Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Eirik Lien
Karl Magnus Grønning Bergh

Attitudes and Perception of AMI Information Security in the Energy Sector of Norway

Master's thesis in Information Security
Supervisor: Dr. Sokratis Katsikas
June 2023

NTNU
Norwegian University of
Science and Technology

Eirik Lien
Karl Magnus Grønning Bergh

Attitudes and Perception of AMI Information Security in the Energy Sector of Norway

Master's thesis in Information Security
Supervisor: Dr. Sokratis Katsikas
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Acknowledgements

This master's thesis represents the culmination of our studies at the Faculty of Information Technology and Electrical Engineering at NTNU Gjøvik. Over the past four years, we have together had the privilege of delving into the complex realm of information security challenges that the world currently faces and will continue to face in the future.

First and foremost, we would like to thank our thesis supervisor, Professor Sokratis Katsikas, who has been an invaluable source of support throughout our journey. He has consistently demonstrated remarkable accessibility, providing us with guidance, advice, and encouragement whenever needed. His mentorship has played a pivotal role in helping us achieve our intended goals. We would also like to convey a special gratitude to Professor Bernhard Hämmerli and PhD candidate Øyvind Toftegård for their contributions in the pre-project phase of our thesis. Their insightful discussions and guidance have been appreciated in shaping our research and enhancing its quality.

We are grateful to our research participants and want to thank them for their commitment, honesty and time. You provided us not only with data, but also valuable insights into the complex world of the energy sector.

A special thank you to all the teaching staff at NTNU Gjøvik for their dedication in imparting knowledge, fostering collaboration, and guiding students through the intricacies of their studies. Their commitment to teaching and their willingness to share their expertise have greatly contributed to our understanding of the subject matter.

And lastly, we want to express our deepest gratitude to our families for their unwavering support and understanding. Their patience, encouragement, and love have been crucial to our success. Without their assistance, we would not have been able to complete this thesis. This acknowledgement serves as a testament to our profound appreciation for everything they have done for us. Monica and Irene, we are forever grateful to you!

Abstract

The digitalization of society in general and critical infrastructure in specific introduces new challenges and attacks surfaces for actors seeking to exploit the cyber domain for political, financial or personal gain. In the energy sector of Norway, the introduction of AMI has contributed to this digitalization, increasing the complexity and requirement for specialized knowledge to protect the infrastructure and the delivery of power. What drives the areas of focus and work in information security is both the regulatory requirements, research efforts and the individual stakeholder's perception of what is important. With different areas of focus and gaps in knowledge, the work of securing AMI can be challenging. Consequently, there is a need to establish the state of information security risk perception amongst stakeholders in the energy sector of Norway to explore the need for alignment of focus and change in perception. This study aims to provide an overview of information security risk perception amongst the stakeholders in the Norwegian energy sector regarding AMI. Moreover, the study will explore the areas of focus amongst scientific academic literature and compare the areas of focus between the literature and the stakeholders of the energy sector. Further, based on the identified differences, the study will propose solutions to reduce these.

In terms of information security, vulnerabilities, threats, likelihood, consequences and assessments of risk in AMI and the differences between the stakeholders' perception and the focus of literature were investigated through exploratory research. Qualitative research designs were employed to carry out the different phases in the study. A systematic literature review was conducted to determine the areas of focus for information security risks in literature. Semi-structured interviews (N=27) were carried out to identify the perception of information security risks amongst the whole chain of stakeholders of AMI in Norway. The collected data from the literature review and the interviews where then compared to identify areas of divergence and further the study explored the need for addressing this divergence through proposed solutions.

The findings indicate that the literature focuses on technical challenges in the distributed elements of AMI, while the stakeholders in general focuses on the system level. The identified literature does not assess the risk in terms of likelihood and consequence, while the stakeholders perceive the overall risk in the different layers of AMI to be low. The stakeholders believe the implemented measures will be able to handle the vulnerabilities and threats. The indications in this study suggests that there may exist a cognitive bias in information security risk perception, incomplete cyber SA and the need for more comprehensive research efforts on the Norwegian implementation. Two solutions are proposed to address these challenges: 1) Increase the research efforts on both strategical and organizational level, and 2) Explore the possibility for establishing a unifying regulatory entity conducting both preapproval of systems and organizations, and supervisions in the field of information security in the energy sector. By applying different methodologies, this study has provided scientific and novel understanding of risk perception amongst stakeholders of AMI in the energy sector of Norway. Further, it has explored the differences that exist between the stakeholders and academic literature in focus areas for risk, together with recommendations for addressing the indicated differences.

Keywords

Advanced Metering Infrastructure
Information security
Consequences
Likelihood
Risk perception
Smart Grid
Threats
Vulnerabilities

Sammendrag

Digitaliseringen av samfunnet som helhet og kritisk infrastruktur spesielt introduserer nye utfordringer og angrepsflater for ondsinnede aktører som utnytter cyberdomenet for politisk, økonomisk eller personlig vinning. I kraftsektoren i Norge har introduksjonen av AMS bidratt til en økt digitalisering, og igjen økt kompleksiteten og behovet for kunnskap og kompetanse for å beskytte infrastrukturen og sikre leveransen av kraft til sluttbrukerne. Arbeidet med og fokusområdene innen informasjonssikkerhet drives fremover av både krav fra myndigheter, forskning i akademia, og den enkelte aktørs oppfattelse av hva som er viktige områder. Ved forskjellig fokusområder og manglende kunnskap innen informasjonssikkerhet vil både den digitale og fysiske sikringen av AMI bli utfordrende. Følgelig er det derfor et behov for å utforske hva som er oppfattelsen av informasjonssikkerhetsmessige risikoer blant interessentene i kraftsektoren i Norge og deres fokusområder i den forstand. Dette vil kunne bidra til å videre utforske behovet for å justere fokus og endre oppfattelsen av risiko ved å sammenligne aktørene og akademia sine fokusområder. Denne studien tar sikte på å gi en oversikt over hva interessentene oppfatter som informasjonssikkerhetmessige risikoer i kraftsektoren i Norge knyttet til AMS. Videre vil studien utforske hvilke områder akademisk litteratur fokuserer på, og sammenligne fokusområdene mellom litteraturen og interessentene i kraftsektoren. Basert på denne sammenligningen og identifiserte forskjeller, vil studien vurdere behovet for og forslå løsninger for å redusere disse.

Med utforskende forskning utdyper studien problemstillingen og forskningsspørsmålene, der kvalitative forskningsdesign ble brukt for å gjennomføre de ulike fasene av studien. En systematisk litteraturstudie ble gjennomført for å identifisere fokusområdene for informasjonssikkerhet og risiko i litteraturen. Semi-strukturerte intervjuer (N=27) ble gjennomført for å identifisere oppfattelsen av informasjonssikkerhetsmessig risiko blant alle interessentene i AMS i Norge. Forskningsutvalget bestod av personer fra forskjellige nivåer innen interessentene som håndterer AMS i ulik grad. Innsamlet data fra litteraturstudien og intervjuer ble analysert og deretter sammenlignet for å identifisere forskjeller i fokusområder. Videre undersøkte studien behovet for å justere fokusområder og oppfattelse av informasjonssikkerhet og risiko gjennom foreslåtte løsninger.

Funnene i denne studien indikerer at fokuset i litteraturen ligger på tekniske utfordringer i den distribuerte delen av AMS, mens interessentene overordnet har fokus på systemnivået. Den identifiserte litteraturen vurderer i all hovedsak ikke risiko i form av sannsynlighet og konsekvens, mens interessentene vurderer den overordnede informasjonssikkerhetsmessige risikoen som lav på alle nivåer i AMS. Interessentene tror at iverksatte tiltak vil kunne håndtere sårbarhetene og truslene i all hovedsak. Videre funn fra denne studien indikerer at det kan eksistere kognitive skjevheter i oppfattelsen av informasjonssikkerhetsmessig risiko, at det er tilfeller av ufullstendig cyber situasjonsforståelse, samt at det er behov for mer helhetlig forskning på den norske implementasjonen. To løsninger foreslås i den forbindelse for å håndtere disse utfordringene: 1) Økning av forskningsinnsatsen på både strategisk og organisasjons nivå, og 2) Utforske muligheten for å etablere en samlende regulatorisk enhet som står for både forhåndsgodkjenning av systemer og organisasjoner, samt tilsyn innen informasjonssikkerhet i kraftsektoren. Ved å benytte forskjellige metoder har denne studien bidratt med vitenskapelig og ny informasjon om risikoforståelse blant interessentene i AMI i kraftsektoren i Norge. Videre har den utforsket forskjellene mellom

interessentenes og litteraturens fokusområder for informasjonssikkerhetsmessig risiko, samt kommet med anbefalinger for å håndtere de indikerte forskjellene.

Nøkkelord

Avansert Måle- og Styringssystem
Informasjonssikkerhet
Konsekvenser
Sannsynlighet
Risikoforståelse
Smart Grid
Trusler
Sårbarheter

Table of contents

List of Figures

List of Tables

Abbreviations

AMS	Avansert Måle- og Styresystem
AMI	Advanced Metering Infrastructure
AML	Adversarial Machine Learning
ANSI	American National Standards Institute
BAN	Business Area Network
CERT	Computer Emergency Response Team
CIA	*Confidentiality, Integrity*, and *Availability*
CIAPI3A	*CIA + Privacy, Identification, Authentication, Authorization, Accountability*
CIS	Consumer Information Systems
CVR	Conservation Voltage Reduction
CNO	Computer Network Operations
CPD	Cyber-Physical Device
CPS	Cyber-Physical System
CSA	Cyber Situational Awareness
CSIRT	Computer Security and Incident Response Teams
DCS	Distributed Control System
DER	Distributed Energy Resource
DMS	Distribution Management System
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Demand Response
DSO	Distribution System Operator
DSSE	Distributed System State Estimation
EDS	Entrepreneur Dispatch System
EPSEM	Extended Protocol Specification for Electronic Metering
FW	FirmWare
GIAC	Global Information Assurance Certification
HW	Hardware
HAN	Home Area Network
HES	Head-End Systems
IAN	Industry Area Network
ICS	Industrial Control System
ICT	Information and Communication Technology
IED	Intelligent End Devices
IDS	Intrusion Detection System
ISAC	Information Sharing and Analysis Center
IoT	Internet of Things
LS	Load Shedding
MBB	Mobile BroadBand
MCU	Main Control Unit
MECH	Mobile Edge Computing Host
MitM	Man-in-the-Middle
MILP	Mixed Integer Linear Programming
MDMS	Meter Data Management System
ML	Machine Learning
NVE	Norges Vassdrags-og Energidirektorat (The Norwegian Water Resources and Energy Directorate)
NIST	National Institute of Standards and Technology
NSD	Norwegian Center for Research Data
OED	Olje- og Energi Departementet
OMS	Outage Management Systems
OLTC	On-Load Tap Changer
PCA	Principal Component Analysis

PII	Personal Identifiable Information
PLC	Power Line Communication
PRA	Probabilistic Risk Assessment
RAN	Radio Access Network
RME	Reguleringsmyndigheten for Energi
SA	Situation Awareness
SCADA	Supervisory Control and Data Acquisition
SEP	Smart Energy Profile
SG	Smart Grid
SLA	Service Level Agreement
SLR	Structured Literature Review
SME	Subject Matter Expert
SSI	Semi-Structured Interview
SW	Software
TSA	Time Synchronization Attack
TSO	Transmission System Operator

1 Introduction

The topics covered by this study are within the field of information security management and concerns perception of risk amongst the different actors within the energy sector of Norway. The study will analyze how the actors perceive information security risks towards the Advanced Metering Infrastructure (AMI) and their attitudes towards the risk picture.

AMI is in short an integrated system enabling smart distribution of electricity to endpoints/end-users[1]. This is facilitated by 2-way communication in near real-time, measuring and collecting the electricity flow and usage data [1, 2]. It consists of Smart Meters (SM), Data Collectors (DC), communication channels, Head-End Systems (HES) and Meter Data Management Systems (MDMS), where the types and level of integration of equipment, network topology, and management systems may vary. A simplified model is visualized in Figure 1.1. This study will conduct research in a Norwegian context, with Norwegian stakeholders[2], where AMI is named the Advanced Measurement and control Systems (AMS)[3]. However, as AMI is an internationally accepted term, it will be used in the sequel.

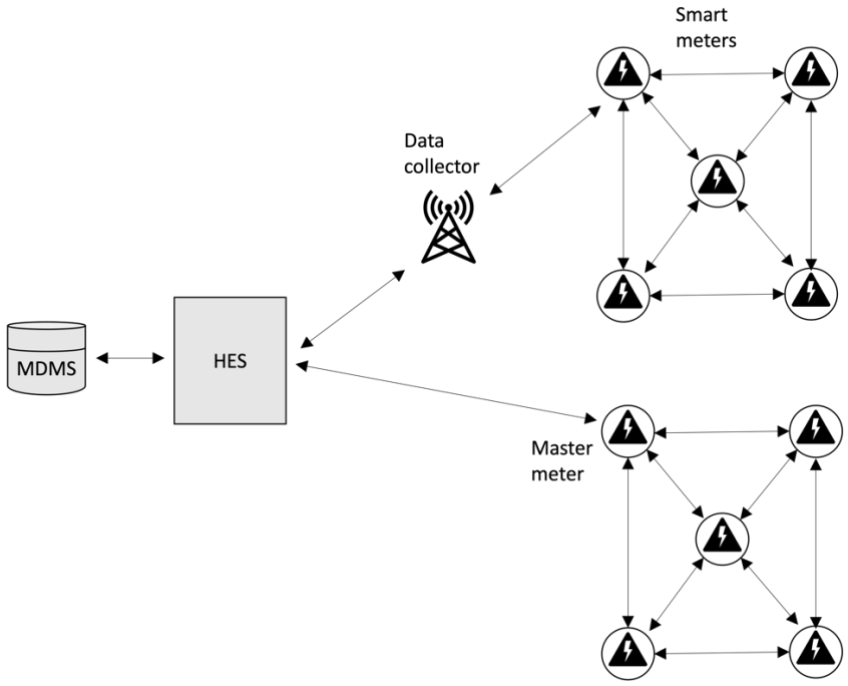


Figure 1.1 AMI simplified network topology, adapted from [1] and [3]

[1] Endpoint is where the AMI is terminated at the consumer side, i.e., the smart meter installed at the customer's premises. End-user is the customer associated with the endpoint.
[2] The research study's definition of a stakeholder in AMI includes energy regulatory authorities, operators of distribution networks, owners or operators of AMI-related equipment and end-users.
[3] Avansert Måle- og Styringssystem – AMS (NO)

In terms of risk and the threat picture for AMI, recent reports from the National Security Authority [4, 5] and the Police Security Service [6, 7] provide an overall picture for critical infrastructure and the energy sector in Norway. Both types of reports convey a warning that Norwegian organizations and infrastructure are already being reconnoitered and mapped out by adversaries, being both state-actors and individuals. In a Cyber Kill Chain@ [8], reconnaissance is the preliminary stage to enable exploitation of the vulnerabilities uncovered in the cyber domain. If the adversaries continue down this chain, it is evident that the vulnerabilities can be exploited as part of cyberattacks with potentially high impacts to the Norwegian society [4]. In reports from 2020 [5, 7], the threats of intelligence operations towards the energy sector[4] are highlighted specifically, where malicious actors in the form of state actors may have the capacity to affect the *Confidentiality, Integrity* and *Availability (CIA)* of the Information and Communication Technology (ICT) systems supporting the sector. As an example, both Russian and Chinese intelligence activities in Norway are mainly related to Computer Network Operations (CNO)[5]. These operations are part of preparations for future conflicts, by reconnoitering and preparing for digital sabotage with the aim of affecting state emergency- and crisis management, the armed forces and societal security services. In a more global context, there are several incidents that show the potential in CNO on critical infrastructure from an alleged state actor, such as Black Energy 3 and Crashoverride. Both hit parts of the Ukrainian electricity grid and caused temporary massive blackouts [9]. These examples serve to show that state actors or other adversaries have both the motivation, resources, and knowledge to exploit vulnerabilities in an interconnected energy sector.

