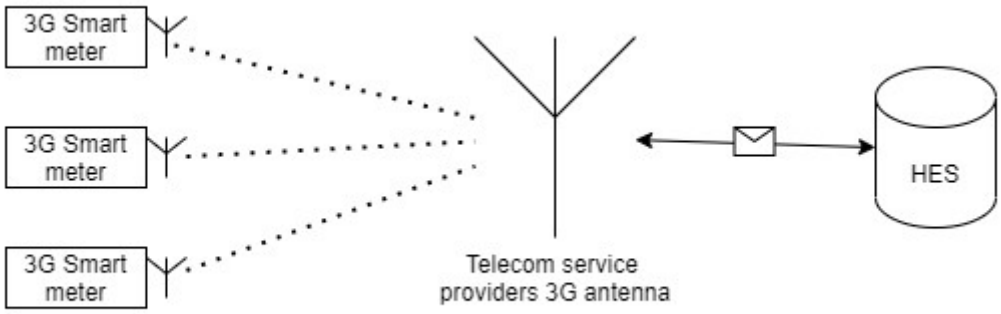


Figure 5 - Cellular smart meter lab

3.1.4 Quantitive data model

Mathematical modelling is the description of natural systems through the mathematical language that is then suitable for transformations and other mathematical treatments to find nontrivial relations among system elements. A model is a mathematical description of the elements of a process and how they influence each other [45].

Qualitative and quantitative are the key concepts in systems' mathematical modelling. Quantitative models are compact representations where a single differential or difference equation may describe the system's performance for a large set of input functions and initial states [45]. Contrary, qualitative models do not require mathematical formalism; they describe qualitative relations between the observed variables. Qualitative descriptions are close to the human way of thinking so that such models are easier to explain and can reveal more information than regression models [46].

Since the system's quantitative mathematical modelling would be overly complex and the research deals with a large amount of empirical data, the quantitative data model offers a better approach.

This decision is backed by the real-life application of the thesis results in which the logs will be collected automatically on devices and analysed on a central server. This process will contain the pre-processing of the collected data and its comparison over different devices or times to identify malicious actor activities.

During the research phase, quantitative modelling will be used to analyse logs to identify possible detection mechanisms, automatic mitigation activities or critical alerts which should be monitored.

3.1.5 Services

To simulate the real life-like environment, the research environment contains the following elements:

- Simplified PLC network
- LAN network
- Cellular network (using cellular service provider SIM card)
- Monitoring solution
- Smart meter management software
- Log server (for log collection, storage, and analysis)

3.1.6 Differences between lab and production environment

Although the research environment is mainly identical to the production one, for example, all production network's device models are used, there are many differences, especially in communication. The primary difference is the cable length between the devices and the device's count regarding the PLC network.

In the lab environment, there are no household appliances, which could create disturbances. In a production network, it is common that cheap electronic devices like inadequate quality power supplies, e.g. used in lighting devices, can generate signals that could disrupt PLC communication. In the lab environment, these kind of disruptors are missing; therefore, communication will not be disrupted. The lack of disruption does not affect the research outcome as it does not change data; it would only disrupt data gathering. This paper will not analyse or test different electronic devices and their effect on the PLC communication channel as this is not in the scope of this work.

LAN network is identical to the network in production. The only difference is the device count in the communication network. The cellular-based communication network is the same as in production.

The system monitoring and log collection methods are identical in the research and production environment. Head End System (HES) is used for centralised smart meter management, and it is responsible for the log collection as well.

3.2 Limitations

This paragraph will briefly describe different limitations related to this research, including technical, third-party, and legal limitations besides the company's restrictions.

3.2.1 Company limitations

Enefit Connect and Elektrilevi set company limitations. This work should not include any confidential information about the real grid which is not publicly obtainable from authentic sources. Additionally, it is prohibited to include in the thesis the following data:

- Passwords
- Customer-related data
- Network addresses
- Network information

3.2.2 Third-party limitations

This work aims to make the smart grid more resilient and better protected against cyberattacks disrupting life vital service. It is essential to notify third parties (e.g. device manufacturer) regarding security flaws found in the system or devices.

Additional smart meter functionality needs to be implemented by the manufacturer; otherwise, it would void the warranty and lose manufacturer support. Therefore, event correlation and clustering method will not be used in this work. The biggest gain of event correlation methods in terms of PLC would be a reduction of network traffic. To gain an advantage of event correlation, manufacturers need to implement this functionality into smart meter devices.

The clustering method is not used in this work as monitoring work is highly dependant on manufacturer-provided log collection methods. Using manufacturer-supported methods, only event codes-based data is logged, removing irrelevant data by design and providing only relevant information.

Event correlation and clustering methods could be applied in the central logging server if enough data is available. Applying these functions to a centralized server is hardly beneficial. It would still require data transfer to happen from smart meters, which is heavliy limited by PLC as a communiction platform and data ammounts needed for storage due to a large number of devices. To benefit from these functions, the manufacturer should implement these at smart meters instead.

3.2.3 Legal limitations

This experiment and analytical work will not be concluded in the live network; therefore, this work will not be under the General Data Protection Regulation (GDPR). There will not be any client-related data involved.

3.2.4 Technical limitations

The communication speed between the data collector and data analysing points can be considered a technical limitation. Compared to a regular fibre optic or copper-based communication speed, the speed offered by PLC is highly moderated. PLC network transmission speed depends on network configuration, distance and protocol used in the system.

In Estonia, the maximum speed used of the distribution network of PLC is 2400 bps[1], which is relatively low compared to traditional ethernet. Since the data transmission speed is limited, the volume of the collected data and collection frequency is limited.

[1] Internally gathered information in Enefit Connect

4 Smart meter cyber threats

Electricity theft is a common problem worldwide as this is a beneficial activity for the malicious actor [47] [48]. AMI system is considered as a tool against energy theft [47]. Smart meters, which are vital components of AMI, provide many more functionalities than traditional electricity meters, but with these computer-like capabilities, new security attacks are introduced [49].

Attack tree is a visual aid tool used for modelling and visualisation of attack vectors, emerging from the late 90s. The result is an easily understandable scheme, which helps to describe a connection between attack vectors, goals and nodes [50]. Attack trees will not be used in this work; it is here only for the reader to understand better information displayed in the picture.

Energy theft against AMI could be accomplished in several different ways, which can be described by the energy theft attack tree - Figure 6 [51].

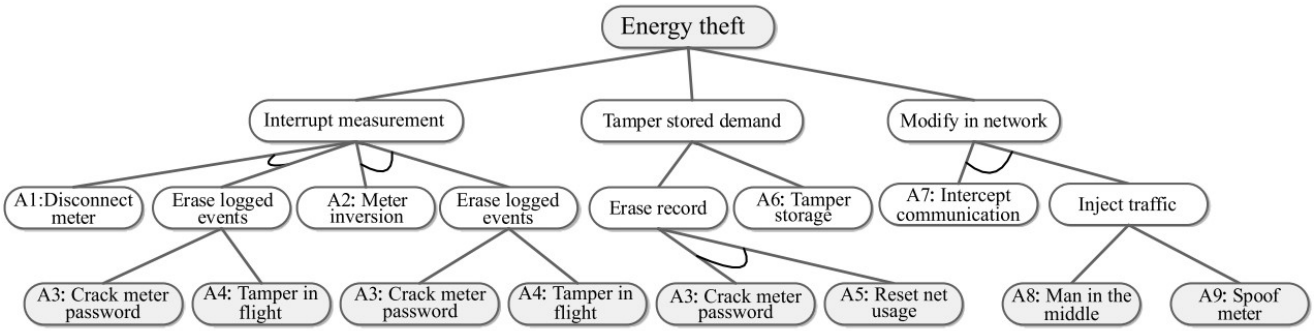


Figure 6 - Attack tree for energy theft

The second important attack vector is the denial of service (DOS), which attack tree visualized in Figure 7 [52].

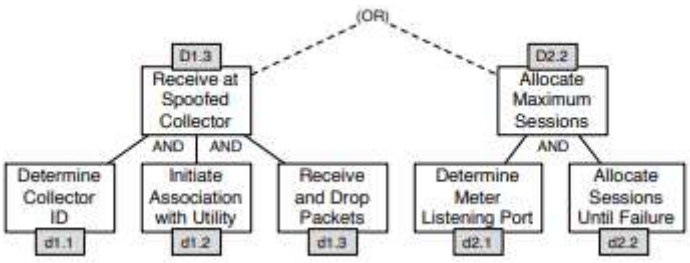


Figure 7 - Denial of service attack tree

4.1 Smart meter related threats

Smart meter related threats can be categorized into three main categories: system-level threats, threats to the theft of service or threats to privacy and confidentiality [53].

System-level threats are related to regular operation of the grid – smart meter network tampering or takeover, denial-of-service by interrupting electricity delivery, compromise of the backend, etc.

Energy service-related threats - metering device tampering or replacement to report different electricity consumption, metering device physical movement or other metering device manipulation.

Threats to privacy and confidentiality – message interception in the network, data concentrator infection to mirror data to third party device etc [53].

4.2 Malicious actors

The different kind of attackers could be categorized based on their skill level and motivation:

- Curious eavesdroppers: Those attackers are mostly interested in the activities of their neighbours out of curiosity.
- Greedy customers: The goal of these attackers is to steal electricity and lower costs.
- Malicious eavesdropper: Their purpose is to use collected data for bigger criminal activity, for example, breaking into a house.
- Swanky attackers: These attackers want to prove that they can access the system or show off their abilities.
- Active attackers: These attackers aim to launch larger-scale terrorist attacks against the whole power grid.
- Intrusive data management agencies: Private information collected for the company benefit or gain, e.g., marketing.

Three types of attackers motivated to commit energy theft:

- Customers are usually motivated by personal gain by tampering with data sent from a smart metering device to reduce electricity bills. In developing countries, people commit energy theft due to their poor infrastructure, poverty, and irregularities in the system.

- Organized crime: Motivation is derived from the monetization of energy theft. Experienced hackers can leverage smart meters. Suppose their success is rooted in the poor design of the AMI system - for example, the same password is used in multiple devices- hackers can gain access to a significant portion of the system and possibly amplify profit.

- Utility company insiders: Employees of utility companies are considered as trusted, but there could still be people who have the motivation to misuse authorised access to a system for personal gain [51, pp. 107-108].

4.3 Smart meter attack vectors

Smart meters are devices that combine IT features with operational technology (OT) devices functionality, so these devices introduce attack vectors from the IT side and combined threats from both worlds.

4.3.1 Unauthorized access to device

Insufficient security can lead to the tampering of HES. Since the network's centralised management system, its leveraged security helps the intruder gain access to smart meters [22]. This attack could affect the whole smart meter network and disrupt service to all customers in that service provider's region.