With this as a concerning backdrop, the Office of the Auditor General conducted an audit of the Norwegian Water Resources and Energy Directorate's (NVE[6]) work on ICT security in the power grid in Norway [10]. The findings and conclusions revealed vulnerabilities within the different sectors and how the power companies and the regulatory authorities work with ICT security in general. Based on the above-mentioned reports and their findings, it is evident that both vulnerabilities and threat actors exist, that give rise to substantial risks in the Norwegian energy sector.

Several literature surveys regarding the state of information security within AMI have been undertaken, where the focus often lies within specific infrastructure elements [11-13]. Others have a more holistic approach, where AMI is seen as a system of systems and to a greater extent, reveal the interdependencies within [14-16]. And by looking at both the individual elements and AMI as a system of systems, they all show challenges and risks when it comes to protecting the CIA of ICT systems and data in the energy sector.

The vulnerabilities and threats detailed in the above-mentioned reports and articles can entail severe risks with potential widespread effect within critical infrastructures and the society. With this backdrop, the risk assessments conducted within the energy sector and AMI should be able to encapsulate and provide sufficient controls to the risks entailed. A similar study conducted in Sweden in 2016 [17] shows gaps in knowledge and awareness regarding the interdependencies, vulnerabilities, and threat landscape in Internet-of-

[4] The energy sector in Norway contains all organizations involved in energy- and water resource management, including the power sector.
[5] CNO is a term used for digital sabotage, digital intrusions, cyber intelligence and preparations for such activities [5]
[6] Norges Vassdrags- og Energidirektorat (NO)

Things (IoT) in general and AMI in specific. This can to a certain degree imply that the assessments conducted for and knowledge of such systems are incomplete and deficient.

1.1 Problem description

One of the hallmarks of the modern world is the level of digitalization of the society and the interconnected nature of all elements within. The society has grown dependent on ICT, helped by the digitalization. While contributing to prosperity and value added, the digitalization can also introduce new challenges and increase the attack surfaces. A prominent and relatively new addition to this, is the introduction of the AMI within the energy sector.

The digitalization of the society has happened at a fast pace, and is influencing the ability to maintain a sufficient level of security as stated in [4]. It has made the digital value chain dynamic, complex and challenging to grasp, and introduces new vulnerabilities and interdependencies between organizations. As such, it is challenging to keep track of the vulnerabilities and the risks they entail. The vulnerabilities introduced may be exploited by adversaries with different intentions, motivations, and resources available. And as the society takes advantage of the digitalization, the adversaries will utilize the same advantages to exploit the vulnerabilities.

Within the information security domain, an argument can be made that there is a gap or deviation in knowledge and awareness regarding one's assets, their vulnerabilities and the threat landscape as described in [18]. This is also evident for AMI in the energy sector [14, 17]. If such gaps are not addressed, they may lead stakeholders to introduce security controls and measures that are not grounded in a realistic risk picture or are just inappropriate and irrelevant.

To visualize and highlight potential gaps and deviations, it is necessary to collect and analyze the state of AMI information security and compare it to the perceptions of AMI information security amongst the stakeholders in the energy sector. This study seeks to explore and compare the state of AMI security according to literature with the perceptions and attitudes of the stakeholders regarding information security. The differences that may be found can then aid the stakeholders to achieve an increased level of awareness of the information security challenges that need to be addressed to reduce the risks to the energy sector.

1.2 Justification, motivation and benefits

The vulnerabilities and threats within ICT and IoT may pose a significant threat towards the AMI, as [1, 15, 16, 19] show some of the potential impacts from different attacks exploiting a variety of vulnerabilities. [1] details five possible impacts: (1) Theft of data, (2) Theft of power, (3) Localized denial of power, (4) Widespread denial of power and (5) Disruption of the grid. These impacts can vary in duration but will have detrimental effect on other critical infrastructure and societal functions which all are dependent on a reliable and stable power supply. A concrete example in [1] is the impact a widespread (and successful) bricking attack on SMs could have on end-users: Millions of smart meters in need of replacement at the same time, incurring huge financial cost, lengthy replacement period due to the sheer number of smart meters, which again extends the black-out period for the customers. A timely question to ask is then: How well are the individual user, societal services and other critical infrastructure prepared to deal with extended periods of power outage? The overarching example presented above shows the

importance of taking risk-informed decisions regarding how AMI should be protected, and to implement a sufficient level of protection. If the stakeholders and decision makers have an insufficient understanding of associated risks, the consequence can be the use of resources on controls and measures that are incomplete, insufficient, or lacking overall.

A similar study within this field has been identified in [17], where the focus is on IoT in general as part of critical infrastructure sectors (water, energy, and health monitoring) in Sweden. It has a relatively narrow selection of participants from a limited set of stakeholders in the energy sector, where the participants are divided into categories of strategic, development and operational. To get more fine-grained data, this study seeks to expand the numbers of participants to encapsulate the whole chain in the AMI, from distribution service operators to the customer/end-user, and also include energy regulatory authorities in Norway[7].

The contributions of this study will benefit stakeholders in the Norwegian energy sector conducting risk assessments of information and information systems, by providing a snapshot of the participants' perception of risk and by contributing to enhanced awareness of information security challenges in AMI. This is achieved by highlighting potential divergence between the stakeholders' perceptions and attitudes towards information security risks, and the perceived state as reflected in the scientific literature. By doing this, a future benefit may be a more realistic risk picture and contribution to a more accurate focus of the information security work in AMI.

1.3 Research questions

This study seeks to answer the following problem statement:

What are the attitudes and perceptions of information security risks within AMI in the energy sector of Norway?

To answer the problem statement, a set of more specific research questions (RQs) have been developed:

RQ1: What information security risks are prevalent within AMI according to the literature?

With this question, the study will conduct a Structured Literature Review (SLR) of relevant research to analyze the state of vulnerabilities, threats, and risks to AMI.

RQ2: What information security risks are prevalent within AMI according to stakeholders of AMI in Norway?

With this question, the study will use Semi-Structured Interviews (SSI) to investigate how the different stakeholders perceive information security risks, and what are both current and future enablers and challenges in this regard.

[7] The Norwegian Regulatory Authority (RME) and the Norwegian Water Resources and Energy Directorate (NVE) constitute the main regulatory authorities of the energy sector in Norway.

RQ3: How does the information identified in the literature review compare to the attitudes and perceptions of stakeholders of AMI in the energy sector of Norway?

Based on the findings in RQ 1 and 2, the study will analyze and discuss the potential similarities and differences between the scientific literature and the stakeholders' perception of information security risks in AMI.

RQ4: How can potential divergence between literature and stakeholder perception of information security risks within AMI in Norway be addressed?

This question seeks to identify potential methods for addressing the mismatches between literature and stakeholder perception of information security risks and reducing the divergence.

1.4 Planned contributions

The contribution of the study conducted in this master's thesis will be evidence-based knowledge of the perceptions of information security risks in AMI. In addition, the thesis will contribute with evidence-based knowledge of the divergence in perceived risk between stakeholders of AMI and scientific literature and how this divergence can be addressed.

The study will in this regard contribute to the information security work for stakeholders of AMI. This will be achieved by addressing the security challenges that introduce risks to the development and operation of AMI. By analyzing the perceptions and attitudes of security in AMI and by comparing the findings with the current state of security in AMI according to literature, the study will highlight the potential divergence in awareness and areas of focus. The result from this study may also provide valuable input to energy regulatory authorities, by indicating how information security risks are perceived and understood by their constituents. This can enhance how guidance and regulations are formed and enforced in the sector.

1.5 Thesis structure

The structure of the research study is as follows:

Chapter 2 places the research study in the context of a larger body of work and positions the study in a theoretical structure connected to the master's thesis program.

Chapter 3 outlines and justifies the design and methodology chosen to answer the problem statement and RQs defined in Chapter 1. The research design is described in detail together with the selection process to show an understanding of relevant scientific methodology theories.

Chapter 4 describes the analysis of the results obtained for both SLR and SSI.

Chapter 5 discusses the results and analysis regarding the RQs and puts them into context. Outliers, additional findings, and limitations of the study are also discussed.

Chapter 6 summarizes the study and main findings by answering the RQs. Future research directions based on this study are also proposed.

2 Background and related work

This chapter will put the research study into context with a larger body of work and position the study in a theoretical structure connected to the master thesis' program. It describes human perception and convergence challenges pertinent to the problem statement and the RQs. Further, it describes and defines the most common terms used within information security and gives an overview of the AMI in a Norwegian context.

This chapter will also identify and describe the knowledge available in literature sources that are related to the problem statement and the RQs identified in Section 1.4. By giving an overview of both why/why not and how the literature aids in answering the RQs, the study will also be able to seek out areas where there are gaps in the literature.

2.1 Background and terminology

The master thesis is for both authors a continuation of the NTNU course "IMT 4203 Critical Infrastructure Security" and the survey paper[8] delivered as part of the overall assessment. Further, the thesis builds on the NTNU course "IMT 4205 Research Project Planning" and the project plans[9][10] developed for parts of the methodology and structure of the thesis.

The problem statement and topic of the research study relates to the NTNU's program in information security and to the program track management of information security.

2.1.1 Security in the cyber domain: Information security and cyber security

Information security deals with the protection of the *Confidentiality, Integrity* and *Availability (CIA)* of information and information systems and assets [20]. Security in this term describes the state of being secure and free from harm, and the actions taken to ensure security of someone or something. These three characteristics describe the utility of information and have been seen as the industry standard for IT security since the development of the CPU. The concept of information security has since developed and to encapsulate the development, the following characteristics and processes have been added to create a more robust model: *Privacy, Identification, Authentication, Authorization*, and *Accountability*. These aspects are also referred to as the security objectives of information security and will be used further in the research study when building a framework for comparison of information security risk aspects with the abbreviation *CIAPI3A*.

In terms of security in cyber space, several attempts have been made to put ICT and information security in context with the cyber domain and its continuous evolvement,

[8] . P. Frogner, E. Lien, and K. M. G. Bergh, "Smart energy metering and its infrastructure – A survey on vulnerabilities and information security challenges," Department of Information Security and Communication Technology, Term paper, 2021
[9] E. Lien, "OSINT as a risk assessment method in information security," Department of Information Security and Communication Technology, Project plan, 2021
[10] K. M. G. Bergh, "Employment of cyber warfare tactics towards the total defence concept," Department of Information Security and Communication Technology, Project plan, 2021

and how they relate to cyber security. However, based on accepted standards such as ISO/IEC 27000 series and the definitions therein, information security as a concept can be interpreted as encapsulating both ICT and cyber security [21, 22]. Information security is defined in ISO/IEC 27000:2018 as "preservation of *confidentiality, integrity* and *availability* of information"[23]. Further, ISO/IEC 27032:2012 defines cyber security as "preservation of confidentiality, integrity and availability of information in the cyberspace" [24, p.4]. Based on these definitions, information security revolves around protecting information assets in all domains and technologies, while cyber security is confined to information assets in cyberspace, visualized in Figure 2.1. Security in this regard involves protecting the *confidentiality, integrity* and *availability* of the information assets.

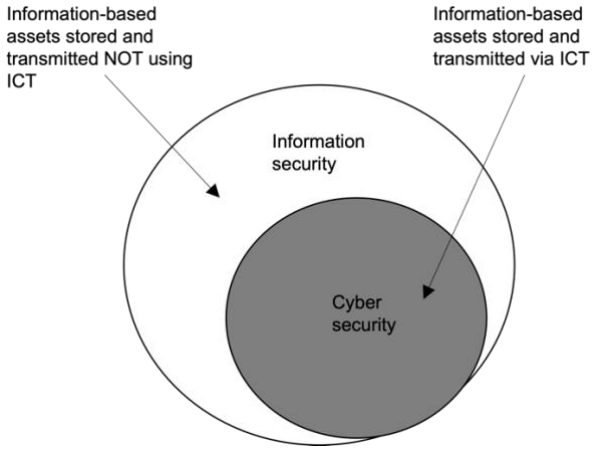


Figure 2.1 Information and cyber security

Both [21] and [22] higlight how concepts are misaligned or suffer from lack of distinction, where information security and cyber security are often seen as equal concepts with little distinction between them. However, cyber security and information security cover different aspects and areas of security, and as such must be used according to what needs to be protected. By juxtaposing the concepts, confusion can arise as to what characteristics, processes and services to use. As described earlier, the concepts possess different aspects and reach, and are to some extent overlapping. In a Norwegian context, there are examples from governmental publications and regulations where terms are used interchangeably, such as "cyber security", "ICT security" and "digital security" in the National Cyber Security Strategy for Norway [25].

2.1.2 Information and cyber security terminology

In this section, the most common term used within the study are defined. As described above, terms within information and cyber security can have different definitions depending on the context and use. Most definitions are adapted from the International Organization for Standardization (ISO) Online Browsing Platform's Terms & Definitions[11], the International Electrotechnical Commission (IEC) Electropedia[12], and the National Institute of Standards and Technology (NIST) Computer Security Resource Center's glossary[13]. All these platforms produce compilations of definitions from their respective information and cyber security publications and standards.