Gaining access to one smart meter's password could mean access to all smart meters if the service provider uses the same password for every device, so that the password protection is a key element of smart meter's security, however -according to [52]- there are several methods to get to know it. Physical monitoring of smart meter optical port could provide a way for password extraction when utility is using management port. If the physical access is not obstructed or monitored, the password hash becomes available

from the smart meter's memory. Smart meter diagnostic protocol spoofing could also set up an authenticated session to obtain an established session for metering data submission.

4.3.2 Denial of service attacks

A denial-of-service attack **(**DoS attack**)** is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled [54].

DoS can be executed against smart meters by the allocation of the maximum session number. This action might lead to the exhausting memory or operating system resources of the smart meter [52]. Although this attack affects only a single customer, the attack can be executed multiple times against different customers remotely.

Disruption of commands sent to smart meters could be accomplished by intercepting and dropping the commands sent to smart meters. This attack could render controlling device impossible using remote control methods and cause utility to send operator physically to on-site service [52]. The attack could affect the service of the whole network.

Another format of denial of service attacks is a flooding attack called puppet attack when the attacker hijacks one or more normal nodes and uses them as puppets. An attacker sends data packages containing attack information to these puppets. Puppets will start generating and sending out unlimited volumes of request and route reply packages. Mesh network communication bandwidth is limited, and excess route packages will exhaust bandwidth and result in denial of service [55] [56]. This attack could compromise the whole smart meter network.

As these devices are usually using low computing power capable chips, the device's resource is limited. CPU overload could be achieved by sending encrypted frames to devices [57].

4.3.3 Information alteration attacks

This attack can be executed by smart meter data transmission tampering by interfering with the connection between smart meter network interface card (NIC) and data concentrator or server [52]. The attack, called Man in the Middle, can interfere with one

or many targets. If the attacker targets PLC, then multiple devices become affected in that area.

Smart meter data alteration could be achieved by injecting malicious code or data into the physical memory of a smart meter. This could be achieved by exhausting network bandwidth to cause smart meter network disconnection from the network. After disconnection, the smart meter will start writing network usage/monitoring data to the device's physical memory. Then the attacker would leverage this process to inject malicious code or data into smart meter physical memory to override or read information from the smart meter. After data has been altered, network connection would be restored [55]. This attack could affect one to many devices, depending on the attacker target.

4.3.4 PLC specific smart meter attack vectors

Two major attack types can heavily influence PLC communication. The physical communication layer jamming is the most basic attack against smart meters by injecting signal along the electricity line used for communication to decrease the signal-to-noise ratio. Jamming attacks could additionally be divided into three subcategories – noise jamming, interference jamming and correlated jamming [57] [58]. This attack would target one to many devices, depending on nearby devices count.

The overflow in the node log attack based on every smart meter must register in a hub to interact with the network. This registration uses the smart meter's MAC address as unique node identification (NID) address. An attacker can leverage this registration process in poor firmware implementation by sending multiple registration requests with different MAC addresses [57] [58].

4.3.5 Other types of attack vectors

Smart meters are combining multiple industries like the energy sector, IT, telecommunication. However, there are several different threats related to telecommunication methods. These are not in the scope of this work because telecommunication companies provide these services.

4.4 Event priorities

This chapter will categorise events by priorities, which should, and can be monitored by a utility. Events will be chosen based on different attack vectors described in the previous chapter.

The event's priorities were divided into three categories: critical, medium, and low priority - the selection of the categories based on the effects and consequences of the events on the overall network.

To have a more tinged set of priority levels, the opinion of specialists from the IT security and power industry is also gathered and included in this work. Several company employees were questioned for better understanding - Information security manager, manager of metering device management department and fraud detection department manager.

4.4.1 Critical priority

Event is considered critical if it causes service disruption to 20 or more clients or is energy theft related. In addition to this, the following events are also considered critical due to their effect on the system:

- HES system information tampering;
- Password extraction or eavesdropping to gain unauthorized access to smart meter;
- Smart meter diagnostic protocol spoofing;
- Man in the middle attack between data concentrator and HES;
- Physical communication layer jamming;
- Smart meter DoS puppet attack.

4.4.2 Medium priority

Event is considered a medium priority if it causes service disruption to 5 - 20 clients or fits any of the following categories:

- Maximum session number allocation;
- Disruption of commands sent to smart meter;
- Unplanned maintenance work on smart meters (including firmware upgrades);
- Anomaly detection based on periodical events.

4.4.3 Low priority

Event is considered a low priority if it affects less than five clients or fits any of the following categories:

- Diagnostic events
- Single smart meter physically damaged by probing or unauthorised access
- Single smart meter switched off by local malicious activity.
- Smart meter lid removal by customer

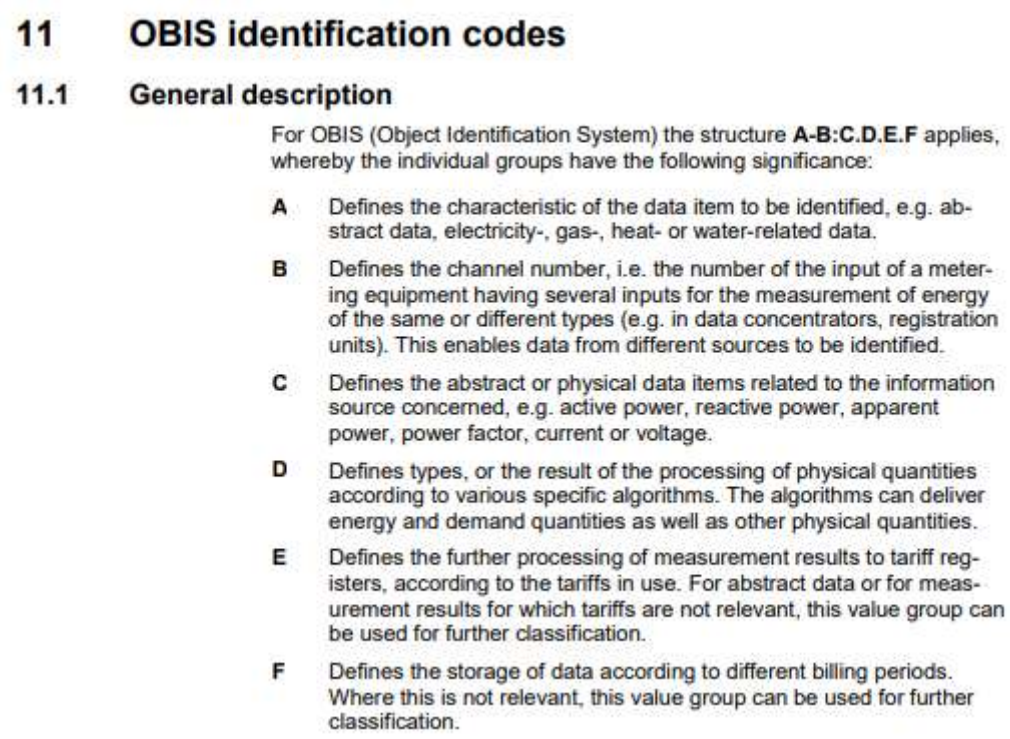
5 Collection of the data

Data will be collected from several sources during the research log, like device management software, data concentrator, smart meters, and HES. The various data source helps to gain an overview of the different levels of data logging and find methods to capture information from different sources.

Data is transferred between HES and devices over International Electrotechnical Commission (IEC) protocol 62056 and using Object Identification System (OBIS) codes.

Each manufacturer defines a code table for alerts, events, and other status codes, which are mainly used for information transmission over communication channels to reduce curious eavesdropper category chances to extract any valuable information with low effort.

Landis and Gyr specific OBIS identification codes are part of the .MAP120 software manual [59]. The structure of the Landis and Gyr OBIS code can be seen in Figure 8 [59].



11 OBIS identification codes

11.1 General description

For OBIS (Object Identification System) the structure **A-B:C.D.E.F** applies, whereby the individual groups have the following significance:

A Defines the characteristic of the data item to be identified, e.g. abstract data, electricity-, gas-, heat- or water-related data.

B Defines the channel number, i.e. the number of the input of a metering equipment having several inputs for the measurement of energy of the same or different types (e.g. in data concentrators, registration units). This enables data from different sources to be identified.

C Defines the abstract or physical data items related to the information source concerned, e.g. active power, reactive power, apparent power, power factor, current or voltage.

D Defines types, or the result of the processing of physical quantities according to various specific algorithms. The algorithms can deliver energy and demand quantities as well as other physical quantities.

E Defines the further processing of measurement results to tariff registers, according to the tariffs in use. For abstract data or for measurement results for which tariffs are not relevant, this value group can be used for further classification.

F Defines the storage of data according to different billing periods. Where this is not relevant, this value group can be used for further classification.

Figure 8 - OBIS identification code structure

Depending on function, there are four different packages available from manufacturer:

- Service tool – Landis+Gyr .MAP110;
- Parameter editor – Landis+Gyr .MAP120;
- Parameterisation tool – Landis+Gyr MAP120;
- Parameter editor – Landis+Gyr MAP190 [60].

Parameter editor - .map120 will be used for this research.

5.1 Event simulation on smart meters

Before data collection, the following activities will be conducted on the tested devices to gain sufficient data. The events help to identify how devices will respond to these kinds of activities and how this information will be available:

- Lid removal;
- SIM card removal;
- Power cut;
- 3G antenna removal;
- SSH remote connection;
- HTTP session initiation;
- Modem disconnection.

5.2 Information collection from .MAP120 software

Manufacturers provide smart meter management software for device configuration, called .MAP120 (Figure 9). This software provides access for different maintenance and configuration activities; our interest is to identify possible events which could be configured for monitoring. The software also offers basic device management and

configuration. .MAP120 can communicate with devices using different communication channels: optical port, serial, Secure Shell Protocol (SSH) and HTTP.