[11] https://www.iso.org/obp/ui#home
[12] https://www.electropedia.org/
[13] https://csrc.nist.gov/glossary

Accountability is a property of information and information systems that ensures that the actions of users, devices or processes can be attributed to the unique user, device or process responsible for the action [20]. In information systems, accountability can be provided by several means, such as by different logs tracking the activity of users, devices, and processes in the system.

Authentication concerns the verification of an entity's identity (e.g., user, process or device), often expedient prior to granting access to resources in an information system [23, 26]. This can be achieved using different means, such as cryptographic certificates, passwords, or Hardware (HW) tokens (e.g., one-time key generator).

Authorization is a process following *identification* and *authentication*, and defines what users, devices or process have been explicitly authorized to do [20]. In the context of information and information systems, this can involve being authorized to access or modify information and information assets.

Availability is the property of information and information systems whereby access to information, data or systems have been ensured in a timely and reliable manner to an authorized entity [23, 26]. In AMI, this objective is set to ensure a timely and reliable access to the data/information, services and power delivery enabled by AMI.

Confidentiality of information or information systems is defined as restricting the access only to entities (e.g., user, process or device) that are authorized, and preventing unauthorized access [23]. This can be achieved through different means, e.g., encryption, classification of information and information systems, implementation of security policies and secure information and data storages. It is considered one of the key security objectives in information security, together with integrity and availability. In AMI, this objective can be described as allowing access to AMI information and data only to authorized entities, such as the customer at the endpoint, the Distribution System Operator (DSO) or the AMI operator.

Consequence is the *impact* of an incident, both direct and indirect on objects and objectives [23]. In nature, it can be certain or uncertain, but intended unwanted incidents (e.g., a cyberattack) do not have to be successfully completed to create consequences, as mitigated incidents may also have consequences.

Cyberattack is an attack via cyberspace on an organization's information and/or physical systems and networks connected to cyberspace. The aim is to exfiltrate, control, disrupt, destruct or degrade of the systems' resources or the information and data residing within [27]. A cyberattack can be considered a precursor of a cyber incident, and a single attack can lead to several incidents.

Cyber-Physical Systems (CPS) in short are interacting networks that integrates sensing, actuation, and computation in connected devices. The computation aspects involve data transfer and processing with IT, while sensing and actuation involves sensing and actuation with Operational Technology (OT) in the physical world. The integration of the IT and OT related aspects, coupled with specific timing constraints for both, are considered the defining features of CPS [28]. In the context of the Smart Grid (SG), AMI itself can be seen as a CPS, and also a part of the CPS that constitutes the SG, thus being part of a cyber-physical system of systems [29].

Cyberspace can be seen as a compounded and global domain, which originates "from the interactions of people, software (SW) and services on the Internet by means of

technology devices and networks connected to it, which does not exist in any physical form"[24, p.4]. Internet is further defined as globally interconnected networks of information systems infrastructures, residing in the public domain [24, p.5]. However, the term *cyberspace* can also be used for networked information systems not necessarily directly linked to internet.

Cyber-threat applies as a definition to any situation or event that can negatively impact organizations, their operations or assets, individuals, the Nation state, or other organizations through an information system by breaching the *confidentiality, integrity* and *availability* of information systems and information within these systems [26]. A threat can be ambiguous in nature and concerns the potential for an unwanted intended impact if the threat is realized. As such it differs from cyberattacks and cyber incidents, which are actions that have already manifested themselves as impacts.

Exposure is a measure of the extent that an asset, individual or organization is exposed to a risk [30]. It is also related to the concept of predisposing condition, where a specific condition within an organization, information system or process can increase or decrease the likelihood of adverse impacts if threats are successfully initiated. An example is a stand-alone information system with no external network connections, where the isolation itself of the network decreases the likelihood of exposure for specific threats, such as network-based cyberattacks. Another example is vulnerabilities based on predisposing conditions, such as the use of outdated technologies in communication networks. These vulnerabilities will create a predisposition toward threats resulting in negative impacts [27].

Identification is a prerequisite for authentication and authorization and concerns the ability of an information system to recognize individual users, devices or processes from a collection of similar users, devices or processes [20]. It is considered one of several minimum security requirements for information and information systems, as described in [26].

Incident is an unexpected or abnormal occurrence, situation or condition at any given time of a system, product, service, or project [31]. An incident can be either intended or unintended and cause both positive and negative impacts. An incident is also referred to as an event [30]. In cyberspace, an incident affects or potentially affects the *confidentiality, integrity* or *availability* of information systems or information processed, stored and transmitted within the systems [26].

Information is defined as an occurrence of an information type, such as communication or representation of knowledge in the form of facts, opinions, processes or data, independent of medium [27].

Information security risk is the risk to "organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation" [27, p.B-6] due to the breach of *confidentiality, integrity* and/or *availability* of information systems and/or information.

Information security risk management refers to the process of coordinated actions and activities to form and control an entity with regard to risk to information and/or information systems it controls [23]. The entity can be the organization, specific parts of the organization (section, a service, or a specific location), information system, or control-mechanisms (existing or planned).

Integrity is considered a property of information and information systems whereby information, data or systems have been guarded against unauthorized and improper modification or destruction. This term includes ensuring non-repudiation and authenticity [26]. In AMI, this objective shall assure that data/information and its source has not been tampered with.

Likelihood of occurrence is an element in the equation of calculating or defining risk, and is a subjective estimate of the probability of a threat's capability to exploit a specific vulnerability or several vulnerabilities arising in an asset [27].

Non-repudiation is a characteristic concerning the ability to assure the occurrence of a specific action or event and its involved entities [23]. In general, it provides the means to determine whether a specific entity was involved in a specific activity such as processing, storing, or transmitting information.

Privacy of individuals in information security is the assurance that information is only used in ways authorized by the provider of the information [20, p.8]. This entails that the *confidentiality* of and the access to information is protected and can be seen as a measure of the provider's trust on the security of the information.

Risk is defined as a measure of to what degree an asset or entity is threatened by an incident or event. A method for calculating risk is to use a function of (1) *impacts* arising from if the *incident* or event takes place, and (2) the *likelihood* of occurrence [27]. However, risk will have both subjective and objective components, as described in [32]. The subjective risk components consist of the individual's own estimate of risk, i.e., their perceptions of risk. This may diverge from objective risk, which is risk that exists independently of the individual's personal beliefs, i.e. a statistical expectation value of the severity of the results [33].

Vulnerability is defined as "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [23, p.11] and [27, p.B-13].

2.1.3 Integration of IT/OT

In this section, the effects of integration of IT/OT are briefly described, as these effects have a growing influence in the energy sector and AMI due to increased interconnectedness of IT and OT.

Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), are often referred to as Operational Technology (OT). These systems are used to monitor and control critical infrastructures such as energy, oil and gas pipelines, water distribution, sewage systems and production control [34]. Traditionally, the OT systems have had a degree of physical separation from IT infrastructures. However, with changing technologies and a drive towards data-driven and remote operations, the two technological environments are becoming integrated, as visualized in Figure 2.2. With this integration, the previously standalone, secured, and isolated environment of OT is now being connected to, and to a certain extent accessible via different systems. With this interconnection, different cyber security challenges are introduced (e.g., malware exploiting vulnerabilities and dependencies), i.e., challenges that are typically associated with IT infrastructures can

now affect traditional OT systems and their cyber resilience[14] capability. An overarching benefit of such an interconnection is the data flows between the systems, making OT and its data available and accessible from the IT environment. The data flows can include critical information such as frequency, voltage, temperatures, proximity levels, control signals and other sensor signals. However, due to the aforementioned integration, OT data and associated control mechanisms are now increasingly exposed and vulnerable to cyberattacks, exploiting assets and their vulnerabilities in OT systems by traversing from or exploiting the IT systems [36].

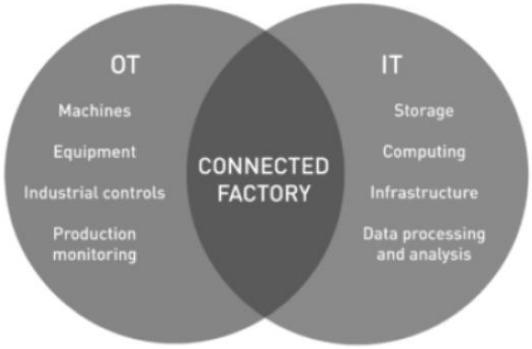


Figure 2.2 Integration of OT and IT, reprint from [37]

Examples of known attacks in the OT environment is the Stuxnet, Black Energy 3 and Crashoverride, where malware propagated from the IT environment and into ICS. The malware had specific physical impacts on the targeted systems and other dependent systems, such as other critical societal systems in the case of Black Energy 3 and Crashoverride. The effects were often limited in time and reach, but clearly show some of the potential of attacks on OT systems.

The consequence and risks by the aforementioned integration can be challenging to comprehend and predict, due to OT consisting of largely legacy systems which to a certain extent are insufficiently documented [36]. In addition, they often use proprietary protocols and have limited resources, making the further development or implementation of new functionality challenging. As such, the consequence and risks introduced by integrating OT and IT can manifest themselves as new vulnerabilities and threats, creating unknown or unpredictable impacts.

In the context of AMI, the effects of the integration are also evident when ICS are integrated and interconnected in the SG with the AMI. The benefits, such as a higher degree of controllability and optimization of the grid, needs to be compared to the downfalls this integration entails, such as increased complexity, new vulnerabilities, and exposure to threats.

[14] Cyber resilience is defined as the ability of systems using, or enabled by, the cyber domain, to withstand, recover and adapt to damage or disruption from attacks, adverse conditions or compromises [35].

2.1.4 Advanced Metering Infrastructure

The overarching goal of this study is to assess the perception of information security risks to AMI and compare it to the risks identified in the literature. To scope the area of focus, the study will identify an AMI reference model for the Norwegian implementation in this section. To give the necessary input to this implementation, a generic description of AMI and its components is given in the following paragraphs.

The development of AMI has been enabled by the technological advancements in the society, but also driven by economical and regulatory incentives, e.g., to ensure cost-efficiency in terms of controlling the grid and implementing new services. Today, AMI is an integrated system of systems, consisting of SMs, communication networks, and management systems. The setup enables near real-time data exchanges between the service endpoints and DSOs. The data exchanged towards the DSOs can be used to detect power outages, measure frequency and voltage, and conduct load-balancing. At the endpoints, the data flow enables the customers to take a more active role in the grid, by the provision of consumption data, automatic billing, and to more easily become a Distributed Energy Resource (DER)[15] [1]. This interaction aids in streamlining the distribution of electricity and is a major component of the SG system.

The main components of AMI are communication channels, smart meters, connected end-user electronics (denoted as Intelligent End Devices - IED), data collectors (also denoted as concentrators), HES and MDMS. The communication channels connect the other components together through various protocols and with different topology and can be both wired and wireless. AMI consists not of a single technology, but as the name implies, integrate different several technologies into a configured infrastructure. The different technologies create a complex system of systems, whose components are interconnected and mutually dependent on each other for safe and reliable operations. The nature of the components of AMI and the networks between them causes interaction between both physical and cyber elements, making AMI a CPS in the SG.

Smart meters are cyber-physical devices in the form of electronic electricity meters. The main functionality can include real-time measuring and reporting of power consumption and quality (frequency and voltage), remote connection and disconnection of electricity at endpoints, and time-based load control. A SM consists of a metrology unit measuring the power consumption. The data are transferred to the Main Control Unit (MCU, also called meter terminal), which processes the data before transmission to HES through the communication module (placed within the MCU, along with the master circuit switch). The meter itself may consists of several interfaces, such as the Home Area Network (HAN), auxiliary meters (e.g., gas and water), and towards other controlled units for local control of individual devices. The SM is visualized in Figure 2.3. Configuration, operation and management of the different functions and the meters themselves can be conducted remotely, and the data from the devices can be collected based on schedules or on demand [1, 38]. A smart meter typically has two communication flows: One towards the head-end of AMI (the DSO) and another to the internal networks of the endpoints (denoted as Home, Business, or Industry Area

[15] A DER is a small-scale electricity supply or demand resource connected to the electric grid. They can consist of micro-turbines, small windfarms, solar panels or battery storage units, located at enterprises or at private properties. The common denominator is that all DERs need to be controlled by the local DSO, directing their operations similar to regular power plants.

Network: HAN, BAN or IAN). The HAN/BAN/IAN can provide interoperability with consumer or industry devices (such as IoT and IIoT), enabling functionalities such as a graphical user-interface for consumption data and Load Shedding (LS)[16]. With an increase in DERs with fluctuating production (e.g., solar panels and windmills in microgrids), combined with different energy storage solutions, the DSOs need the ability to exchange data with the endpoints to control the flow of power in the grid. The prevalence of SMs make them a natural hub of the DERs to ensure the data flow between the devices and the HES.

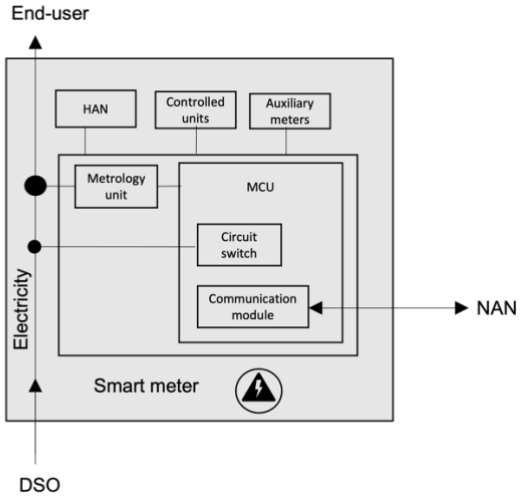


Figure 2.3 Schematics of a generic SM

The communication network enables the flow of data between the different functions and components of AMI. The architecture of AMI is highly flexible and can accommodate a wide range of communication technologies. In [39], Kabalci describes the communication within the SG and AMI in great detail and how the choice of technology is based on different inherent properties between both wired and wireless communication. A simplified description of the architecture is that Wide-Area Networks (WAN) connect the HES to a set of gateways in the grid, where the gateways are connected through Neighborhood Area Networks (NAN) to smart meters at the endpoint. Locally at the endpoint, consumer devices can be connected to the smart meters through HAN, BAN, or IAN[17]. In a Norwegian context, the smart meters and DCs are often connected in NANs through radio mesh networks, and through Mobile BroadBand (MBB) to HES at the DSO or AMI operator. Another configuration is the use of master meters as collectors in a NAN, which are connected directly to HES through MBB [2, 40-42]. The main networks of AMI (HAN, NAN and WAN) are often used to divide the AMI into three different areas or tiers [43], where each tier utilizes different communication technologies to connect the components within to the rest of the AMI.

Data collectors are the gateways in the communication channels, connecting the SMs to HES, enabling the flow of data. The role of the collectors is visualized in Figure 1.1, where a mesh network with both a master meter and a DC act as gateways. In a

[16] LS is a function that enables the DSO to reduce the load on the grid by remotely disconnecting non-essential loads at the endpoint. This is done to balance the load in the grid in high-load scenarios.

[17] Common standards used for wireless sensor networks are EN-13757 (SM-DC) and IEEE 802.15.4 (low data-rate, basis for ZigBee and WirelessHART, used in HAN and NAN) [3]

Norwegian context, not all DSOs use DCs, but instead master meters or individual meters with SIM-modules are installed [2].

HES and MDMS are found at the DSO or AMI operator. The HES is the front-end system of AMI at the DSO and serves as the interface between AMI data and the backend systems. From HES, the data is transferred to the backend and a multi-modular structure consisting of several different systems. In this structure, the MDMS functions as the central module where other backend applications and systems fetch relevant data from [44]. These systems and applications are set up to automate several functions such as billing and reactions to shifts or emergencies in the gird (e.g. Consumer Information Systems (CIS), Outage Management Systems (OMS), Distribution Management System (DMS) and Entrepreneur Dispatch System (EDS)) [2]. Both HES and MDMS are situated inside the DSO or AMI operator's premises.

In a Norwegian context, the DSOs have different approaches as to how the backend is operated. The larger DSOs often opt for running the backend inhouse, while small and medium sized providers can use a combination of inhouse and 3rd party service providers [2]. Mohassel et. al. in [44] point out that regardless of the design of the backend and what services and applications are integrated, it has to address three important demands: (1) "improvement and optimization of operation of utility grids", (2) "improvement and optimization of utility management" and (3) "enabling customer engagement" [44].

AMI as a part of the SG is facilitating the necessary communication architecture for SG. AMI can be considered the enabling factor for SG communication at the consumer endpoints and outwards to the DSOs. NIST has described a conceptual model of the SG with seven logical domains in [45], where each domain contains both actors and applications. AMI is here seen as an application (a task performed by one or more actors in the different domains) and is used to communicate between the domains of customer, distribution, operations, market and service provider. This model is however only intended as a framework for discussing the current grid architecture and the evolving SG, but it shows the position of AMI in the SG and how it can contribute to an efficient, safe and reliable grid by enabling near real-time 2-way communications between domains. Figure 2.4 shows the different domains and the flows of communications and electricity.

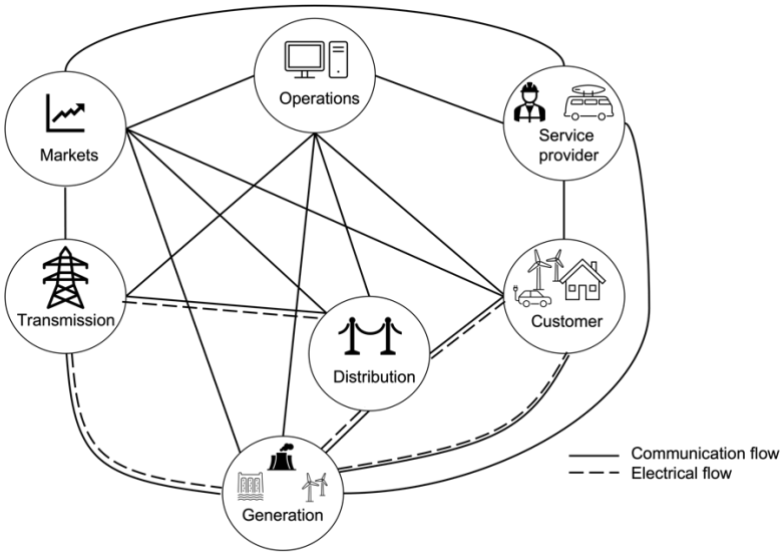


Figure 2.4 SG architecture conceptual model, reprint from [45]

The AMI reference model, visualized in Figure 2.5, is based on a review of literature on the different elements described in the previous paragraphs [1, 2, 38, 39, 44, 45] and architecture descriptions of Norwegian grid operators found in reports from NVE and SINTEF [2, 40-42]. This model visualizes the scope of the study, which will focus on information security risks from the interfaces at the SM up to and including the MDMS at the DSO. The end-user or customer domain from the HAN-port is thus considered out of scope.

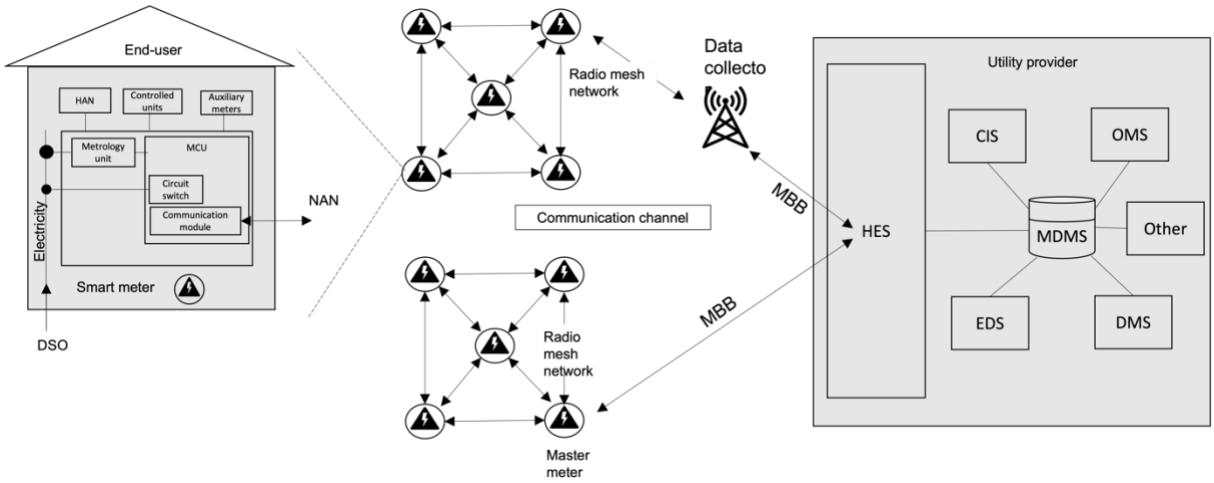


Figure 2.5 AMI architecture reference model, adapted from [2, 40-42]

2.2 AMI in Norway[18]

As described previously in this chapter, the main purpose of introducing AMI is to streamline the distribution of electricity by using ICT to automate meter reading and management functions. To provide insight in the Norwegian implementation of AMI, the following sections will elaborate on a high level how the Norwegian power system is structured, based on the distribution of roles and responsibilities enacted by the Energy Act of Norway [46]. This structure consists of several stakeholders in production, transmission and distribution, where the most relevant entities and their interrelations are presented.

The ministry level consists of the Ministry of Petroleum and Energy (OED)[19], which holds the overall responsibility for the electrical power system. Their main task is to coordinate and integrate the energy policy in a cross-sectoral manner to ensure a coordinated and holistic approach to energy generation, distribution and use in Norway.

The regulatory authority consists mainly of NVE and holds the responsibility for managing the water and energy resources in Norway. They are subject to OED and is the national regulatory authority on electrical energy, responsible for auditing and supervision of compliance with legislation and regulations. Further, NVE is responsible for national contingency planning and preparation in the energy sector, for both emergencies and crisis. The Regulatory Authority for Energy (RME)[20] is a separate department within NVE, which is delegated the responsibility for ensuring compliance with regulations and legislation assuring equal terms of competition in the market for electrical energy and an efficiently and securely operated power grid. Further, the Norwegian Directorate for Civil

[18] In Norway, AMI is denoted as AMS (Avansert Måle- og Styresystem (NO)).
[19] Olje- og Energidepartementet (NO).
[20] Reguleringsmyndigheten for Energi (NO).

Protection (DSB)[21], the Data Protection Agency[22], the Norwegian Metrology Service[23] and National Security Authority (NSM)[24] are other regulatory authorities with responsibilities within the energy sector and other critical societal functions.

The end-user is the customer which consumes the electrical energy delivered through the distribution network. This may also be seen as the outer perimeter of the distribution network, where an electricity SM is connected and measures, registers and reports the energy consumed by the end-user.

Electrical power producers are engaged with production of the electrical energy which is sold in the electrical power exchange. In a Norwegian context, there are several large producers, with Statkraft being the largest producer in terms of yearly production in TWh.

The Transmission System Operator (TSO) has the main responsibility for transmission security by coordinating the production and consumption of electrical energy, ensuring load balancing in the power system. In Norway, Statnett is the system operator, and is subject to OED. Statnett is also responsible for operating and developing the transmission grid in accordance with societal requirements.

The DSOs (also called utility companies) are responsible for the operation and maintenance of the distribution and regional electricity network in their specific area of operation. The distribution network is the last mile in the electricity network, connecting the end-users to the power network and transferring electrical energy, thus giving the DSOs regional monopoly in the distribution network. Regarding AMI, it is the DSOs which are responsible for collecting metering and settlement data and for the operation of AMI.

The power suppliers purchase electrical energy via the markets provided by the power exchanges, or they act as both electrical power producers and power suppliers. The power produced or purchased is then sold to the end-users, and delivered to them through the DSOs that the different end-users are connected to. To ensure equal terms for all power suppliers and DSOs, the Energy Act obliges the DSOs to deliver electrical energy to the end-users regardless of who is the power supplier. It also ensures that end-users can purchase electrical energy from any power supplier.

The power exchanges are international marketplaces which facilitate the purchase and sale of electrical energy, and aid in reconciling the market with supply and demand [47]. In Norway there are two licensed power exchanges, NordPool AS and EPEX SPOT, which handle the physical trade of electrical energy, in addition to the services required to support such activity. Their main tasks are to run the Day-ahead and Intraday trade, where the Day-ahead market sets the price and production for the following day on an hourly basis. This price is based on the production and transmission capacity in the grid, and the purchase and sales bids delivered to the market. The Intraday market is facilitating energy trading within one hour prior to the delivery of the energy. This ensures the possibility for various stakeholders to be in balance energy-wise if the actual production or consumption is different than what was estimated in the Day-ahead market.

[21] Direktoratet for Samfunnssikkerhet og Beredskap (NO)
[22] Datatilsynet (NO)
[23] Justervesenet (NO)
[24] Nasjonal SikkerhetsMyndighet (NO)

Elhub is a centralized IT-system which acts as a data hub for measurement data and customer information connected to settlements, invoicing and change of suppliers in the Norwegian electricity market [48, 49]. Together with AMI and the SM it ensures a purely digital chain in the market, with a secure and efficient handling of customer information and measurement data from the SM. In addition, Elhub performs the calculation and distribution of settlement basis, based on the measurement data received. The different DSOs are responsible for transferring measurement data with a quality assurance to Elhub, where the data is processed and made available for the stakeholders in Elhub (e.g., power suppliers, third parties (after consent from the end-user), and the end-users themselves). This method ensures a common hub for relevant data from AMI for the different stakeholders, providing an efficient and neutral exchange of measurement data and customer information.

The power supply's contingency organization (KBO)[25] is the primary structure for the coordination and management of the Norwegian power supply domain. It consists of all units that operate or own facilities with significant importance for the operation of the Norwegian power supply domain and is led by NVE. Based on the relevant regulations[26], all KBO-units are obliged to ensure a sufficient level of security, an updated contingency plan based on their type of operations, and to implement necessary actions to prevent, mitigate and handle the impacts from extraordinary situations [51]. As an organization, KBO's main task is to implement a structure that provides all relevant stakeholders in the Norwegian power supply domain with both responsibilities and tasks in times of crisis and emergencies.

2.2.1 Requirements for AMI in Norway

The implementation of AMI and SMs was mandated by the Regulation on Measurement, Settlement, Invoicing of Network Services and Electrical Energy (Regulation on Settlements) in 2011[27], where all measuring points (endpoints in the AMI network) were required to have a SM installed. The regulation sets requirements both for functionality and security in AMI, which are complemented by other regulations and guidelines. In terms of regulations relevant for AMI security, Sæle et al. in [53] identified the following regulations: the Power Contingency Act, the Regulation on Settlements, the Personal Data Act[28] and the Electricity Meter Regulation[29]. The identified regulations set different and overlapping requirements, and the following sections will present the requirements, focusing on the ICT and information security-related requirements.

2.2.1.1 Regulation on Settlements

The functional requirements are based on two main functionalities: measuring functionality and control functionality. The control functionality enables the DSO to issue commands, configure and remotely control the supply of electricity at the end-users. The measuring functionality contains all elements enabling measurement of several

[25] Kraftforsyningens Beredskapsorganisasjon (NO)
[26] Units which are part of KBO are obliged to follow provisions regarding contingency and security found in the Energy Act (Energiloven (NO), (ch 9)), the Power Contingency Regulation (Kraftberedskapsforskriften (NO)) §§ 3-5c and 5-3c, the Power Rationing Regulation (Kraftrasjoneringsforskriften (NO)) and the National Security Act (Sikkerhetsloven (NO)) [50].
[27] Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.(Avregningsforskriften) (NO) [52].
[28] Personopplysningsloven (NO) [54]
[29] Forskrift om krav til elektrisitetsmålere (NO) [55]

parameters in the grid and the transfer of such data to the DSO through the communication infrastructure. In terms of ICT-related functional requirements, it states that AMI shall provide:

- Local storage of data, where the SM shall register and store measured values with a maximum frequency of 60 minutes, and minimum of 15 minutes. The SM shall store the data until they are transferred to the DSO. In addition, the SM shall be able to register the flow of active and reactive power in both directions.
- Standardized interfaces, which facilitate communication based on open standards with external equipment (e.g., units displaying consumption and electricity pricing).
- Inter-SM communication, where each SM shall be able to connect and communicate with other types of SMs, including the transfer of data.
- The ability to break and limit the power output at the measuring point (SM) by control functionality and signaling.

In terms of information security requirements, the regulation states specifically that the responsibility for securing the AMI (both physically and logically) lies with the DSOs. Further, all solutions regarding security in AMI must meet the requirements to information systems in the Power Contingency Regulation. Requirements related to information security in the Regulation on Settlements can be summarized in the following bullets, which are derived from §4-6:

- Authorization, where equipment and users that intend to communicate to or within AMI, must be preapproved and authorized by the DSO prior to be granted access. At the measuring point with the end-user, the access to the SM's interface is restricted to the end-user, the DSO and authorized third parties. At other measuring points within the AMI, the access is restricted to the DSO and authorized third parties. An overarching requirement for the connection of new equipment and users to AMI is that the level of security must at least be maintained or enhanced.
- Accountability, where all changes in SW and configuration in AMI must be traceable to the specific user, the time and what changes were performed.
- Confidentiality, where all communication in AMI between the SM and the HES/MDMS must be protected with end-to-end encryption. However, this requirement can be waivered if the communication channel uses a separate network closed for unauthorized entities.
- Authentication and integrity, where all SW-updates, patches and new SW in AMI need to be authenticated by the DSO or their provider prior to installation.
- Resiliency, where AMI must always be able to function as intended. The compromise of a SM and/or its communication with HES/MDMS shall not compromise other SMs, their communication with HES/MDMS or the HES/MDMS itself.