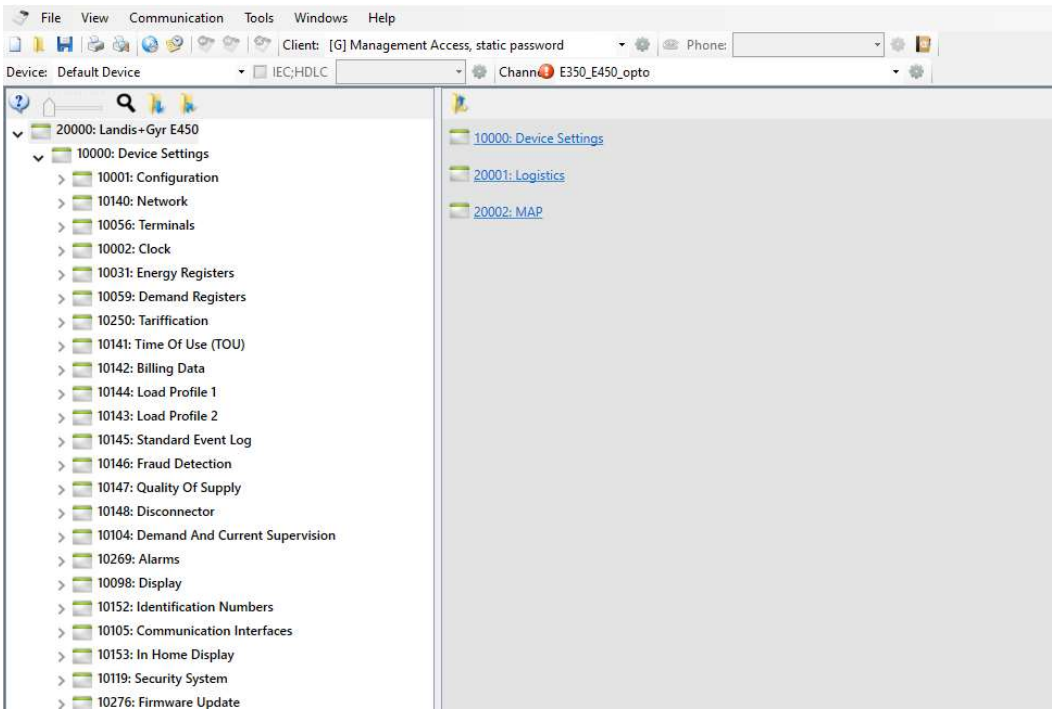


Figure 9 - Screenshot of .MAP120 software

.MAP120 software is mainly used by technicians who are responsible for device configuration, debugging or installation. This software can be used for physical device configuration, configuration backup, configuration restoration etc. This software is also used for monitoring data collection from smart meters, which events could be collected and which will be transmitted by the device to the HES system.

5.3 Log collection from devices

Data from the tested devices could be collected using HES software (using SSH).MAP120 device management software or the HTTP web interface.

Data output is formatted, depending on device, system, and export type, usually in XML, excel or text format.

5.3.1 HES data

The data collected by the centralised controlled environment will be extracted using a web interface produced by a device manufacturer (Landis and Gyr). Data could be

exported from HES in excel format, and event codes are being translated in the HES system and displayed in Figure 10.

2019-06-04 18:00:33+03:00	3.19.17.85	Communication: Modem failure	Event	2019-06-05 09:27:17+03:00
2019-06-03 18:01:55+03:00	3.1.283.29	Communication: New PDP context established	Event	2019-06-04 09:28:48+03:00
2019-06-03 18:00:32+03:00	3.19.17.85	Communication: Modem failure	Event	2019-06-04 09:28:48+03:00
2019-06-02 18:01:27+03:00	3.1.283.29	Communication: New PDP context established	Event	2019-06-03 09:26:28+03:00
2019-06-02 18:00:32+03:00	3.19.17.85	Communication: Modem failure	Event	2019-06-03 09:26:28+03:00
2019-06-02 15:20:40+03:00	3.26.131.37	Voltage quality: Normal Voltage Phase 1	Event	2019-06-03 09:26:28+03:00

Figure 10 - HES output in excel format

HES will not be used for data gathering as this is merely an interface for the operator and only shows information predefined in the device.

5.3.2 Data concentrator debug data

Using the web interface, it is possible to collect the entire debug log in text format from the data concentrator. The dataset gives detailed information of the connected devices, including device software and firmware version, configuration, customer config, resource usage, different logs etc, which can be seen in Figure 11.

In the case of the tested device, the log contained more than twenty thousand events. Depending on log type, the collected period of logs was different, from a day to a month. For example, syslog output was from 2 weeks, and config messages were output for over a month.

Log size changes up to a limit according to the period and events taking place on devices. The manufacturer has limited debug log output to export only a certain amount of information depending on period and events count, depending on the log type.

```
## VERSION ##
## VERSION HISTORY ##
## SERIAL NUMBERS ##
## RTC ##
## UPTIME ##
## CONNECTION STATUS ##
## CONFIG ##
## HW CONFIG ##
## CUSTOMER CONFIG ##
## PRODUCTION EEPROM DATA ##
## DISK USAGE ##
## MEMORY USAGE ##
## NETWORK INTERFACES ##
## ROUTE INFORMATION ##
## NETSTAT INFORMATION ##
## FIREWALL INFORMATION ##
## PROCESS INFORMATION ##
## SLABINFO ##
## UNIX DOMAIN SOCKETS ##
## TCP SOCKETS ##
## FSCK ##
## MTD INFO ##
## BOOTLOADER ENV ##
## IO STAT ##
## IPC FACILITIES ##
## INSTALLED IPKG PACKAGES ##
## APPLICATIONS ##
## APPLICATIONS RUNTIMES ##
## APPLICATIONS MEMORY USAGE ##
## APPLICATIONS DETAILS ##
## APPLICATIONS TIMERS ##
## ODEP STATISTICS ##
## PUSH STATISTICS ##
## CONFIG MESSAGES ##
## ALARMS ##
## EVENT NOTIFICATIONS ##
## DMESG ##
## SYSLOG ##
## EVENT LOG ##
## UNIT CHANGE LOG ##
## MODEM EVENT LOG ##
## PUSH EVENT LOG ##
## ACTIVE ALARM LOG ##
## ACCESS LOG ##
## SECURITY LOG ##
## CONFIGURATION LOG ##
## GSM FIELD STRENGTH LOG ##
## TEMPERATURE LOG ##
## HTTP SESSION LIST ##
## REGISTRY VALUES ##
## TLS PROXY RULES ##
## TLS PROXY CONNECTIONS ##
## TLS CERTIFICATES ##
## FIRMWARE UPDATE JOBS ##
## SOFTWARE UPDATE JOB ##
## PLC STATISTICS OF ALL TIME ##
## PLC STATISTICS OF PREVIOUS PERIOD ##
## PLC STATISTICS OF CURRENT PERIOD ##
## UNITS PLC SUMMARY ##
## UNITS PLAN SUMMARY ##
## UNITS G3 SUMMARY ##
## UNIT LIST ##
## INACCESSIBLE UNIT LIST ##
## ASSOCIATIONS ##
## PLC REGISTRATION HISTORY ##
## UNIT 'xxxxx' COMM STAT ##
## UNIT 'xxxxx' TIME STAT ##
## UNIT 'xxxxx' READING PROFILE AND READING STATUS ##
## READING PROFILE SELECTORS ##
## READING DELAYS ##
## READING STATISTICS ##
## READING PROFILE 'x' ##
## READING PROFILE 'x' UNIT LIST ##
## PUSH PROFILE SELECTORS ##
## PUSH PROFILES ##
## G3 EVENT LOG ##
## G3 ROUTE TABLE ##
## G3 NEIGHBOR TABLE ##
## G3 PATH TABLE ##
## G3 ACTIVE NODE TABLE ##
## G3 DEVICE TABLE ##
## G3 TIME SYNC TABLE ##
## CORE DUMPS ##
## HSM KEYS ##
## LAST REBOOT LOG ##
```

Figure 11 - Debug data topics

5.3.3 Smart meter log data

From the smart meter web interface, it is possible to obtain a complete debug log, in which all diagnostic and log data is accessible. The optical port will be not used as this is not feasible due to low physical protection (could physically be easily removed, tampered etc.), and this communication interface is usually disabled on devices. SSH and HTTP over LAN are also options for communication if only insufficient information is available through the HES application or web interface from smart meters.

Raw smart meter data is outputted in Extensible Markup Language (XML) format. Log data is delivered using timestamp with specific event code(s) in numeric form. Since it contains codes without the proper manufacturer specifications, the processing of the log

is unfeasible. Event code is translated in HES. This kind of obfuscating could keep malicious actor with low skillset away unless they do not have a translation table on hand. Example data can be seen in Figure 12.

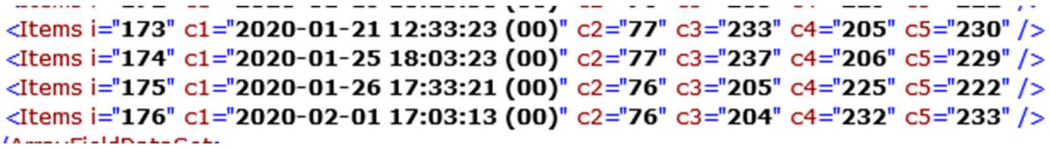


Figure 12 - XML log example

5.4 Findings of data collection methods

Data can be extracted using several methods from smart meters. Data layout and structure is heavily dependent on the channel which will be used for data gathering.

For data gathering .MAP120 and HTTP device interfaces will be used because as these are manufacturer-approved and available methods for a utility or operator to use in the production system or give required information about available information on devices. These communication channels will provide the best overview of available data, as, from the device HTTP port, it is possible to collect whole debug data for analytical work. Optical port, serial and LAN interfaces will not be used as these are not commonly used or are disabled on this kind of setups.

HES system did not provide sufficient data; therefore will not be further analysed.

Debug log is meant for an operator for problem-solving and error tracking on the device. In this thesis, the log data will be used to identify which events are obtainable from devices for monitoring.

6 Data analysis

During the data collection period, the log files of three different devices were captured, resulting in over a hundred thousand log records in total. This chapter will introduce the analysis of the extracted files and conclude the most relevant information and findings in the light of previously introduced smart meter attack vectors and classifications based on event priorities.

6.1 Information collected using .MAP120 analysis

This paragraph will introduce the data that can be collected from smart meters and the different predefined events that can be configured by manufacturer-supplied software '.MAP120'. If an event occurs, the smart meter sends data to HES, transmitting information to the monitoring system where either alarm or monitoring event will be triggered and forwarded to the operator.

The analysis of possible alarms available on the device can help to narrow down the scope but keep it tight enough. Information collected using .MAP120 is included in appendix 2.

Events can be divided into several main categories based on their event type: Alarm triggers, power quality, fraud detection and generic events

6.1.1 Alarm triggers

Alarm triggers events are the events that could be configured using .MAP120 software on smart meters to transmit manufacturer predefined alarms, including errors about system/device, fraud attempts, bad voltage quality and alarms related to M-bus devices[1], which can be seen in Table 1.

[1] M-bus is a Modbus protocol-based PLC communication channel.

Table 1 - Alarm triggers defined by the manufacturer

Alarm triggers	Clock invalid
Alarm triggers	Replace battery
Alarm triggers	Program memory error
Alarm triggers	RAM error
Alarm triggers	NV memory error
Alarm triggers	Measurement system error
Alarm triggers	Watchdog timer elapsed
Alarm triggers	Fraud attempt
Alarm triggers	Total power failure
Alarm triggers	Power resumed
Alarm triggers	Missing neutral
Alarm triggers	Phase asymmetry
Alarm triggers	Current reversal
Alarm triggers	Phase sequence incorrect
Alarm triggers	Unexpected consumption
Alarm triggers	Key exchanged
Alarm triggers	Bad voltage quality L1-L3
Alarm triggers	External alarm
Alarm triggers	Local communication attempt
Alarm triggers	Disconnect/reconnect failure
Alarm triggers	Fraud attempt M-Bus device 1-4
Alarm triggers	Communication error M-Bus device 1-4
Alarm triggers	New M-bus device installed channel 1-4
Alarm triggers	Disconnect/reconnect failure
Alarm triggers	Valve alarm M-Bus device 1-4

6.1.2 Power quality events

Power quality-related events, which could be extracted from the device using .MAP120 are collected from the power quality event log and provide information about over- and undervoltage, bad voltage quality, missing neutral or voltage. A smart meter can also detect current without voltage, phase leakage, phase asymmetry, remote disconnection/connection, or manual connection/disconnection of network and supervision monitor related events.

6.1.3 Fraud detection events

Fraud detection events, defined by the manufacturer, are pretty limited; it is possible to detect physical access (meter cover, terminal cover, physical tampering), strong magnetic field, multiple authentication failures, replay attack and current reversal events.

6.1.4 Generic events

Generic events can be extracted from multiple registers, including standard event log, disconnector event log and fraud detection event log. It is possible to detect power up/down, time adjustment, invalid clock, Time of Use (TOU) registration, RAM, program, Non-volatile (NV) memory, measurement system and watchdog errors, firmware upgrade related events, parameter changes, local communication attempts, billing period changes, extension board errors, Home Area Network (HAN) communication errors, load profile cleared event and remote communication statuses.

Depending on device type, PLC smart meters also have information regarding supervision monitoring 1-3 threshold, disconnector control state-related events and manual/remote disconnection/connection and disconnect/reconnect failure status.

6.2 Data collected from devices

The author collected data from smart meters and data concentrators by exporting full debug logs using HTTP based web interface. This data will be analysed, and only the most relevant information is described in this section.

6.2.1 Linux generic information

From the complete debug log, it is possible to extract operating system related metadata, hardware-specific information, boot loader related information and Linux version, which is in use during device operation.

Device uptime is separately logged and is displayed in the following format:

“10:29:13 up 98 days, 5:10, 0 users, load average: 0.22, 0.18, 0.18”

Hardware config log consists of ethernet addresses, central processing unit (CPU) model and serial number, power supply serial number and device serial number.

Customer config log consists of information about the cellular connection (Access point name (APN), user, password, ping IP and task scheduling information), network time protocol (NTP), server internet protocol (IP) address and how often time is updated.

Disk usage could be logged used regular Linux type disk usage statistics about disk space allocation and different mount points.

Memory usage can be monitored using the memory usage log, which shows statistics about random access memory (RAM) usage on the operating system and Linux swap information.

Process information shows the output of the Linux process ID, user, and application.

6.2.2 Smart meter generic information

As smart meters and data concentrators are relying on Linux architecture, Syslog will provide generic Linux based operating system syslog information. Apart from the ordinary Linux log, syslog also includes the following relevant information:

- Security settings: Security policy and/or authentication mechanism missing;
- Connect script failed;
- dc_network_wake_up: Timeout when waiting COMMS_IP_UP;
- Network interface wake-up failed!;
- open_connection failed! Resource temporarily unavailable;
- Wakeup connection failed!;
- Modem multiplexer down;
- eneatc_read_unsolicited failed: Input/output error;
- Modem not OK. Connection timed out;
- No answer from modem!;
- Cannot initialize modem!;
- Modem multiplexer recovery failed immediately.

The event log will consist of different alarms and notifications. From gathered data, selection of relevant log items:

- ALARM_LID_OPEN;
- ALARM_RTC_INCORRECT_TIME;
- NOTICE_MODEM_CONNECTION_RESET ();
- NOTICE_ODEP_CONNECTION_TIMEOUT ();
- NOTICE_PUSH_CONNECT_ERROR ();

- ALARM_WEAK_GSM_SIGNAL ();
- ALARM_GSM_CONNECTION_DOWN ();
- NOTICE_STARTUP {"cause":"first_boot"};
- NOTICE_REBOOT {"cause":"powerbreak"};
- ALARM_PLAN_MAC_NOT_DEFINED;
- ALARM_POWER_CUT;
- ALARM_LOCAL_ETHERNET_UP;
- NOTICE_MASTER_TIME {"old time":"2019.06.27 00:09:24","new time":"2019.11.18 14:54:27"};
- ALARM_MODEM_UNREACHABLE;
- ALARM_GSM_CONNECTION_DOWN;
- ALARM_PLAN_NO_SYNCHRO;
- ALARM_PLAN_OUT_OF_ORDER;
- NOTICE_SMS_SEND {"phone number":"}.

Event notifications are notifications generated by the manufacturer, triggered at a defined event on the device. Event notification log consists of alarm ON event notifications and event notifications:

- NOTICE_ALL_DATA_REMOVED;
- NOTICE_PROCESS_WD_FAIL;
- NOTICE_OUT_OF_MEMORY;
- NOTICE_RECOVERY_DONE;
- NOTICE_TAMPERING_DETECTED;

Alarm ON event notifications:

- ALARM_RTC_FAULT;
- ALARM_OVER_TEMPERATURE;
- ALARM_NO_SIM;
- ALARM_LOW_DISK_SPACE;
- ALARM_LOW_INODES;
- ALARM_UNIT_SIMULATOR_ACTIVE;
- ALARM_LID_OPEN;

Alarms are detected based on the event log and will generate an alarm in the alarm log with timestamp:

Activation Time	Description
2020.02.04 00:09:21	ALARM_WEAK_GSM_SIGNAL.

Relevant items from modem event log:

- NOTICE_PUSH_REQUEST_EXPIRED (07 01000000);
- NOTICE_PUSH_WAKEUP ();
- NOTICE_PUSH_WAKEUP_OK ();
- NOTICE_PUSH_CONNECTING ();
- NOTICE_PUSH_SENDING_DONE ();
- NOTICE_PUSH_RECEIVING_DONE ();
- NOTICE_PUSH_CLOSING ();
- NOTICE_PUSH_CLOSE_OK ().

The temperature log reports device temperature every 10 minutes and with an accuracy of 0.25c. This is inputted in log – Timestamp - 30.75

Firmware update jobs provide the log provides firmware update jobs historical data, which can be seen in Figure 13.

```
## FIRMWARE UPDATE JOBS ##
fwupdate_cfgtool: /usr/lib/libcrypto.so.1.0.0: no version information available (required by /lib/libdc.so)

-------------------------------------------------------
Job Id                : 7176
Job state             : Done
Job result            : Success
Activation time       : 2018.01.04 15:49:00
Expiration time       : 2018.01.11 06:00:00
Closing time          : 2018.01.05 04:17:00
Push time             : 2018.01.05 04:33:38
Image ID              :
Image URL             :
User name for server  :
Block size            : 64
Priority              : HIGH (6)
Retry count           : 100
Retry delay           : 30
```

Figure 13 - Firmware update job log

6.2.3 Network activity-related information

Network information shows statistics and information about the network, including a point-to-point virtual private network (VPN) interface. Additionally, route

information provides information about network routings in Linux generic style. Netstat is also Linux related generic information that provides data about ping failures, connection activations, connection resets, connection uptime and previous connection starting time. Additionally, if the smart meter/concentrator has a SIM card installed, its serial number also will be logged along with modem model type and failures. Netstat information shows information about datagrams transferred and stored on device, active internet connections, state, IP, sent and received packages and protocol type.

Relevant items from signal event log:

- -93 dBm (10) 3.2% - 6.4% (5) UMTS (3G) 1: Registered, home net 1: Registered, home net;
- -999 dBm (99) Unknown (99) Unknown 2: Not reg., searching 0: Not registered.

HTTP session list log consists of entries of services and IP-s connected to them, as shown in Figure 14.

```
## HTTP SESSION LIST ##
   age    login    last  errors  locked  service  user                client
-------------------------------------------------------------------------------------
5198843     3326      19       0       0  http     service
7647814     3408    3314       0       0  http     service              127.0.0.1
```

Figure 14 - HTTP Session list log

Relevant events collected from modem event log are following:

- NOTICE_MODEM_SHUTDOWN ();
- NOTICE_MODEM_SHUTDOWN ();
- NOTICE_PING_FAILURE ();
- NOTICE_MODEM_RESTART_REQUEST {"cause":"modem test failed"};
- NOTICE_MODEM_SHUTDOWN {"cause":"restart request"};
- NOTICE_MODEM_READY {"modem":""};
- NOTICE_MODEM_CONNECTING {"apn":""};
- ALARM_MODEM_UNREACHABLE;

- ALARM_GSM_CONNECTION_DOWN;
- ALARM_MODEM_UNREACHABLE.

Relevant log entries in registry values log:

- cpu.load.15min=15.9375;
- cpu.load.24h=15.5336;
- gprs.activations=1878;
- gprs.current.start_time=1519227147;
- gprs.current.start_uptime=7726413;
- modem.firmware.version={Modem firmware version}.

TLS proxy log consists of information about network proxy rules, which is formatted like typical Linux iptables.

TLS proxy connections provide information about network connections made to the device using the TLS encryption method, cypher name, bits, transmitted and received data count, subject name of certificate, serial, end and start time, peer and local IP address/port.

TLS certificate logs will include trusted certificates, their metadata and certificate signature.

6.2.4 PLC specific information

PLC statistics log of the previous period can be seen in Figure 15.

```
## PLC STATISTICS OF PREVIOUS PERIOD ##
ask: /usr/lib/libcrypto.so.1.0.0: no version information available (required by ask)
ask: /usr/lib/libcrypto.so.1.0.0: no version information available (required by /lib/libdc.so)
PLAN statistics
 statistics collected since    : 2018.03.01 00:00:00
 statistics collected until    : 2018.03.02 00:00:00

 idling time                   : 28m 12s         1.96  %
 background task time          : 22h 55m 13s     95.50 %
 plc controlling time          : 17m 5s          1.19  %
 reading time                  : 5m 1s           0.35  %
 processing time               : 14m 29s         1.01  %
 period duration               : 1d 0h 0m 0s     100 %
 throughput                    : 0.880 msg/s, 3169.7 msg/h
 message statistics:
   Credit   Sent successfully  Sent total   Failed   Wasted time (estimate)   Wasted bandwidth (estimate)  Quality (%)
        0                71430       72268      838                 20m 57s                         1.5 %       98.8 %
        1                 2314        3039      725                 36m 15s                         2.5 %       76.1 %
        2                  605         689       84                  6m 18s                         0.4 %       87.8 %
        3                   20          34       14                  1m 24s                         0.1 %       58.8 %
        4                   43          43        0                      0s                         0.0 %      100.0 %
        5                    0           0        0                      0s                         0.0 %        0.0 %
        6                    0           0        0                      0s                         0.0 %        0.0 %
        7                    0           0        0                      0s                         0.0 %        0.0 %
    Total                74412       76073     1661                1h 4m 54s                         4.5 %       97.8 %
```

Figure 15 - PLC statistics of the previous period

PLC statistics of the current period consists of the same information as PLC statistics of the previous period, with the main difference of timeframe observed.