2.2.1.2 The Power Contingency Regulation

All units in KBO are subject to the Power Contingency Regulation, that provides guidance for prevention, incident handling and mitigation of extraordinary incidents which can cause harm or stop the production, transmission, distribution and turnover of electrical power or district heating [56]. The regulation does not set specific requirements, but overarching intentions, to be more adapted to changes in technology, emerging threats and the organization of the power sector and the companies.

Regarding information security, chapter 6 in the regulation details requirements to protect information and information systems. There are several paragraphs relevant to AMI and information security, as identified by Sæle et al. [53]; these are summarized below, based on this work:

- §6-2 Sensitive power information: Specific and detailed information concerning the power supply that can be used to damage facilities, systems or by other means affect functions relevant to the power supply are deemed as sensitive power information. This type of information is subject to duty of confidentiality as stated in the Energy Act §9-3. Sensitive power information includes:
    - All systems handling functions related to operational control systems.
    - Detailed information concerning the power system and infrastructure, such as one-line wiring diagram, and classified substations with wiring diagrams.
    - Descriptive overview of the distribution power networks to critical societal functions.
    - Mapping of earth-bound cabling and pipe networks.
    - Preemptive security measures and contingency plans against intended sabotage and damage.
    - Location of reserve operating centers and other contingency centers.
    - Detailed assessments of vulnerabilities which can be used for intended sabotage and damage.
    - Overall overview of backup solutions, spare material or maintenance contingency of importance for handling intended sabotage or damage.
- §6-8 Back-up: Organizations are required to have updated back-ups of critical information, SW and configurations of operational control systems relevant for operation, security and recovery of the power supply. Copies of the back-up must be stored remotely in a secure location, but with ease of access for the organization. In addition to operational control systems, this paragraph is relevant to securing the operation of AMI.
- §6-9 Digital information systems: This paragraph concerns the protection of confidentiality, integrity and availability of digital information systems, which by implication also includes AMI. An overarching principle stated here is that all organizations must have a level of basic security founded on accepted standards, where the following aspects are covered:
    - The requirement to be able to identify and document assets, services, values and users in their digital information systems.
    - The requirement to conduct risk assessments and to keep them updated.
    - To ensure resiliency of their digital information systems by securing the systems and being able to protect, detect and mitigate unwanted incidents.
    - Contingency, where the organizations are required to handle unwanted incidents in their systems and recover to normal operation without undue delay.
    - Outsourcing, where the level of security must be maintained or improved if organizations are outsourcing services to third parties.
    - Security audit, where the organizations are required to conduct regular audits of the implemented security measures for their digital information systems. Authorized
- §6-10 Breaker functionality in AMI: As all SMs in Norway are required to have breaker functionality implemented, the DSOs are required to protect the

functionality against unauthorized access and use. They are required to implement separate security measures for the breaker functionality, including:

- Remote control, where only the DSOs are authorized to perform remote control from access-controlled zones. Vendors with remote access to the breaker functionality must be contained to EFTA, EU or NATO countries, but where exemptions can be made based on country-specific risk assessments and ongoing supervision from the DSO.
- The implementation of appropriate control schemes, where the DSOs are required to implement schemes for the breaker and update functionality, preventing single entities from being able to perform mass disconnection of SMs in a single event.
- Remote updating of SW, where all remote updating of entities in AMI are required to take place from an access-controlled zone.
- Individual security measures of each SM regarding breaker and update functionality, ensuring that incidents compromising a single SM do not compromise the security of other SMs.

2.2.1.3 The Personal Data Act

All organizations in Norway which conduct non-automated and automated handling of Personal Identifiable Information (PII) are subject to the Personal Data Act. It contains both national regulations specific to Norway and the EU General Data Protection Regulation (GDPR), where GDPR has precedence in cases of dispute.

In terms of AMI and PII, the power consumption information is connected to a SM serial number at a unique address, which again can be connected to a specific homeowner. This implies that power consumption information can be regarded as PII, and thus is subject to the Personal Data Act [57]. This restricts the power suppliers and DSOs in how and when they can use such data, as they can only use the PII necessary for invoicing of the customer and cannot store customer-related data for more than 3 years. In all other matters, the customer has the sole rights of their own data and who should have access to it. By complying with the Act, the DSOs will have to provide a sufficient level of information security to ensure that PII information is only used for authorized purposes, and not misused or lost.

Sæle et al. [53] identified article 32 in terms of information security, as it concerns the security when handling PII. The article states the responsibilities of the data controller and data processor[30] to provide suitable technical and organizational measures to achieve a sufficient level of security with regard to the risk of a breach. This includes, based on suitability:

- Pseudonymization and encryption of PII.
- Ensuring persistent confidentiality, integrity, availability and robustness in information systems and services handling PII.
- Recovery of availability and access to PII in due time after an unwanted incident.
- A process for consistent testing, analysis and assessment of the effectiveness of the implemented technical and organizational security measures.

[30] DSOs can act as both the data controller and data processor, with the exception when they use third party providers to handle PII. The third-party providers are then considered data processors.

In matters concerning the Personal Data Act and PII, it is the Data Protection Authority who acts as both the supervisor and ombudsman, supervising compliance with the privacy regulations [58].

2.2.1.4 The Electricity Meter Regulation

The Electricity Meter regulation put forward requirements for both new and operational electricity meters, and mainly concerns metrology requirements, ensuring that the correct measurement is used. The Norwegian Metrology Service is the supervising authority for the regulation, and it conducts regular supervisions of electricity meters in operation at different DSOs.

In an information security context, § 19 concerns protection against manipulation and deals with security requirements for both HW, SW and connected equipment:

- HW and SW with decisive impact on the metrological properties must be designed so that they can be secured. The implemented security must enable detection of tampering and intervention in both.
- Locally or remotely connected equipment must not impact the metrological properties, e.g., causing erroneous behaviour.
- Data and SW with decisive impact on the metrological properties, and metrological parameters which are stored or transferred, must be protected against both intended and unintended effects.
- The total power consumption which forms the basis for invoicing must not be possible to reset during use of the electricity meter.

To protect the metrological properties, both HW, SW, data and external connections must be secured from both intended and unintended effects, both physically and logically.

2.3 Information security in AMI

The motivation for information security in AMI is closely hinged with the development in the society in general, where the increased use of ICT systems and the connections between the systems increases the attack surface. As the society is growing more and more dependent on ICT, it has become a strategic asset, and critical for the normal functioning of the society. The ICT infrastructure, and the information and data being stored, processed and transferred within will then become attractive targets for a variety of malicious actors and at risk for intended and unwanted incidents, in addition to the unintended unwanted incidents such as natural disasters. This entails a need to secure and protect the infrastructure and the information and data. But with increasing numbers of connected devices and systems and the pace of ICT development, the attack surface and vulnerabilities they represent can be challenging to understand and protect against. In the context of AMI and the energy sector, this is evident with the integration of IT and OT as described in Section 2.1.3, where ICS are being integrated and connected with the AMI and SG, creating connections between different ICT systems previously separated.

In 2014, the Norwegian government appointed the Committee of Digital Vulnerabilities in Society[31], tasked with investigating the digital vulnerabilities in the society. Based on the identified vulnerabilities, they were further tasked with proposing specific measures aimed at strengthening the national contingency and reduce the digital vulnerabilities. In 2015, the result of the committee's work was presented in the investigation "NOU

[31] Digitalt sårbarhetsutvalg (NO), [59].

2015:13 Digital sårbarhet – sikkert samfunn". The investigation points out how critical societal functions have become dependent on ICT and their digital value chains, and how the span and complexity of the systems and chains can lead to insecurity as to where vulnerabilities arise and where the impact will be. Further, the investigation states how the pace in the development of ICT adds to these challenges by a rapidly changing risk and threat landscape where societal functions are experiencing incidents based on new, unknown and sophisticated methods. The investigation found these challenges in all critical societal functions, including the energy sector and AMI.

In terms of AMI and the energy sector, the investigation highlights how ICT has been an important tool in the energy sector for several years, and how its use has changed in recent years. ICT systems used to support operations and to supervise and remotely control facilities in their value chain were previously autonomous and independent of other ICT systems used by the companies. As of today, these systems have increased in complexity, and with demands of increased efficiency and security of supply, have become more integrated and connected to adjacent systems. This has led to the realization of several gains, but also increased the potential attack surfaces. One of the main reasons for the increased integration and connections between different ICT systems in the energy sector, is the implementation of AMI and SMs, which extensively use ICT systems to realize their potential. The implementation of AMI has at the same time increased the mutual dependence between the energy and telecom sector, as the communication within AMI utilizes commercial telecom services as carriers. AMI and SMs thus are substantial contributors to increased attack surfaces and vulnerabilities, due to the increased connection between ICT systems within the energy sector and reinforced dependencies between sectors of critical infrastructure.

Chapter 13.5.3 *Vulnerabilities related to smart grids*[32] specifically concerns the vulnerabilities in AMI and SMs. It demonstrates the criticality and vulnerability in functionality (e.g., the breaker functionality) and the current and future organization of the systems and processes used to operate AMI. It points out how unauthorized access to the control and configuration systems substantially increases the potential impact of intended and unintended incidents. Further, the complexity and scale of the AMI makes it challenging to gain overview of the interfaces and mutual dependencies within and to other connected systems. This indicates that the ensuring confidentiality, availability and integrity of data, communication and HW is crucial to enable a secure and reliable operation of AMI and is with the current implementation and operation already challenging to maintain. The future implementation and use of AMI and their set of new challenges may lead to different requirements in information security, but is by [59] evaluated to revolve around the continued automation of AMI and the migration to cloud solutions for various aspects of its operation. Further, the development and prevalence of SG and smart cities will add to the complexity and connectedness, increasing the attack surfaces and the dependencies between the systems. The requirements can be challenging to predict and will be based on how AMI is implemented and further developed. An important aspect in this regard, is to then organize and prepare the system in a flexible manner to accommodate future requirements and potential uses.

2.3.1 Information security in AMI – Areas

The development, implementation and operation of AMI creates different areas for information security, where each area has both distinct and overlapping challenges. This

[32] Kapittel 3.5.3 Sårbarheter i tilknytning til smarte nett (NO)

section will give a brief introduction to the areas of information security which need to be addressed to adhere to the security objectives described in Section 2.1.1. Based on an analysis of the security requirements described in Section 2.2.1, where both functional and information security requirements are included, several areas relevant to information security in AMI were identified, which are visualized in Figure 2.6.

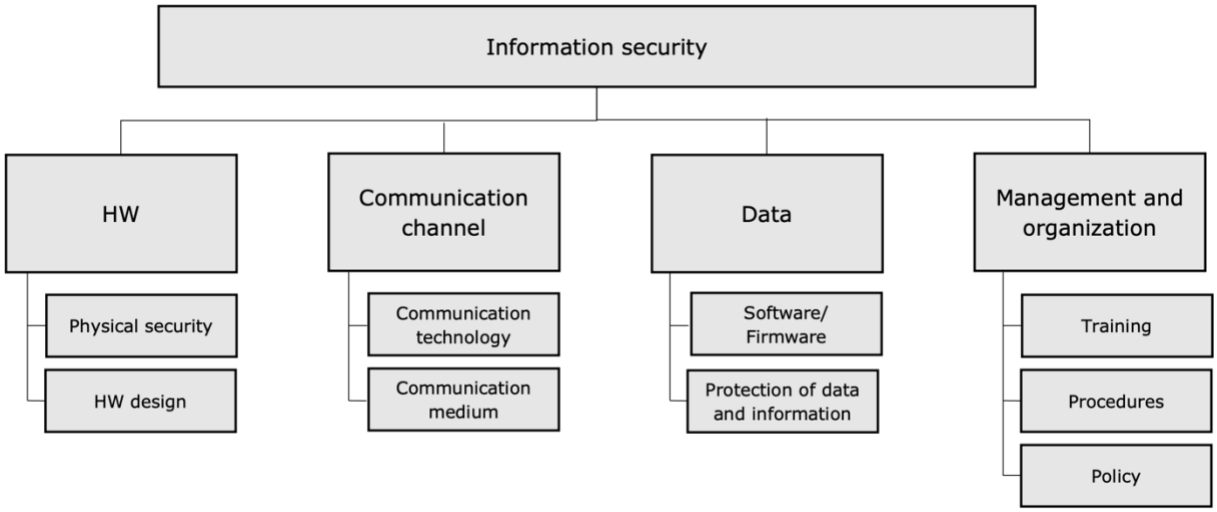


Figure 2.6 Information security in AMI

Hardware contains both the aspects of physical security and HW design. Physical security concerns measures designed to prevent unauthorized access, i.e., whether the system and/or its elements are physically secured. Both the interfaces and the communication channel can be considered elements of the system and are often the most accessible and exposed elements in the system. Physical security must consider different physical attacks to the system, such as physical modification of elements or part of an element to gain unauthorized access to data or communication, theft of elements for reverse engineering or extraction of data, and the physical disabling of elements or parts of an element. HW design security concerns how the different layers in protocol stacks are designed and secured, by assessing the different dependencies of the layers and mapping and mitigating vulnerabilities within the components of the different elements. Attacks on hardware design flaws and vulnerabilities may require physical access to elements but can also be conducted remotely.

In terms of AMI, both aspects concern securing the system and the different elements within, from the SM at end-users to the HES/MDMS at the utility control center. The physical security in AMI may entail physically restricting the access by placing elements in secured facilities with access controls. However, the distributed nature of AMI elements and the communication medium do not always facilitate physical security, e.g., by outdoor mounting of SMs at end-user facilities and the wired or wireless communication used between elements. In AMI, the distributed elements outside the utility control center are most prone for physical exposure, and often the most challenging to protect physically, i.e., the SMs, the DCs and the communication channels. Physical exposure is also a concern for the security of HW, where physical access is in some cases a prerequisite for exploiting HW vulnerabilities. In addition to the physical access, HW security is also affected by the maturity level of the design and development process, and the operation of the technology. A mature technology is often characterized by prolonged use and extensive patching and development, ridding it of most of the inherent issues and challenges. But, as the distributed elements of AMI have been

implemented over a relatively short period of time and in a vast volume, they can be to some extent characterized as immature. [60] and [61] are two examples of inherent design vulnerabilities in protocols used in the AMI that may affect the information security objectives in AMI if exploited by malicious actors.

Communication in AMI can be divided into the communication medium used (wired or wireless) and the specific communication technology used in the medium (e.g., Power Line Communication (PLC) or optical fibers, Wifi or cellular). The different technologies and media are used at different areas or tiers within AMI, as described in Section 2.1.4, and are divided into the following:

- HAN, which resides at the end-users, and concerns the communication between SMs and auxiliary equipment (other meters like gas and water), and devices connected to the HAN port at the SM. The devices connected to the HAN port are often connected to and controls other equipment (e.g., EV chargers, AC units) by direct or internet connection. These networks and connections are not considered part of AMI and are the responsibility of the end-user. In HAN, the communication between auxiliary equipment is considered part of AMI, and thus needs to be secured.
- NAN, which is the network which connects the end user and SMs to the local mesh network with DCs and master meters. The exposure and accessibility of this network depends on the medium and technology used but must be secure and reliable to secure the rest of the tiers.
- WAN is the overarching network which connects the different NANs with the control center and the HES there. The WAN also includes the MDMS, which handles the incoming data and provides control commands in return. Due to the volume of SMs, frequent exchange of data and commands, and the distance between HAN, NANs and WANs, the WAN is often based on wired media. This provides a higher bandwidth and is to a certain extent less exposed than wireless connections.

Data is both the SW/Firmware (FW) running on devices and the data and information produced within. SW and FW may contain both intended and unintended flaws and be implemented in a way that may affect security. This relates to a certain extent to the maturity of the design, development and testing processes. Shortfalls in all are relatively common, but in contrast to HW flaws which are permanent, SW/FW flaws and vulnerabilities can be corrected by patching and updating. The data and information produced, stored, processed and transferred by SW/FW will also need to be secured, but their security largely depends on the security of the other areas (HW, SW/FW, communication channel and organization in the context of AMI).

In terms of AMI, the security of SW/FW is crucial in all elements of the system. The maturity of the design, development, testing and operational use are as important as in HW and physical maturity. It can be expected that SW/FW faults and vulnerabilities will equally occur in the elements of AMI as in ordinary ICT. However, in contrast to regular ICT systems, AMI does not consist of a relatively homogeneous and common mass of elements and communication channels. The variety of elements, their properties and required functionality and how they interact and communicate in AMI have entailed development and implementation of new systems to enable communication and the handling of its data. The complexity in AMI and the different interfaces and connections will introduce security challenges, and to handle these, proprietary or tailored solutions

have been introduced. To further complicate matters, the volume of SM implementations and the pace of rollouts can also have affected the maturity and design of SW/FW. The distributed elements may have resource constraints to reduce cost and time to market, thus possibly restricting the options for SW/FW updates. As mentioned in [59], an important aspect is then to implement solutions and elements that accommodate future requirements and use in order to continually improve information security.

Organizational security concerns the sociotechnical challenges, where technical and social aspects are interrelated, and is a recognition of the organizational and human aspects in information security in addition to the technological aspects. In any organization there is an interaction between social aspects (e.g., organizational culture, knowledge sharing, learning) and technical aspects (e.g., technical security controls, automation). This implies that information security does not only revolve around technological aspects but is affected by social aspects and by how these aspects interact, as well. The organizational security aspects may directly affect the relevance of technical security aspects, where the efficiency and relevance of technical control functions and mechanisms are dependent on how they are perceived and handled by the organization and its members. A technical control is meaningless if it is circumvented by the organization's members.

To ensure organizational security and an appropriate understanding and adaptation of technical controls, policies and procedures should be addressed and established, together with appropriate training. Organizational policy will in this regard provide its members with instructions on the appropriate use of information and information systems to comply with information security requirements. The boundaries given within policies give the organization both managerial guidance and technical specification of what is authorized and what is prohibited use, and the defined roles with accompanying rights and responsibilities. To assist the organization's members in following the policies, a set of procedures should be developed. These describe in detail what must be done to comply with the abovementioned policies, and in an information security context, may describe password hygiene, actions-on during cyberattacks, handling of access control etc. Further, to create understanding and a more desirable behavior in handling of controls, procedures and policies, sufficient security and awareness training is required. By developing awareness on the threats and risks related to the use of information and information systems and the intent and function of technical controls implemented to mitigate the risks, a more favorable behavior may be achieved.

2.4 Human perception and situational awareness in information security

In this chapter, the notion of human perception of information security risks is elaborated on and describes some of the perspective taken in this study. But to understand perception, it is necessary to first understand the overarching concept of Situational Awareness (SA), where perception is an integral part of building SA.

2.4.1 Situation awareness

Situational awareness (or situation awareness, SA) as a concept has its origins within military aviation, but has since expanded to a variety of domains, as identified within the literature reviews conducted by Salmon et. al in [62]. Further, in [63], Endsley underlines the importance of SA in decision making in complex and dynamic environments, where examples from aviation and air traffic control, medicine and military

combat operations are put forward. Common characteristics of such environments are numerous system parameters, time-critical decision making and rapidly changing situations, where even short-time lapses in SA can lead to serious consequences. In such environments, the individual factors working memory and attention are limiting the individual's ability to form SA [63].

SA can have different meaning and definitions depending on the perspectives used. In this study, the perspective will be the cognitive viewpoint, looking at the human ability to comprehend technical impacts and draw conclusions to make informed decisions. The concept of SA has a broad range of descriptions and definitions, where the most accepted and cited concept is provided by Endsley [62]. She describes SA as "knowing what's going on" [63, p.36] and further defines it as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [64, p.792].

The concepts of perception, comprehension and projection within Endsley's definition are the basis for the Three Layer Model representing the development of SA, as an input to decision-making and execution [64]. This is a mental model created to overcome the individual's limitations and deal with the characteristics of a dynamic and complex situation to form improved SA. An important consideration with this model, is the separation of the constructs of decision making, performance and SA. These constructs will have different factors affecting them, and different approaches to influence them. The Three Layer Model is visualized in Figure 2.7, where SA is split into three hierarchical levels that represent increasing levels of SA.

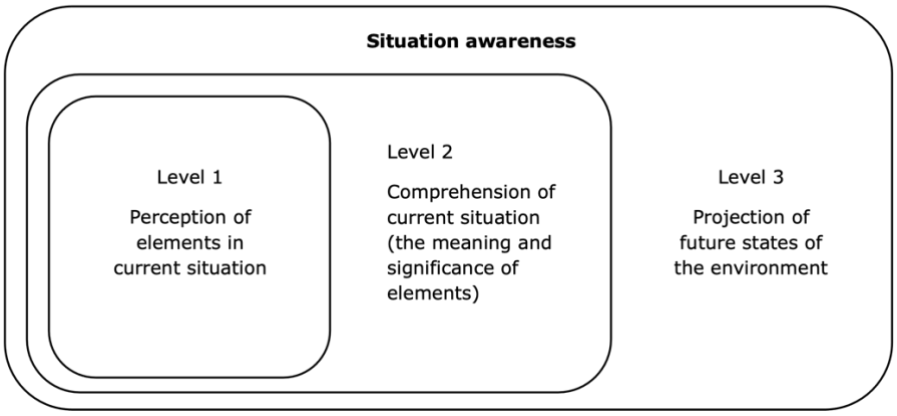


Figure 2.7 Mental model of situation awareness, adapted from [63, Figure 1]

Level 1 in the model concerns the individual's perception of the states, attributes, and dynamics of elements in the environment. This information can be perceived through system displays or directly through the senses and will form the foundation for the individual's SA. As an initial stage in gaining SA, it is crucial for the next stages and the forming of complete and accurate SA. Incomplete perception, with knowledge of only some of the elements, or inaccurate perception, with flawed knowledge of the value of elements, can lead to inaccurate and incomplete SA [63]. This can take different form, such as simply an individual failing to perceive information relevant for SA regarding the task, or misperception of signals or other information inputs. Endsley and Jones performed a study on sources of SA errors in aviation in [65], where reports from Aviation Safety Reporting System where analyzed and further classified SA errors into the levels of the mental model. Incomplete or inaccurate perception of elements in level 1 caused 76,3% of the errors. These errors occurred when information was unavailable,

difficult to distinguish and detect, misperceived, or due to failure to monitor data or memory loss. In comparison, level 2 and level 3 errors constituted of 20,3% and 3,4% respectively. One underlying cause for level 1 errors can be the common factor for complex and dynamic environments: The abundance of data and information. Perception of relevant information can be demanding when the individual is presented with vast amounts of data to consider.

The aspects of perception can be transferred to different domains, e.g., ICT and cyber environments. This is based on the fact that these environments can be complex and dynamic, characterized with rapidly changing situations, time-critical decision making and abundance of data and information to consider. And, as in other environments, to produce improved SA, level 1 perception needs to identify relevant data and information. Enhanced SA provides a valuable input to the decision making process, and may form the decision making process itself [63].

Level 2 in the model is about understanding the meaning and significance of the identified information in relation to relevant goals and objectives. By synthesizing the information, the individual can form patterns with other elements and create an integrated picture of the environment, comprehending the situation. The individual's own previous experiences, goals, preconceptions and expectations will influence how the information is valuated and integrated with the overarching goals to obtain comprehension [62]. In this regard, more experienced individuals may utilize mental models to better integrate the information with the goals. Inexperienced individuals, without a sufficient mental model and experience, may obtain the same level 1 SA, but can fall short when it comes to integrating the information with relevant goals and objectives to obtain comprehension of the situation [62, 63]. As an example, the managerial level in a power distributor must comprehend that receiving instructions from their Computer Emergency Response Team (CERT) regarding urgent updates of smart meters implies a vulnerability discovered in AMI.

Level 3 in the model involves the ability to predict future states of the situation in the near term. By combining the perception and comprehension of the situation (level 1 and 2 SA) with experience, an individual will be able to estimate future states of elements in the situation [62, 63], however with a limited time span. Continuing the previous example and based on their comprehension of the situation, the managerial level may predict that the vulnerability discovered will likely affect the organization and their customers. This forecast can guide them in the decision process to find the best course of action to ensure normal operations and enhance resilience. One action can be the scrambling of the crisis response team to track the situation and the mitigating actions in detail.

2.4.2 Situation awareness for cyber-physical systems – Information security

Based on its architecture and the interactions in the network, AMI is clearly a CPS, interacting with both physical and cyber components. This entails a need to handle both physical and cyber incidents, and to identify, assess and manage risk in both domains. Based on this, SA would be necessary in both domains for holistic risk management.

The general definition from Endsley in [63] can also be adapted to underline the specific environments in CPS, as has been done for Cyber Situational Awareness (CSA) in [66]:

"Cyber Situational Awareness is the perception of the elements in the cyber environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" [66, p.3].

In this definition, CSA can be seen as a subset of SA, concerning the cyber environment. However, it cannot be treated as a detached environment, but can be combined with other environments providing other types of SA to create a holistic picture and overall SA. In CPS, both the physical and the cyber environment will contribute to CPS SA and can be seen as a more extended subset of SA than CSA.

Both domains in CPS SA have distinct characteristics that need to be considered in relation to the definition provided by Endsley. The physical environment is as described in [63] confined to the physical world with clear boundaries and governed by the laws of physics. In contrast, the cyber environment is not confined to the physical world but exists in a space where there are no boundaries and is a seemingly limitless environment. The limitlessness can entail abundance of data and information to consider, and an important aspect for CSA is the ability to focus on the relevant aspects of this environment, depending on the goals and objectives.

Another differentiating characteristic is how information and data are perceived in the physical versus the cyber environment. In the physical domain, information for SA can be captured relying on both physical observations and through sensors. In the cyber domain however, information for SA is captured by exclusively using a variety of sensors. The actions in cyber space are seldom physically visible, as in producing a physical impact, and due to the complexity and variety of data and information, it often needs to be processed and analyzed to be human-readable.

The next characteristic is the discrepancies in potential performance between the physical and the cyber domain. Performance in terms of resources needed is relatively small in a cyber conflict compared to conventional conflicts. In a cyber conflict, a single, determined individual can challenge large organizations and even nation states. The speed of events is another performance factor, where changes in cyber space can happen at an exceptionally higher pace compared to the physical domain. An example is Denial-of-Service (DoS) attacks in critical infrastructures such as a financial institution. Customers may at one point have full access to their accounts, whereas in the next moment, a Distributed Denial-of-Service (DDoS) attacks floods the servers, forcing them to drop all connections. The last performance factor is the reach of the cyber environment, based on the limitlessness and lack of boundaries. Due to the interconnectedness and dependence on ICT today, the cyber environment has an almost global reach within seconds and can produce effects all over the world.

The last characteristic is the change in advantages between the attacker and defender [66]. In the physical domain, defensive operations have traditionally attained several advantages, e.g., in terms of resources and manpower necessary. However, in the cyber domain the advantages have shifted to the attacker. One contributing factor is the challenges in attribution, as the attacker can hide their identities utilizing different tools and techniques. Non-attributed threats or attacks make it difficult to form an efficient and sufficient response and recovery, as the sophistication, and potentially the motives and goals, can be unknown. Another factor is the limitlessness described under performance, where the attacker is not bound by time or place but have a global reach in terms of actions and impacts. The attacker also has the advantage of combining the physical and cyber domain, by exploiting human weaknesses in the physical domain to

obtain access and goals in the cyber domain, e.g., through social engineering attacks [66].

2.4.3 Risk perception

In terms of perception as described in Section 2.4.2 and 2.4.3, this study will in the semi-structured interviews explore what cyber risks, threats and vulnerabilities are perceived amongst the actors in AMI, with a sample consisting of individuals from different organizations and organizational levels.

The perception of risk is a subjective judgement, i.e., an individual's own assessment of risk. This can deviate from the objective risk, i.e., risk that is present regardless of the individual's perception or knowledge of risk, as described by Skotnes [67] and Larsen et. al. [68]. Both Skotnes and Larsen et. al. highlight the complexity of individual risk perception processes, pointing out how different models of risk perception are employed from fields such as engineering and psychology. The most common and well-recognized fields of research according to Larsen et. al. is the psychometric paradigm and heuristic and biases. Skotnes in addition describes intuitive risk perception in general, where perception is based on how risk is communicated, on previous experiences of risk and on mental mechanisms for handling uncertainty.

The psychometric paradigm is a model containing nine dimensions of perception, which can be adapted to cyber risks as described by Larsen et al. in [69]. This model has a cognitive approach, looking at perception processes as mainly cognitive, where the dimensions are representations of mental maps of risk perceptions. The dimensions are using explanatory scales and are presented in Table 2.1 which was published in [68] and is based on [69] and [70]. The intention with this model is to be able to both understand and predict risk.