Units PLC summary of PLC units shows overall statistics about PLC functioning, as shown in Figure 16.

```
## UNITS PLC SUMMARY ##
ask: /usr/lib/libcrypto.so.1.0.0: no version information available (required by ask)
ask: /usr/lib/libcrypto.so.1.0.0: no version information available (required by /lib/libdc.so)

Total amount of units             : 11
Communication quality (last 24h)  : 86.3 %

Amount of accessible units        : 8
Acc. unit comm. quality (last 24h) : 96.1 %
All PLC units

Unit id          Quality (24h)  Succ msgs  Sent msgs    Failures     Status
-------------------------------------------------------------------------------
                                   100.0       8315        8316         0          (0  ) OK
                                   100.0       8386        8387         0          (0  ) OK
                                   57.1          72         126        21          (256) WAITING FOR SECURITY PARAMETERS
                                   56.4         106         188        31          (256) WAITING FOR SECURITY PARAMETERS
                                   99.8        8315        8328         0          (0  ) OK
                                   100.0       8314        8318         0          (0  ) OK
                                   99.7        8308        8337         0          (0  ) OK
                                   93.3        8310        8910         0          (0  ) OK
                                   88.4        8294        9379         0          (0  ) OK
                                   67.1          94         140         1          (256) WAITING FOR SECURITY PARAMETERS
                                   87.3        8299        9501         0          (0  ) OK
```

Figure 16 - Units PLC summary

Unit list log shows other devices unit identifier numbers connected to this concentrator.

The unit list should be monitored, and an alert should be generated if a new device is added or a device is removed from the list.

Inaccessible unit list logs devices, which are inaccessible by this data concentrator.

This should be monitored and checked; if any new device added to the list, it most certainly is a cyber event as availability has been compromised.

PLC registration history shows a timestamp with a unit identifier when a new registration is created. Registration means that two devices successfully have set up a new connection.

Unit communication statistic logs consist of information about different smart metering devices connected to the data concentrator and communication statistics between them. Example log can be seen in Figure 17.

```
## UNIT '               ' COMM STAT ##
ask: /usr/lib/libcrypto.so.1.0.0: no version information available (required by ask)
ask: /usr/lib/libcrypto.so.1.0.0: no version information available (required by /lib/libdc.so)
general
 * id                     :
 * status                 : OK (0)
 * unit type              : E450 IDIS
 * plc type               : PLAN
 * max pdu size           : 126
 * device[1] MID checksum : DE30CEBE
 * device[1] serial number :
 * device[1] utility id   :
 * device[1] param id     :
 * device[1] config id    :
 * device[1] fw version   : V
 * installation state     : Internal value:              65535
                            INSTALLATION:           COMPLETED

plc specific data
 * system title           :
 * mac address            : 6
 * Previous sent credit   : 0
 * Previous real credit   : 0
 * Credit for next msg    : 0
 * registration time      : 2018.02.13 17:08:19
 * delta phase            : 0 degrees
 * repeater               : Dynamic repeater (2)
 * repeater status        : True
 * vde[1] lsap            : 1
 * vde[1] vde             : 3080
 * vde[1] security policy : 2
 * vde[1] conformance     : 00000000000011010000011101
 * vde[1] max pdu size    : 1500

Security settings

 Frame counters:
 * Global TX frame counter                      : 2273983
 * Global RX frame counter                      : 2272867
 Current security settings
 * Current data transfer security policy        : 2: All messages are encrypted
 * Current data access security mechanism       : 5: High Level Security (HLS) - GMAC
 * Hashed current LLS password                  : 2BD39913B381987D3AFA521C75E8FD8C7EA9F1D9
 * Hashed current global unicast encryption key : 56178B86A57FAC22899A9964185C2CC96E7DA589
 * Hashed current global broadcast encryption key: 6B8F0429829EDE51E1071909DFDBDD7B78825D2B
 * Hashed current authentication key            : 58361C793128E3B2AEC5302512764l8C232BF277

 New security settings
 * Hashed new global broadcast encryption key   : 6B8F0429829EDE51E1071909DFDBDD7B78825D2B

communication statistics
 * contacted after powercut: yes
 * total msgs sent         : 10803660
 * total msgs succ         : 10791910
 * total quality           : 99.9 %
 * last succ time          : 2018.03.02 10:29:35
 * last fail time          : 2018.03.01 20:27:30
 * consecutive failures    : 0
 * processing time         : 0s
 * roundtrip time average  : 922 ms
 * Successfully sent messages by credit:
   Credit      Messages
   0           10790663
   1           1050
   2           156
   3           24
   4           17
   5           0
   6           0
   7           0
 * hourly sent messages :
   00  h:     368/368      100.0 %  |    12  h:     283/283      100.0 %
   01  h:     354/354      100.0 %  |    13  h:     392/392      100.0 %
   02  h:     409/409      100.0 %  |    14  h:     371/371      100.0 %
   03  h:     343/343      100.0 %  |    15  h:     415/415      100.0 %
   04  h:     265/265      100.0 %  |    16  h:     366/366      100.0 %
   05  h:     307/307      100.0 %  |    17  h:     355/355      100.0 %
   06  h:     317/317      100.0 %  |    18  h:     337/337      100.0 %
   07  h:     330/330      100.0 %  |    19  h:     355/355      100.0 %
   08  h:     355/355      100.0 %  |    20  h:     385/384       99.7 %
   09  h:     332/332      100.0 %  |    21  h:     334/334      100.0 %
   10* h:     188/188      100.0 %  |    22  h:     366/366      100.0 %
   11  h:     414/414      100.0 %  |    23  h:     375/375      100.0 %

* registration history:
  2018.02.13 17:08:19
  2017.09.02 16:08:21
  2017.07.06 21:04:43
  2016.09.11 21:15:07
  2015.05.24 10:03:05
```

Figure 17 - Unit comm stat log example

This info could be correlated between unit list log to identify the anomaly.

Unit time statistic logs contain information about connected unit ID, last reading time, unit time and the time difference between concentrator and unit.

This could be used to verify if the smart meter and concentrator time are synchronised.

Unit reading profile and reading status provide information about last consumption reading, capture period, priority and register id.

This could detect any unauthorised configuration changes on the device and if readings are captured from smart meters.

6.3 Findings

Collected data shows sufficient data available from AMI network devices that could be used for monitoring. The information gathered previously in this work will be analysed and described in this chapter. Collected data from HES is included in Appendix 2.

6.3.1 Unauthorised access monitoring

Unauthorized access to the device could be detected by using manufacturer supplied methods for monitoring using fraud detection event log:

- Terminal cover removed;
- Terminal cover closed;
- Meter cover removed;
- Meter cover closed;
- Multiple authentication failures;
- Decryption or authentication failure;
- Replay attack.

Information collected from debug files prove that it is additionally possible to monitor the following logs:

- Netstat information - active sessions/connections to device;
- Process information – possible malicious processes running;
- HTTP session list – active unauthorized sessions;
- TLS proxy connections – unauthorized connections;

- TLS certificates – unauthorized certificates added to a device could provide traces of unauthorized access happening in future or past attempts.

6.3.2 Information alteration monitoring

Visibility over information alteration attacks could be monitored using different events from manufacturer supported and manual gathering of information from devices. The following information could be gathered using manufacturer supported methods:

Alarm triggers could be used to detect the following errors: program memory error, RAM error, Non-Volatile (NV) memory error, key exchanged.

Standard event log triggers could be used for detection of the following events: Power down, power up, strong DC field detected, no strong DC field anymore, watchdog occurred, firmware ready for activation, firmware activated, passive TOU programmed, one or more parameters changed, global key(s) changed, firmware verification failed, local communication attempt, firmware update limit reached, HAN communication error, HAN communication ok, remote communication error, remote communication ok, profile checksum error, parameter restoration failed, profile checksum ok, passive TOU activation failed, load profile cleared, event log cleared.

Fraud detection events could be used to detect decryption or authentication failure and replay attack.

Power quality event log detects anomalies in power transmission – Phase asymmetry, missing neutral, power factor below a threshold, phase leakage.

There is available information about network, RAM, hard disk, and configuration monitoring from debug logs. If RAM or CPU usage increases more than usual, then this means that malicious code could be running on the device or non-standard network connections are ongoing with the device.

6.3.3 DOS attack monitoring

DOS attack monitoring could be done by detecting authentication failures, network resources monitoring and anomaly detection. Using the manufacturer-provided solution, it is possible to detect the following events:

- Fraud detection event log provides multiple authentication failures, decryption or authentication failure or replay attack events,

- The disconnector control log provides information about remote disconnection remote connection.

Using information gathered from debugging files, it is possible to monitor TLS proxy connections, TLS proxy rules, HTTP sessions list, netstat information and route information logs to detect unauthorised connections to devices or made by devices.

Monitoring device resources could support the detection of DOS events – CPU, RAM, network usage as this could provide information about malicious code running on the device.

6.3.4 PLC specific attack monitoring

PLC specific events could be monitored using manufacturer supplied events or debug information from the device itself. Manufacturer monitorable events:

- Alarm triggers events – Bad voltage quality events, M-bus related events if M-bus is used in the system;

- Power quality event log – bad voltage quality events, phase leakage.

It is possible to collect information about devices connected to the data concentrator using PLC statistics and units list could help identify anomalies from debug log.

6.3.5 Simulated activities

Smart meter lid removal generated log entries of meter cover removed and closed accordingly and as predicted.

For SIM card removal, the meter cover had to be removed, which generated the meter cover removal alert. The next step was to remove the communication module, to access the SIM card slot. Communication module removal caused additional entries in debug log. After the SIM card removal, no SIM card event was generated and saved in log files.

Power cut simulation caused few entries into log files – Missing voltage, power cut alarm and local disconnection. The result was expected because the test device was operating

over a mobile network, and smart meters have a battery installed internally for this kind of causes, so the smart meter could report to the server the reason for going offline.

3G antenna removal itself only affected the signal strength 5db and generated meter lid removal event needed to access antenna.

SSH and HTTP sessions did not generate any significant entries detectable using manufacture supplied methods. It is possible to detect these events by monitoring the access log and HTTP session in the HTTP session list with client IP from the full debug log.

6.4 Event priorities

Using event priorities presented before, it is possible to organize events based on their probable cyberattack cause into three categories.

6.4.1 Critical events

Events are considered critical if more than 20 clients could be affected by a malicious actor. Critical events are chosen based on attack vectors and priorities described previously. Events that are considered crucial and must be monitored are described in Table 2Table 2.

Table 2 - Critical priority events

Category	Name of event	Method of collection	Attack vector
Fraud detection events	Multiple authentication failure	HES	Information alteration
Fraud detection events	Decryption or authentication failure	HES	Information alteration
Fraud detection events	Replay attack	HES	DOS attack
Alarm triggers	Key exchanged	HES	Information alteration
Standard event log triggers	HAN communication error	HES	DOS attack
Standard event log triggers	HAN communication ok	HES	DOS attack
Communication channels status	Diagnostic port status	Debug log	Information alteration
Communication channels status	Ethernet status	Debug log	Information alteration
Communication channels status	SSH	Debug log	Information alteration
Communication channels status	Cellular	Debug log	Information alteration
Communication channels status	PLC	Debug log	Information alteration
Operating system resource usage	Hard disk space	Debug log	Information alteration
Operating system resource usage	RAM	Debug log	Information alteration
Operating system resource usage	CPU usage	Debug log	Information alteration
Serial numbers	Unit serial number	Debug log	Information alteration
Serial numbers	SIM card serial number	Debug log	Information alteration
Generic data	Last configuration update	Debug log	Information alteration
Generic data	Last firmware update	Debug log	Information alteration
Data concentrator connections	Connected device name	Debug log	PLC specific attack
Data concentrator connections	Connected device serial number	Debug log	PLC specific attack
Data concentrator connections	Connected device netowork address	Debug log	PLC specific attack

6.4.2 Medium priority

Medium priority events provide visibility over the grid about events that could affect a small portion of the network (e.g. substation distribution area). These events should be monitored to ensure grid service operation all over the network. Medium priority events are considered events that affect 5 to 20 clients. These events are described in Table 3.

Table 3 - Medium priority events

Category	Name of event	Method of collection	Attack vector
Standard event log triggers	Remote communication error	HES	DOS attack
Standard event log triggers	Remote communication ok	HES	DOS attack
Power quality event log	Undervoltage L1-L3	HES	PLC specific attack
Power quality event log	Overvoltage L1-L3	HES	PLC specific attack
Power quality event log	Missing voltage L1-L3	HES	PLC specific attack
Power quality event log	Missing neutral	HES	PLC specific attack
Power quality event log	Phase asymmetry	HES	PLC specific attack
Power quality event log	Bad voltage quality L1-L3	HES	PLC specific attack
Power quality event log	Current without voltage L1-L3	HES	PLC specific attack
Power quality event log	Power factor below threshold	HES	PLC specific attack
Power quality event log	Power factor normal	HES	PLC specific attack
Power quality event log	Phase leakage	HES	PLC specific attack
Power quality event log	Critical overvoltage L1-L3	HES	PLC specific attack

6.4.3 Low priority

Events are categorised as low priority events if malicious activity is directed against five or fewer devices. Events considered low priority are shown in Table 4Table 4.

Table 4 - Low priority events

Category	Name of event	Method of collection	Attack vector
Standard event log triggers	Profile checksum error	HES	Information alteration
Standard event log triggers	Parameter restoration failed	HES	Information alteration
Standard event log triggers	Profile checksum ok	HES	Information alteration
Power quality event log	Phase asymmetry	HES	PLC specific attack
Fraud detection events	Missing neutral	HES	PLC specific attack
Fraud detection events	Power factor below threshold	HES	PLC specific attack
Fraud detection events	Phase leakage	HES	PLC specific attack
Fraud detection events	Terminal cover removed	HES	Information alteration
Fraud detection events	Terminal cover closed	HES	Information alteration
Fraud detection events	Strong DC field detected	HES	Information alteration
Fraud detection events	No strong DC field anymore	HES	Information alteration
Fraud detection events	Meter cover removed	HES	Information alteration
Fraud detection events	Meter cover closed	HES	Information alteration
Generic data	No sim card	Debug log	Information alteration
Generic data	Over temperature	Debug log	DOS attack
Generic data	Low inodes	Debug log	DOS attack

6.5 Monitoring data proposal

To provide visibility about unauthorized access to the device, physical device abuse, DOS attacks, the service provider should monitor events presented in this section based on priorities:

- Events and alarms defined by manufacturer – Alarm triggers, standard event log, fraud detection logs, power quality event log;
- Communication channels status – enabled or disabled (diagnostic port, optical port, ethernet, SSH, cellular, PLC);
- Operating system resource usage over time (Hard disk space, RAM, CPU usage);
- Additional information available from the device - disk space, no sim card, over-temperature, low inodes, lid open etc.;
- Available serial numbers (CPU, unit serial number, SIM card);
- Last configuration update;
- Last firmware update;
- Uptime;
- Data concentrator connected devices and their serial numbers.

7 Detection and alerts

Based on analytical work and threats described in 4.3, this section recommends which logs and events should be monitored. Additionally, based on which events, automatic alerts could be generated.

From analysing data, due to a large number of devices in the network and low PLC network speed, collecting all this data from every device could be impossible because of the low bandwidth and high latency of PLC.

3G smart meters are more capable and could potentially transmit this data, but the next bottleneck could be computing resource on the server or even the network layer before the server. Therefore, it is mandatory to select only the most relevant information about devices.

7.1 Monitoring events

The following events should be logged to gain visibility over network devices status and cyberattacks taking place against the smart metering system.

General smart meter events:

- Alarm triggers;
    - Clock invalid;
    - Replace battery;
    - Program memory error;
    - RAM error;
    - NV memory error;
    - Measurement system error;
    - Watchdog timer elapsed;
    - Fraud attempt;
    - Total power failure;
    - Power resumed;
    - Missing neutral;
    - Phase asymmetry;

    - Current reversal;
    - Phase sequence incorrect;
    - Unexpected consumption;
    - Key exchanged;
    - Bad voltage quality;
    - External alarm;
    - Local communication attempt;
    - Disconnect/reconnect failure;
    - New M-bus device installed channel 1-4;
    - Valve alarm M-Bus device 1-4;
- Power quality event log all options;
- Disconnector event log all options;
- Fraud detection event log all options;
- Standard event log all options.

Additionally, from the device directly, there is available information, which either manufacture should add support to or utility gather this information using other methods (SSH, for example):

- Software and hardware version;
- Device uptime;
- Users logged in to the system;
- Hardware configuration monitoring (CPU model, serial number);
- NTP information (NTP IP, Scheduled task information);
- Disk usage;
- Process list;
- Memory usage;
- Network interface information;
- Route information;
- Netstat.

Cellular type smart meter specific events:

- Customer-specific APN settings (APN name, IP);
- Connection status including SIM serial no.

PLC type smart meters specific events:

- Alarm triggers events (bad voltage quality events, M-Bus related events – if m-bus is used);
- Power quality events log (Phase leakage, missing neutral);
- PLC unit list;
- PLC registration history;
- Inaccessible device list.

7.2 Automatic alerts

From a cybersecurity point of view, the following automatic alerts should be generated based on the following events defined by the manufacturer:

- All alarm trigger events;
- All fraud detection events;
- All standard event log events;
- All disconnector control log events.

Additionally, events should be generated based on information available from debugging file on the device:

- Route information - New network routes added;
- Connection status log - a drastic increase of connection activation, resets or uptime changes happen, SIM card serial number change;
- Process information log – New unplanned process created/added;
- Event log – Manufacturer defined alerts, additionally start-up/reboot, power cut, ethernet up/down, connection down, time out of sync, plan out of order and entries of sent short message service (SMS);
- Modem event log - unplanned Global System for Mobile Communications (GSM), information change or ping failure;
- Temp log - sudden or max temp exceeded ;
- HTTP sessions list – New unplanned HTTP session added to the list;
- TLS proxy rules – If a new rule is added to the list;
- TLS proxy connection – New entries added based on the whitelist;

- TLS certificates – New certificate added to the system;
- PLC statistics;
- Connected PLC meters to concentrator – new device added/removed;
- Inaccessible PLC meter list change – New device added.

To reduce the high rate of false-positive alerts, memory, CPU, disk and network usage should be logged and monitored with thresholds defined based on normal device activity. Normal device activity should be defined based on monitoring specific device models to reduce the possibility of regular device activity generating alerts in monitoring.

8 Conclusion

Smart grid type of network utilizing AMI is a rapidly growing industry standard that is being implemented worldwide. The implementation of smart meters introduces new attack vectors that could affect the electricity network's stability worldwide.

The author analysed over a hundred thousand logs to identify possible monitoring and automatic alert generation events. This paper provides a basic framework of events that should be monitored by utilities that have implemented AMI type of network.

8.1 Analysis results

The author analysed the logging capabilities of manufacturer-supplied tools and information from debugging files, presenting interesting findings. As smart meters used in this work are based on the Linux operating system, it is possible to easily gather significant portions of information using SSH or another network type of protocol. A limiting factor could be PLC channel speed, which in Estonia is 2400 bps. Additionally, this might void the warranty or support of the manufacturer. This implies that it is mandatory to pick only the most critical information if using that kind of transmission channel.

Manufacturers should consider implementing event correlation and anomaly detection techniques to reduce data amounts and generate more informative events.

8.1.1 Monitoring suggestion

Using manufacturer-provided tools and methods, it is recommended that the following information is gathered:

- Alarm triggers;
    - Clock invalid;
    - Replace battery;
    - Program memory error;
    - RAM error;
    - NV memory error;
    - Measurement system error;

    - Watchdog timer elapsed;
    - Fraud attempt;
    - Total power failure;
    - Power resumed;
    - Missing neutral;
    - Phase asymmetry;
    - Current reversal;
    - Phase sequence incorrect;
    - Unexpected consumption;
    - Key exchanged;
    - Bad voltage quality;
    - External alarm;
    - Local communication attempt;
    - Disconnect/reconnect failure;
    - New M-bus device installed channel 1-4;
    - Valve alarm M-Bus device 1-4;
- Power quality event log all options;
- Disconnector event log all options;
- Fraud detection event log all options;
- Standard event log all options.

Additionally, the utility could collect this information from smart meters or data concentrators if the collection does not void manufacturer support or warranty:

- Software and hardware version;
- Device uptime;
- Users logged in system;
- Hardware configuration monitoring (CPU model, serial number);
- NTP information (NTP IP, Scheduled task information);
- Disk usage;
- Process list;
- Memory usage;
- Network interface information;
- Route information;

- Netstat.

Cellular type smart meter specific events:

- Customer-specific APN settings (APN name, IP);
- Connection status including SIM serial no.