Voluntariness	To what extent people perceive exposure to a cyber risk as voluntary affect how risky people perceive the related activity to be.
Immediacy of risk consequences	The greater the perceived immediacy of cyber risks are, the higher the perceived risk seems to be.
Knowledge to exposed	When people have knowledge of, and are familiar with the cyber risk in question, they perceive the risk as lower than if they have limited knowledge.
Knowledge to science/experts	Peoples level of perceived risk is affected by to what extent they believe the cyber risks are known to experts or science.
Controllability	Risk perception levels can be reduced if people believe they can control the cyber risks and avoid them from happening.
Catastrophic potential	Cyber risks with a larger impact on a single occasion (catastrophic risk) are perceived riskier than cyber risks with less impact (chronic risk).
Dread vs common	Measures whether the cyber risk in question is something people have learned to live with, or whether it is a risk they have great dread for.
Newness	New or novel cyber risks tend to be perceived as riskier and less controllable than familiar risks.
Severity of consequences	When cyber risks are perceived to have more severe consequences, they are perceived to be riskier.

Table 2.1 Nine dimensions in psychometric paradigm, reprint from [68]

The research area of heuristics and biases concerns how heuristics is used to assess information, and how this can influence biases in perception. Heuristic processes are mental shortcuts and generalizations enabling intuitive predictions and judgements as described by the work of Kahneman and Tversky in [71] and cited in [67, 68]. According to Larsen in [68], the most common heuristic is availability in the area of risk. Availability in this regard concerns how effortless incidents or situations come to mind to assess their probability of occurrence. These mental shortcuts can however create biases, where

Larsen describes the optimistic bias as one acknowledged bias stemming from cognitive heuristics. Larsen further explains how an optimistic bias can expose a systematic divergence between perceived risk and the individual's actual risk for experiencing incidents, referring to the work of Roeser et al. [72] and Weinstein et al. [73].

Both Skotnes and Larsen et. al. in [67, 68] also highlight how trust is a crucial factor in understanding risk perception and how it is formed. Larsen et al. points to how research has shown the importance of trust in management in the organizations and the vendors and service suppliers if there is a lack of knowledge regarding specific risks. Skotnes further states how this trust in an organization, vendor or expert is assumed to be dependent on the perception of several attributes, such as competence and knowledge in the area in question.

2.5 Related work on risk perception of AMI security

In this chapter, related research works on risk perception in the power supply and other critical infrastructure are discussed to give an overview of the subject. The thesis identified a small collection of research during the initial literature review, where one is conducted in a Norwegian context prior to the large-scale implementation of AMI, and one undertaken in Sweden. These articles can be used as a basis for comparison on several levels, such as between countries (e.g., Norway and Sweden) and the changes over time (before and after the mass-implementation of smart meters and AMI).

2.5.1 Risk perception in critical societal services

The most closely related research identified is the work of Asplund and Nadjm-Tehrani in [17], where they investigated the attitudes and perceptions of risk of IoT in three critical societal services in Sweden. The study sought to highlight the risks and perceptions of risk in services where the integration of IoT has been pushed forward both by regulatory requirements, by markets and advances in technology, or a combination. The investigated services were energy, water and societal services, which have distinct differences in aspects such as regulations and technologies used. At the same time, they have common features, as they all are considered critical societal services, with strict requirements on confidentiality, integrity and availability to uphold services. Failure is not an option, as implied in [17].

To describe the perception of risk, the study conducted several interviews based on questions derived from preliminary workshops with actors within the services. The results were presented primarily as summaries with quotes, as the range of professions and alleged complexity of the subject resulted in answers where no clear prevailing theme was found. They also revealed noticeable uncertainty and disaccord on the severity of risks and threats. The variety in risk perception is hypothesized to be grounded in individual experiences and perception of what the future may bring in terms of risks and threats, and differences in competence. However, as stated in the conclusion, the sampling of the study is not large enough to ensure external validity but may provide insight in the challenges with differentiating risk perceptions. The study does not include subjects from regulatory authorities and does not explore how regulatory compliance enforcement affects the risk picture. Different regulatory bodies may have different methods for and depths in guiding and regulating the services in information security risk management, hence creating different understanding for risk and risk assessment in the different services.

2.5.2 Risk perception in electric power supply network companies

The research conducted by Skotnes in [67] investigated a related topic to that in Asplund and Nadjm-Tehrani in [17], looking at risk perception concerning security and safety of ICT systems amongst power supply network companies in Norway. However, the significant insights provided by the study, are the discussion and findings in relation to the factors that can influence the individual's risk perception. Some of these factors can indirectly have affected the findings in Section 5.2, but the causal relationships are outside the scope of this thesis.

An important consideration within the study, is how different aspects are used to distinguish between risk situations or problems. Degree of complexity and uncertainty are two prominent examples, where complexity refers to the challenge of identifying links between causal agents and specific impacts. Uncertainty refers to challenges in predicting events and the subsequent consequences. AMI certainly falls under the description as a complex system of systems, where it can be challenging to identify all of the interdependencies and the links between cause and effect. AMI may also fall under the uncertainty aspect, as the system has been designed so that potential interactions between elements can be challenging to understand, predict or protect against (as most ICT systems). Both aspects have an important role in the understanding of risk perception and can influence how risk is perceived amongst individuals handling complex systems/organizations with potential inherent uncertainties.

In relation to the problem statement in this thesis, one of the findings in this study is that the majority of the respondents' perceived the risk of attacks on the network operators' ICT systems as low. The only statistically significant difference found in regard to perception was between large and small companies, and as such is in accordance with previous studies regarding the effect of company size on risk perception [67]. Larger companies have more rigorous and standardized systems for security management in contrast to smaller companies which operate under a more resource constrained management. Functions and roles are often spread over fewer employees or outsourced to 3rd party contractors. Where smaller companies are resource constrained, the larger companies often have more fine-grained delegation of duties, such as separate ICT and OT departments. This allows them to concentrate knowledge and expertise and may contribute to a more realistic risk perception. However, communication barriers between departments and subcultures, increased complexity (they have potentially a multitude of systems) and outsourcing of tasks, reduce the effect of this knowledge concentration regarding perception of risk.

The level of knowledge was a common theme that may affect risk perceptions. The first aspect of knowledge to discuss, was how knowledge of security often affects how security incidents are interpreted and perceived. Erroneous knowledge and lack of knowledge may lead to incorrect perception of risk. However, the study does not find any correlation between knowledge of security and safety and the perception of risk. This may be due to biases at the respondents in their perception of risks and is to a certain degree underlined by the interviews with the regulatory authority NVE. The study also elaborates on how knowledge in terms of experience can affect perception of risk. By being exposed to incidents involving danger and loss, the individual will often rate similar incidents at a higher risk level in the future. Most of the companies surveyed in the study had experienced attacks on their ICT systems, however almost all of them had failed, and as such they perceived the risk of cyberattacks to be low. This indicates that it may be perceived differently if they had experienced loss or imminent danger of loss. Another

aspect elaborated on, is knowledge and understanding of the complex systems used in the power industry. The study does not present any evidence of this effect but discusses how a lack of knowledge may lead to bias in the perception of risk. As previously discussed, AMI can be defined as a complex system of systems, where such biases may arise.

Another interesting finding was the level of trust and gullibility within the power network companies in relation to ICT security challenges and their providers. Common themes were "it doesn't happen to us" and that security is taken care of by others (e.g., the vendors of systems or the company handling outsourced functions/systems). This will most likely reduce the focus on security in ICT systems, and as such affect the perception of risk within the companies.

The factors impacting perception of risk discussed in the study shows the complexity of perception and how AMI and the architecture itself can affect this together with the size of the companies and the knowledge and experience of ICT security, risks and incidents.

3 Research methodology

The choice of methods is dependent on the RQs and how to answer those, and different methods can be employed to provide the needed knowledge and information. In this chapter, the research study describes and justifies the design and methodology chosen to answer the problem statement and RQs defined in Chapter 1. In this chapter the research design is described in detail together with the selection process to show an understanding of relevant scientific methodology theories.

3.1 Considering methodological options

The study is investigating a field where there exists a large body of research on both information security and perception of risk but limited to the specific field of interest: Risk perception in AMI. Based on this, a challenge was to establish a design to be able to measure and answer the specific RQs. A research design with measurements for information security vulnerabilities and threats was created, and the following sections describe the overarching design of the research project with attention to validity and reliability of the methods chosen.

3.1.1 General research designs

Several methods are presented in [74] and include survey research, case study, content analysis and experimental research. The purpose and characteristics are different for each method and the choice of method depends on the research problem to address and the specific questions to be answered. As such, a study can be divided into different parts, depending on the problem statement and the RQs that need to be answered. However, common to all scientific research, data need to be collected and analyzed, either by quantitative or qualitative methods. Quantitative methods require data that can be transformed to numerical information, whereas qualitative methods concern data that that are textual and informative, and not necessarily transformable to numerical information. By introducing both dimensions in a study, they can substantiate and supplement each other and integrate conclusions from both into a cohesive whole.

In an overarching manner, the study seeks to answer what can be interpreted as a contemporary phenomenon in a real-life context, based on explanatory and exploratory RQs. It wants to explore a situation as it is, and not necessarily determine a specific cause-and effect relationship. In terms of a general research approach, this would deem a qualitative research method the most appropriate approach. In [74, p.269-295], several qualitative designs are described, where one of their main advantages is the ability to explore a phenomenon which has previously not been broadly studied to gain initial insights. The overall design is then qualitative and exploration-based. However, the RQs may need individual methods and strategies, as described in the following section.

To answer the stated problem and the RQs, the research study needed a theoretical foundation and data to analyze, and as such, specific methods to conduct both were identified. Similarly important considerations were how to conduct the validation and verification of the results obtained, based on the chosen methods. In order to produce valid results and draw defensible conclusions, a combination of both qualitative and quantitative data was regarded as expedient. Subsequently, this research study used a

combination of qualitative and quantitative methods, where the semi-structured interviews collected both types of data. This triangulation of methods is described visually in Figure 3.1.

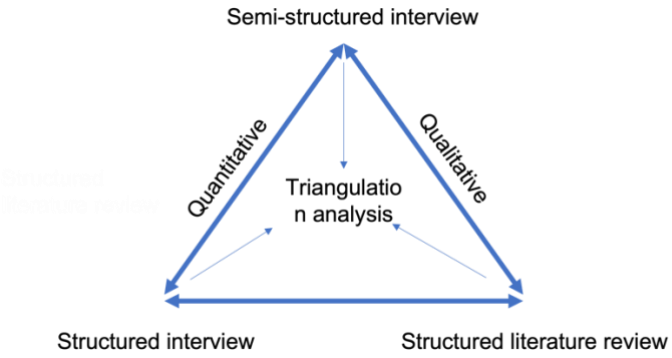


Figure 3.1 Research methodology triangulation, adapted from [75]

3.1.2 Increasing validity and quality

Within all scientific research conducted, an important aspect is to determine if the chosen methods will result in credible and meaningful findings. This entails describing the general validity of the overall research, where different strategies can be applied for both qualitative and quantitative research. Several concepts are described in [74], where the concepts of internal and external validity are laid out with several strategies for enhancement.

The concept of internal validity concerns the ability of the design and data produced to draw plausible and defensible conclusions, where several strategies can be applied [74, p.278]. Three prominent strategies are feedback from others, triangulation and respondent validation, which all aids in enhancing the internal validity. Feedback from others concerns pursuing the opinions from researchers within the field to get their take on the methods chosen, the accuracy of interpretations and findings, and how plausible and valid the conclusions are. Triangulation compares several sources of data with the aim of finding consistencies or inconsistencies within the data. And in respondent validation, a study seeks to validate the findings and conclusions amongst the participants of the study.

The external validity concerns the ability of the research study and its conclusions to be generalizable to other contexts, e.g., to a larger population or other situations. At the same time, external validity and generalization can also imply the ability to transfer or apply the conclusions to similar situations. [74, p.105] describes several concepts that can be used to increase the external validity; using a real-life setting and a representative sample are two examples.

As part of the research design for the study, both internal and external validity were addressed to increase the quality, credibility and generalizability of the study. The main strategies and methods sought to be employed were feedback from others, triangulation of interviews with questionnaires and a representative sample.

3.1.3 Reliability – Bias and backgrounds

In qualitative studies an important consideration for researchers is to explain their role in the research process, by exercising reflexivity or self-reflection [74]. By identifying any

biases that may affect the collection and interpretation of data, a researcher can take action to mitigate the potential effect, and thus increase the reliability of the study.

In terms of personal backgrounds concerning the problem statement for this study, both researchers have backgrounds and experiences from a high strategic level within the Norwegian Armed Forces in the field of ICT. This includes both managerial and on-hands experience at operational, tactical and strategic level within the Armed Forces. The researchers have educational backgrounds from telematics and computer engineering and have worked with cyber security related challenges throughout their careers. Thus, they have both experience and knowledge within the subject, acquired through their professional work and education. These aspects have influenced both the interpretations and decisions they have made during the research, including choice of theory in the SLR, the coding scheme used, and the discussion of the acquired results.

The preliminary work for this research study was conducted as part of the NTNU course IMT 4203: Critical Infrastructure Security, and in the form of a survey report on information security challenges in AMI [14]. The findings from this report may have influenced how the results from the SLR were tabulated, summarized and discussed. This effect may then have cascaded and influenced how the interview guide was formed, by creating questions that follow the topics and findings from the report. The participants may thus have been biased to focus more deeply on these findings and ignore other relevant subjects and topics. This was sought to be mitigated by continuously reviewing the work together with Subject Matter Experts (SME) from industry and fellow students.

3.1.4 Choice of methodology

To enhance completeness and quality of the research study, an overall qualitative method with an embedded design was chosen. This provided both qualitative and quantitative dimensions of the problem statement and enabled the use of different types of data to be compared and possibly triangulate findings. This would aid in producing a more complete and comprehensive understanding of perceptions of information security in AMI.

RQ 1 was answered through a structured literature review, and RQ2 through semi-structured interviews utilizing an embedded design with a structured and semi-structured part. RQ3 was answered through a comparative analysis, identifying the consistencies and inconsistencies between literature and stakeholders to produce evidence-based insights regarding the divergence in information security risk focus and perception.