PLC type smart meters specific events:

- Alarm triggers events (bad voltage quality events, M-Bus related events – if m-bus is used);
- Power quality events log (Phase leakage, missing neutral);
- PLC unit list;
- PLC registration history;
- Inaccessible device list.

8.1.2 Smart meter cyberattack detection

For attack detection, the utility should generate automatic alerts on the following events:

- All alarm trigger events;
- All fraud detection events;
- All standard event log events;
- All disconnector control log events.

Additionally, events could be generated based on information available from debugging file on the device:

- Route information - New network routes added;
- Connection status log - a drastic increase of connection activation, resets or uptime changes happen, SIM card serial number change;
- Process information log – New unplanned process created/added;
- Event log – Manufacturer defined alerts, additionally start-up/reboot, power cut, ethernet up/down, connection down, time out of sync, plan out of order and entries of sent short message service (SMS);
- Modem event log - unplanned Global System for Mobile Communications (GSM) information change or ping failure;
- Temp log - sudden or max temp exceeded;

- HTTP sessions list – New unplanned HTTP session added to the list;
- TLS proxy rules – If a new rule is added to the list;
- TLS proxy connection – New entries added based on a whitelist;
- TLS certificates – New certificate added to the system;
- PLC statistics;
- Connected PLC meters to concentrator – new device added/removed;
- Inaccessible PLC meter list change – New device added.

8.2 Conclusion of analytical work

Using manufacturers tools for log and alarms collection, it is possible to obtain partial visibility over a network with low effort. The utility should use this information as it is considered an easily achievable goal.

Utilities can also prioritise information collection based on the potential disruption size of a cyberattack and only critical monitor events. Still, it is highly suggested to use all identified monitoring events, including medium and low priority.

To gain additional visibility over the AMI network, it is recommended to gather additional data on smart meters. The device manufacturer should support this as it provides much-needed visibility and should not generate too much extra network traffic. Meanwhile, the utility could gather this information from devices by utilizing SSH connection to devices.

PLC network speed is the most significant limiting factor on information gathering viewpoint as this slows transmission and makes it harder to function in near real-time. It is possible to either replace PLC devices with cellular connection or add physical network connection by either fibre optical cable or regular ethernet cable. Additionally, the manufacturer could implement event correlation. This could help speed up communication and reduce latency. Unfortunately, this could mean a significant investment when considering the number of devices in a network.

Device manufacturers should implement additional logging features to gather valuable data about device status, which are considered as critical:

- Communication channels status;

        - Diagnostic port;
        - Ethernet;
        - SSH;
        - Cellular;
        - PLC;
    - Route information – New network routes added;
    - Connection status log;
        - Increase of connection activation;
        - Increase of connection resets;
        - Connection uptime changes;
    - Process information – new processes, which are not in the whitelist is started;
    - Device temperature;
        - Warning notification;
        - Critical notification;
    - HTTP sessions list – Unplanned HTTP session added to list;
    - TLS proxy rules – New rules added to list notification;
    - TLS proxy connection – New entries added to list compared against whitelist;
    - New TLS certificate added to the system;
    - PLC statistics;
        - Connected PLC meters to concentrator;
        - Inaccessible PLC meter list changes/new unreachable devices;
    - Operating system resource usage;
        - Hard disk space;
        - RAM;
        - CPU usage;
        - Process list;
    - Serial numbers;
        - Unit serial number;
        - SIM card serial number;
    - Last configuration update;
    - Last firmware update;
    - Data concentrator connected devices and their serial numbers;

- Software and hardware version;
- Device uptime;
- Users logged in the system – could just be notified of a new user logged in to system;
- NTP information;
    - NTP IP;
    - Scheduled task information.

To reduce the high rate of false-positive alerts, memory, CPU, disk, and network usage should be logged and monitored with thresholds defined based on normal device activity. Normal device activity should be defined and excluded from monitoring as these events would quickly overwhelm operators.

8.3 Verification of proposal

For verification, production testing is needed because from the lab, there is not enough data available to verify required events, e.g. power quality-related events, PLC related communication limitations (length of cable), DOS attacks caused by home appliances.

Verification of the proposal is not included in this paper as this requires production experiments and data. Production testing cannot be conducted due to the nature of electricity grid service and legal limitations (GDPR and confidentiality).

These recommendations and proposal will be input for the H2020 project and will be validated. The validation process will determine if these recommendations are valid, need to be improved or changed drastically. H2020 will validate results over multiple European countries' networks, which constists different manufacturer devices and different network setups. This will provide the best possible verification for this thesis.

8.4 Possible future topics

As this paper concentrates on background research and data available from smart meters, different testing tools should be conducted. Anomaly detection and event correlation techniques could be leveraged to reduce the data amounts needed to transmit over the PLC network, known as low bandwidth.

For future work, there are numerous topics to research as this paper provides recommendations for utilities on how to prioritise and what events should be monitored. This work only used single manufacturer devices, and manufacturers tend to limit tools available for utility. The same analytical work should be carried out using different devices from alternative manufacturers. This would provide more universal recommendations or a better overview of available information from smart meters.

Additionally, the research could be undertaken concerning different methods of securing communication between smart meters. Perhaps blockchain-based communication could be used for data protection, ensuring integrity and data anonymisation for big data analytics.

Machine learning methods applicability could be tested – if AMI data is sufficient for machine learning and if it actually would be beneficial for monitoring and event detection.

Devices using poor quality electronic components or design that can influence the PLC network communication could also be researched. This is a common problem in today's production network and is usually mitigated by installing filters in the communication channel or replacing smart meters with cellular type smart meters.

In future, it is highly recommended to gather logs from multiple devices operating in a production environment. Information could be analysed more in-depth using data correlation methods and anomaly detection.

References

[1] M. C. G. L. D. M. M. R. S. V. S. U. Antonio Puca, "Energy and eMergy assessment of the production and operation of a personal computer," *Resources, Conservation and Recycling,* vol. 116, no. January, pp. 124-136, 2017.

[2] E. Energia, "Eesti Energia - Eesti Energia selgitused Tartu elektrikatkestuse kohta," [Online]. Available: https://www.energia.ee/et/uudised/avaleht/-/newsv2/migreeritud-uudis-269?showLogin=true. [Accessed 16 March 2021].

[3] J. . Zheng, D. W. Gao and L. . Lin, "Smart Meters in Smart Grid: An Overview," , 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6520030. [Accessed 18 3 2021].

[4] A. H. C.-C. L. Chih-Che Sun, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018.

[5] K. Karaishi and M. Oguchi, "Evaluation of Smart Grid Simulation System with Power Stabilization by EV," *Network Protocols and Algorithms,* vol. 5, no. 1, pp. 71-89, 2013.

[6] J. Smith, J. Pereyda and D. Gammel, "Cybersecurity best practices for creating resilient control systems," in *Resilience week (RWS)*, 2016.

[7] G. A. N. Y. Jui-Sheng Chou, "Smart meter adoption and deployment strategy for residential buildings in Indonesia," *Applied Energy,* vol. 128, pp. 336-349, 2014.

[8] M. A. ShanZhou, "Smart meter deployment in Europe: A comparative case study on the impacts of national policy schemes," *Journal of Cleaner Production,* vol. 144, pp. 22-32, 2017.

[9] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasure," in *7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015*, 2015.

[10] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," *IEEE Transactions on Power Systems,* vol. 32, no. 4, pp. 3317-3318, 2017.

[11] CRSrinivasan, "Hobby hackers to billion-dollar industry: the evolution of ransomware," *Computer Fraud & Security,* vol. 2017, no. 11, pp. 7-9, 2017.

[12] T. M. C. S. D. A. K. Plėta Tomas, "Cyber-Attacks to Critical Energy Infrastructure and Management Issues: Overview of Selected Cases," *Insights Into Regional Development,* vol. 2, no. 3, 2020.

[13] R. a. S. F. Anderson, "Smart meter security: a survey.," University of Cambridge Computer Laboratory, United Kingdom, 2011.

[14] C. Bennett and D. Highfill, "Networking AMI Smart Meters," in *IEEE Energy 2030 Conference, ENERGY*, 2008.

[15] D. P. S. M. D. a. P. M. Stephen McLaughlin, “Multi-vendor Penetration Testing in theAdvanced Metering Infrastructure,” in *ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference*, New York, 2010.

[16] S. N. Lighari, B. B. Jensen, D. M. A. Hussain and A. A. Shaikh, “Attacks and their defenses for advanced metering infrastructure,” in *2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, St. Petersburg, Russia, 2014.

[17] C. I. ZIDARU, “THE NEWLYCYBERSEAS PROJECT OF THE ROMANIAN ENERGY CENTER ON CYBER SECURITYACCEPTED FOR FUNDING BY THE EUROPEAN COMMISSION,” Romanian Energy Center, 30 March 2021. [Online]. Available: https://www.crenerg.org/wp-content/uploads/2021/03/210330_THE-NEWLY-CYBERSEAS-PROJECT-OF-CRE-ON-CYBER-SECURITY-ACCEPTED-FOR-FUNDING-BY-THE-EUROPEAN-COMMISSION_CZI_vf.pdf. [Accessed 22 April 2021].

[18] G. Dileep, “A survey on smart grid technologies and applications,” 2020.

[19] M. Q. A. A. A. S. S. A. Naeem Raza, “Study of Smart Grid Communication Network Architectures and Technologies,” *Journal of Computer and Communications,* vol. 7, no. 3, pp. 19-29, 2019.

[20] “Eesti energia - Wikipedia,” [Online]. Available: https://en.wikipedia.org/wiki/Eesti_Energia. [Accessed 06 April 2021].

[21] “Eleringile kuuluvad liinid,” Elering AS, [Online]. Available: https://elering.ee/eleringile-kuuluvad-liinid. [Accessed 17 03 2021].

[22] R. K. Pandey and M. Misra, “Cyber security threats — Smart grid infrastructure,” in *2016 National Power Systems Conference (NPSC)*, Bhubaneswar, India, 2016.

[23] L. O. Nweke, “Using the CIA and AAA Models to Explain Cybersecurity Activities,” *PM World Journal,* vol. 6, no. 12, 2017.

[24] “European Network for Cyber Security - Our Mission,” The European Network for Cyber Security, [Online]. Available: https://encs.eu/our-mission/. [Accessed 28 03 2021].

[25] ENISA, “ENISA - NIS directive,” [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive. [Accessed 30 03 2021].

[26] F. M. Cleveland, “Cyber security issues for Advanced Metering Infrasttructure (AMI),” in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[27] A. a. K. S. a. K. W. Khattak, “Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasure,” in *Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019 (pp.554-562)*, 2019.

[28] P. a. L. Y. a. B. G. a. P. A. a. D. J. a. M. A. Kumar, “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues,” *IEEE Communications Surveys & Tutorials,* vol. PP, pp. 1-1, 2019.

[29] A. a. R. N.-E. Alnasser, “Design of a trust security model for smart meters in an urban power grid network,” in *edings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Montreal, 2014.

[30] W. Ali, G. Dustgeer, M. Awais and M. A. Shah, “IoT based smart home: Security challenges, security requirements and solutions,” in *2017 23 international conference on automation and computing*, 2017.

[31] C.-H. Y. a. J. K. Seul-Ki Choi, “System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats,” *KSII Transactions on Internet and Information Systems (TIIS) ,* vol. 12, no. 2, pp. 906-918, 2018.

[32] S. P. De Dutta, “Security for Smart Grid in 5G and Beyond Networks,” *Wireless Personal Communications,* vol. 106, no. 1, pp. 261-273, 2019.

[33] M. H. M. K. a. S. K. T. Kim, “Mass authentication information injection method for effective security management of AMI device,” in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, 2020.

[34] “Tööstusest - Küberkurjategijate ees uks kinni,” Tööstusest, November 2017. [Online]. Available: https://toostusest.ee/uudis/2017/11/09/kuberkurjategijate-ees-uks-kinni/. [Accessed 28 03 2021].

[35] Elektrilevi, “Uudised - Elektrilevi paigaldab aasta lõpuks 147 000 kaugloetavat arvestit,” June 2013. [Online]. Available: https://www.elektrilevi.ee/uudised/avaleht/-/newsv2/2013/06/12/elektrilevi-paigaldab-aasta-lopuks-147-000-kaugloetavat-arvestit. [Accessed 28 03 2021].

[36] C. F. T. H. F. S. S. B. S. R.-M. D. E. Günther Eibl, “Exploration of the Potential of Process Mining for Intrusion Detection in Smart Metering,” in *3rd International Conference on Information Systems Security and Privacy*, 2017.

[37] Q. R. J. S. Li Y, “Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid,” Beihang University, 2018.

[38] P. S. K. F. E. C. a. D. I. Andrés Molina-Markham, “Private memoirs of a smart meter,” in *In Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys '10)*, New York, 2010.

[39] W. Luan, D. Sharp and S. LaRoy, “Data traffic analysis of utility smart metering network,” in *IEEE Power & Energy Society General Meeting*, Vancouver, 2013.

[40] S. Petai, “Detecting Anomalies in System Logs,” Tallinn, 2014.

[41] N. -. adm, “Agent-based versus agentless log collection - which option is best?,” NXLog, 22 October 2019. [Online]. Available: https://nxlog.co/agent-based-versus-agent-less. [Accessed 13 05 21].

[42] C. Z. K. Z. Xiujuan Wang, “Intrusion detection algorithm based on density, cluster centers, and nearest neighbors,” *China Communications,* vol. 13, no. 7, 2016.

[43] R. Vaarandi, “Tools and Techniques for Event Log Analysis,” TALLINN UNIVERSITY OF TECHNOLOGY , Tallinn, 2005.

[44] W. Li, “Automatic Log Analysis using Machine Learning - Awesome Automatic Log Analysis version 2.0,” Uppsala Universitet, 2013.

[45] F. a. M. E. a. P. M. a. J. A. Castiglione, “Quantitative Modelling Approaches. Reference Module in Life Sciences,” in *Encyclopedia of Bioinformatics and Computational Biology*, 2018, pp. 874-883.

[46] “Research project - Qualitative modeling from data,” University of Ljubliana - Faculty of Computer and Information Science, 2009-2012. [Online]. Available: https://www.fri.uni-lj.si/en/projects/26. [Accessed 12 April 2021].

[47] S. V., J. Prasad and R. Samikannu, “Overview, issues and prevention of energy theft in smart grids and virtual power plants in Indian context,” *Energy Policy,* vol. 110, pp. 365-374, 2017.

[48] T. B.Smith, “Electricity theft: a comparative analysis,” *Energy Policy,* vol. 32, no. 18, pp. 2067-2076, 2004.

[49] M. E. R. Y. Y. R. I. a. A. A. G. S. Yussof, “Financial impacts of smart meter security and privacy breach,” in *Proceedings of the 6th International Conference on Information Technology and Multimedia*, 2014.

[50] B. Y. Seyit Ahmet Camtepe, “Formal methods of attack modeling and detection,” in *Modeling and Simulation of Computer Networks and System*, 2015, p. 841–860.

[51] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen and X. Shen, “Energy-Theft Detection Issues for Advanced Metering Infrastructure,” *Tsinghua Science and Technology,* vol. 19, no. 2, pp. 105-120, 2014.

[52] “Multi-vendor penetration testing in the advanced metering infrastructure,” in *ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference*, 2010.

[53] F. Skopik and Z. Ma, “Attack Vectors to Metering Data in Smart Grids under Security Constraint,” in *IEEE 36th International Conference on Computer Software and Applications Workshops*, Izmir, Turkey, 2012.

[54] Wikipedia, “Wikipedia - Denial of service attack,” [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack. [Accessed 17 04 2021].

[55] B. K. a. S. Abla, “Security concerns in smart grids: Threats, vulnerabilities and countermeasure,” in *2015 3rd International Renewable and Sustainable Energy Conference (IRSEC)*, Marrakech, 2015.

[56] T. Z. Q. Z. Y. W. L. P. Ping Yi, “Puppet attack: A denial of service attack in advanced metering infrastructure network,,” *Journal of Network and Computer Applications,* vol. 59, pp. 325-332, 2016.

[57] Tarlogic, “Smart Meters – Threats and Attacks to PRIME Meters,” Tarlogic, 4 November 2019. [Online]. Available: https://www.tarlogic.com/en/blog/smart-meters-threats-and-attacks-to-prime-meters/. [Accessed 01 04 2021].

[58] J. I. M. N. Gregorio López López, “Cybersecurity Vulnerability Analysis of the PLC PRIME Standard,” *Security and Communication Networks,* vol. 2017, 2017.

[59] L. a. Gyr, “Landis and Gyr MAP 120 User manual,” Landis and Gyr , 26 October 2015. [Online]. Available: https://www.landisgyr.eu/webfoo/wp-content/uploads/2013/03/MAP120_UserManual.pdf. [Accessed 4 April 2021].

[60] Landis+Gyr, “Landis+Gyr MAP tools,” [Online]. Available: https://www.landisgyr.eu/product/map/. [Accessed 20 April 2021].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Madis Männik,

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Smart meter cyber threat detection and mitigation”, supervised by Gabor Visky
   1.1. to be reproduced for preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until the expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until the expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

01.04.2021

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Monitoring events collected using .MAP120 software

Category	Name of event
Alarm triggers	Clock invalid
Alarm triggers	Replace battery
Alarm triggers	Program memory error
Alarm triggers	RAM error
Alarm triggers	NV memory error
Alarm triggers	Measurement system error
Alarm triggers	Watchdog timer elapsed
Alarm triggers	Fraud attempt
Alarm triggers	Total power failure
Alarm triggers	Power resumed
Alarm triggers	Missing neutral
Alarm triggers	Phase asymmetry
Alarm triggers	Current reversal
Alarm triggers	Phase sequence incorrect
Alarm triggers	Unexpected consumption
Alarm triggers	Key exchanged
Alarm triggers	Bad voltage quality L1-L3
Alarm triggers	External alarm
Alarm triggers	Local communication attempt
Alarm triggers	Disconnect/reconnect failure
Alarm triggers	Fraud attempt M-Bus device 1-4
Alarm triggers	Communication error M-Bus device 1-4
Alarm triggers	New M-bus device installed channel 1-4
Alarm triggers	Disconnect/reconnect failure
Alarm triggers	Valve alarm M-Bus device 1-4
Power quality event log	Undervoltage L1-L3
Power quality event log	Overvoltage L1-L3
Power quality event log	Missing voltage L1-L3
Power quality event log	Missing neutral
Power quality event log	Phase asymmetry
Power quality event log	Bad voltage quality L1-L3
Power quality event log	Current without voltage L1-L3
Power quality event log	Power factor below threshold
Power quality event log	Power factor normal
Power quality event log	Phase leakage
Power quality event log	Critical overvoltage L1-L3
Power quality event log	Critical undervoltage L1-L3
Power quality event log	Phase asymmetry

Disconnector event log	Disconnector ready for manual reconnection
Disconnector event log	Manual disconnection
Disconnector event log	Manual connection
Disconnector event log	Remote disconnection
Disconnector event log	Remote connection
Disconnector event log	Local disconnection
Disconnector event log	Limiter threshold exceeded
Disconnector event log	Limiter threshold changed
Disconnector event log	Disconnect/reconnect failure
Disconnector event log	Local reconnection
Disconnector event log	Supervision monitor 1-3 threshold exceeded
Disconnector event log	Supervision monitor 1-3 threshold ok
Disconnector event log	Disconnector control state changed
Fraud detection event log	Terminal cover removed
Fraud detection event log	Terminal cover closed
Fraud detection event log	Strong DC field detected
Fraud detection event log	No strong DC field anymore
Fraud detection event log	Meter cover removed
Fraud detection event log	Meter cover closed
Fraud detection event log	Multiple authentication failure
Fraud detection event log	Replay attack
Fraud detection event log	Current reversal
Fraud detection event log	Measurement system checksum error
Standard event log	Power down
Standard event log	Power up
Standard event log	Daylight saving time enabled or disabled
Standard event log	Clock adjusted (old date/time)
Standard event log	Clock adjusted (new date/time)
Standard event log	Clock invalid
Standard event log	Replace battery
Standard event log	Battery voltage low
Standard event log	TOU activated
Standard event log	Error register cleared
Standard event log	Alarm register cleared
Standard event log	Program memory error
Standard event log	RAM error
Standard event log	NV memory error
Standard event log	Watchdog occurred
Standard event log	Measurement system error
Standard event log	Firmware ready for activation
Standard event log	Firmware activated
Standard event log	Passive TOU programmed
Standard event log	External alert detected
Standard event log	One or more parameters changed

Standard event log	Global key(s) changed
Standard event log	Firmware verification failed
Standard event log	Unexpected energy consumption
Standard event log	Local communication attempt
Standard event log	Phase sequence revesal
Standard event log	Asynchronous billing period reset
Standard event log	Synchronous billing period reset
Standard event log	Firmware update limit reached
Standard event log	Extension board error
Standard event log	HAN communication error
Standard event log	HAN communication ok
Standard event log	Remote communication error
Standard event log	Remote communication ok
Standard event log	Profile checksum error
Standard event log	Parameter restoration failed
Standard event log	profile checksum ok
Standard event log	Passive TOU activation failed
Standard event log	Load profile cleared
Standard event log	Event log cleared