This study conducted a literature review to create a theoretical foundation and overview of the current information security risks in AMI. The review was used as a basis for conducting survey research and connected the research's findings to a larger body of research. [74, p.159] describes survey research as asking individual subjects questions, further tabulating and analyzing the answers, in order to draw inferences or identify patterns in a specific population. As it captures a transitory compilation of data, it can be used to generalize about the problem statement for a longer period of time. However, this may rely heavily on the studied subject and its pace of development. To increase the generalizability in a world where change is continuous, survey research would have to be repeated over time. The design of the survey research consisted of interviews. Further, the interviews were created with an embedded design to more efficiently produce both qualitative and quantitative data. This involved both a structured and a semi-structured

part in the same interview setting. By triangulating the findings obtained with the different methods, the study could to some degree perform a comparative analysis.

3.2 RQs and applied methodology

The research process is illustrated in Figure 3.2 and consisted mainly of three parts. In part 1, a systematic literature review was performed to answer RQ 1 and form the questions for interviews. In addition, the review provided an extensive basis for knowledge of the topic in research and contributed partly to Chapter 2. Part 2 describes the survey process of interviews with the embedded design, which answered RQ 2. Finally, in part 3, the answers from RQ 1 and 2 contributed to answering RQ 3 and RQ 4.

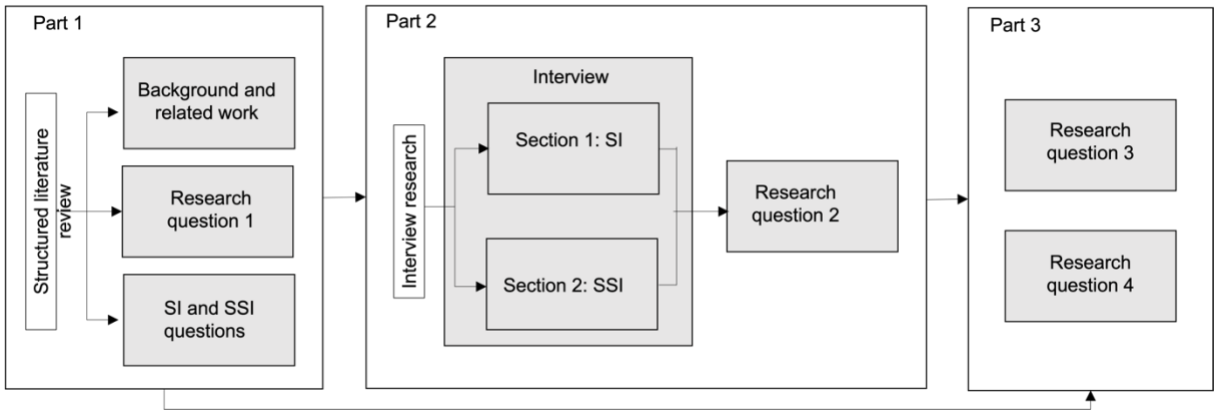


Figure 3.2 Research process, adapted from [76]

3.2.1 RQ 1: Literature review

This question seeks to explore and categorize a broadly studied subject to scope and classify the research within the field. In this case, the classification and scoping concern the information security risks in AMI in the energy sector. As described in [74, p.70-91], a literature review will be suitable for such instances of qualitative research. The literature review will seek to classify the vulnerabilities, threats, consequences, their likelihood and assessment of risks towards AMI, based on the research trends discovered within the literature. Data will be collected and categorized according to the classification scheme and used to form the interview questions and as input to the comparative analysis in RQ 3.

When conducting academic literature reviews, the format and procedures may differ depending on the context and the purpose of the review. However, they are all analyses of previously conducted research, where the aim is to add to the knowledge with new perspectives or highlight gaps in the reviewed research. In [77], several methods are presented, which are grouped into two main categories: Traditional and systematic.

The literature review conducted in this thesis is based on a defined aim and RQ, compiling a significant number of sources of information on the subject of AMI security, with the aim of answering the question of: *What information security risks and threats are prevalent within AMI according to literature?* A systematic literature review will therefore be chosen as the method, using the steps, phases and principles detailed in [77, p.103-127]. Utilizing such a methodology will aid in obtaining structure and transparency in the process and result. Further, it will provide means or methods to minimize bias and to ensure strict scoping, providing a manageable level of results to

review. The phases are visualized in Figure 3.3 and described in detail in the following sections:

Figure 3.3 Phases in a systematic literature review

3.2.1.1 Phase 1 scoping review

In the scoping review, the main goal was to get an overview of the topic itself and the available scientific literature within the field. The review included the NTNU course "IMT 4203 Critical Infrastructure Security"[33], and the term paper produced by the authors as part of the course [14], where literature and knowledge gaps relevant to the topic were identified. However, the scope of the review needed to be broadened to accommodate the defined problem statement and the developed review questions.

The first step in this phase was to define the question the review was set to answer, i.e., RQ 1: *What information security risks and threats are prevalent/significant within AMI based on/according to literature?* But to answer this question, a set of more tangible review questions were developed:

1. What are the prevalent information security-related vulnerabilities in AMI?
2. What are the prevalent information security-related threats in AMI?
3. What are the impact and consequences of potential attacks in AMI?
4. What are the prevalent information security-related risks assessed in AMI?

To clarify the interconnection between vulnerabilities, threats, risks and impacts, the thesis has adopted the definitions given in Section 2.1.2.

Further in this phase, the plan was to use a diverse selection of academic search engines and databases; [78] identifies several of those and the lessons learned using the different sources. Based on this, the following engines were initially included: ScienceDirect, IEEExplore, Web of Science and ACM Digital Library. NTNU's university library Oria and Google Scholar were also used to get a more extensive view of the field of research as they produce aggregated results from other sources. Due to this they were also excluded from the literature review itself. By using a selection of different search engines, the aim was to collect a more diverse selection of academic literature and information, possibly from a varied selection of academic areas, and to counter the fact underlined in [78]: There is not a single search engine that will find all of the primary research.

The next step was to develop a set of specific keywords and Boolean search strings to ensure the search targeted the research area and topic and produced a selection of reports and literature within the scope. Table 3.1 gives an overview of the result of the scoping review.

[33] https://www.ntnu.edu/studies/courses/IMT4203#tab=omEmnet

Search engines	IEEExplore
	ACM Digital Library
	ScienceDirect
	Web of Science
Literature	Journal article
	Conference proceedings
	Government publications
Keywords	Information security
	Cyber security
	Risk
	AMI
Search string	((information OR cyber) AND security) AND (risk OR vulnerability OR threat OR assessment) AND ("advanced metering infrastructure" OR "advanced metering system" OR AMI OR AMS)

Table 3.1 Result scoping review

3.2.1.2 Phase 2 comprehensive search

The comprehensive search was built on phase 1 and consisted of searching the identified search engines using the Boolean search string on the whole body of the publications, i.e., on all fields in the search filters. A wide application of the string was chosen, as the scoping review revealed few search results when applied only to title, abstract and keywords. The search initially was not limited to a specific period, in order to get the full body of research conducted in the field. However, in phase 3 Quality assessment, the period from 2012 to 2023 was set as an inclusion criterion. This is based on the pace in development and application of AMI, and the introduction of the Norwegian regulation on AMI[34] in 2011. Further, after the quality assessment process in the same phase, the material's references were scrutinized using snowballing, thus identifying further relevant research not captured by the comprehensive research.

Table 3.2 shows the search results obtained when the search string was applied within the different search engines:

Search engines	**Results**
IEEExplore	133
ACM Digital Library	116
ScienceDirect	876
Web of Science	98
Total	1223

Table 3.2 Results from search engines

3.2.1.3 Phase 3 Quality and relevance assessment

This phase comprised indexing the identified material, identifying relevance and quality criteria and then applying the criteria on the material. Microsoft Excel was used to index the material and document the process of assessment. The relevance assessment consisted of applying inclusion and exclusion criteria to each paper by evaluating the year of publication, title, abstract, introduction and conclusion. Due to a larger body of research, the assessment was conducted consistently to obtain research with the most relevance to the review questions and the overall problem statement for the study. Table 3.3 shows the identified inclusion (I) and exclusion (E) criteria for relevance.

[34] Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv (Avregningsforskriften) - Kapittel 4. Avanserte måle- og styringssystem (NO) [52]

Criteria		
Inclusion	I1	Articles published from 2012-2023
	I2	Access to full-text articles
	I3	Articles written in English or Norwegian
	I4	Articles related to information security vulnerabilities, threats, impacts or assessment of risks to AMI
Exclusion	E1	Same articles from different research database
	E2	Articles published in magazine, books or white paper
	E3	Articles concerning SG in general
	E4	Articles not related to information security in AMI

Table 3.3 Relevance criteria

The quality assessment consisted of evaluating the remaining material against a checklist. Jesson et. al. propose in [77, p.116-122] several different checklists, such as the COREQ32 and "Hierarchy of research study design", but this depends on the type of research reviewed and the methods used in the research. The book also proposes a set of key features that can be used to ground the quality assessment, and is scalable with additional features from the reviewer [77, p.121-122]. The thesis adopted this set of starting features and further developed them into a checklist described in Table 3.4.

Criteria	Questions for assessment	Quality rating
Peer-reviewed	N/A	Yes/ No
Title relevance	N/A	Low/ Medium/ High
Abstract relevance	N/A	Low/ Medium/ High
Review question relevance	N/A	Low/ Medium/ High
Problem statement relevance	N/A	Low/ Medium/ High
Introduction	What are the ambition and objectives of the study?	Descriptions
	What is the rationale for the study	
	Is there a link to theory?	
Method	What is the research design?	Descriptions
	Why were this design chosen?	
	How is the sampling conducted?	
Result	What types of data are collected?	Type
	What is the validity and reliability of the data?	Low/ Medium/ High
	How, where, why, when and by whom was the data produced/collected?	
	What method was used for analysis?	Type
	What is the validity and reliability of the analysis?	Low/ Medium/ High
Discussion and conclusion	Are the possible limitations in methods and results discussed?	Yes/ No
	Does the result answer the problem statement and review questions?	Yes/ No
	Are any possible biases discussed and analyzed?	Yes/ No
Overall formal quality	What is the quality of language and grammar?	Low/ Medium/ High
	How is the quality of structure in the article?	

Table 3.4 Quality assessment, based on [77]

After the relevance and quality assessment, 29 articles were included, and a snowballing search was performed on these by using the references in the articles to find related and comparable research. Phase 3 is visualized in Figure 3.4, and following these steps resulted in the final set of material detailed in Table 3.5.

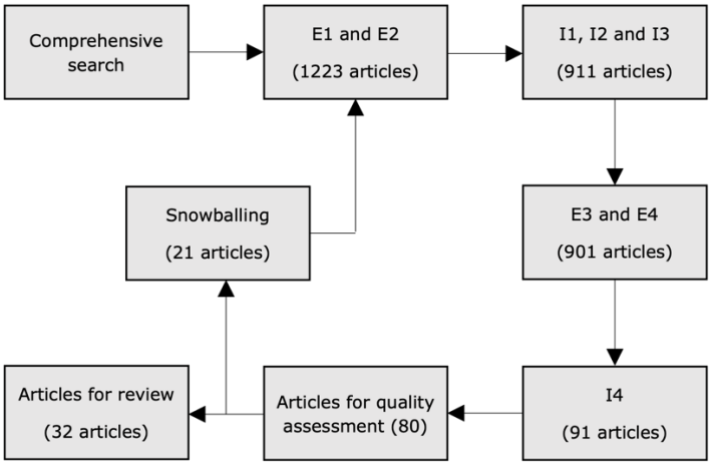


Figure 3.4 Relevance and quality assessment

Search engine	Type of publication	Qual	Quan	Mixed	Total
IEEExplore	Journal	1	1	-	7
	Conference proceedings	3	2	-	
	Government publications	-	-	-	
ACM Digital Library	Journal	-	-	-	4
	Conference proceedings	-	4	-	
	Government publications	-	-	-	
ScienceDirect	Journal	6	2	1	9
	Conference proceedings	-	-	-	
	Government publications	-	-	-	
Web of Science	Journal	6	1	-	9
	Conference proceedings	2	-	-	
	Government publications	-	-	-	
Snowballing (IET, SpringerLink)	Journal	1	-	-	3
	Conference proceedings	1	-	-	
	Government publications	1	-	-	
					32

Table 3.5 Included material after phase 1-3

3.2.1.4 Phase 4 Data extraction

In this phase each article was reviewed and evaluated in a data extraction sheet based on the review questions identified earlier. This entailed reading the full text of the material, and extract relevant data by commenting on relevant aspects, and catalogue vulnerabilities, threats, consequences, risks and assessments described. These were used as input in the following phases.

3.2.1.5 Phase 5 Synthesis

The next phase in the systematic review was the synthesis of the selected articles, based on the data extracted in phase 4. The overarching aim was to give a summary of the characteristics and present the findings in a meaningful way. The comments and data extraction sheet aided in highlighting the consistencies and inconsistencies, establishing connections and identifying knowledge gaps in the material reviewed. Further, it aided in establishing categories for the deductive codes, providing a framework for the comparative analysis with the findings from RQ 2 (SSI). The categories, framework and the comments were also used as input in forming interview questions for both the structured and semi-structured part. The list of deductive codes and categories are described in Table 5.1, which is inspired and adapted from [74].

3.2.1.6 Part 6 Write-up

The write up consisted of summarizing the most important aspects and conclusions regarding the review questions and the overall problem statement for this research study. This enabled the study to answer RQ 1, aided in forming interview questions, provided additional material for Chapter 2, and lastly provided a crucial element in the comparative analysis in Section 5.3.

The information and findings from the SLR related to the RQs is aggregated in Section 4.1. The result from the analysis is then discussed in Section 5.1.

3.2.2 RQ 2: Interviews

This question seeks to answer how information security risks associated with AMI are perceived and understood by different stakeholders within the Norwegian energy sector. The main methodology for collecting data was primarily semi-structured interviews, based on questions inspired by the SLR, inputs from supervisor and colleagues, and academic sources. Such an approach will capture what Leedy [74, p.159] describes as a moment in time, by acquiring information about the perceptions and attitudes of the interviewees. The objective is to learn and generalize about a larger population based on the findings from a sample of the population, also called inductive reasoning [74].

The method of semi-structured interviews revolved around a set amount of relevant questions, in addition to more individually tailored questions as recommended in [74, p.282]. The method enabled the study to probe answers if necessary to reveal hidden details and making sure the questions are fully answered. In order to ensure a productive interview and obtain reliable and relevant data, the interviews were planned and conducted in line with the 7 stages of an interview inquiry, described by Brinkmann and Kvale in [79]. The stages are described below, with the activities conducted in each stage.

1) **Development of themes:** The first step refers to defining the research topic and purpose of an interview investigation, by formulating the *why* and the *what* of the interview. Answering both questions enable the investigation to better answer the *how* question in the next step: Designing the interview, i.e., defining the methods to reach the goal and meet the purpose of the investigation. As described in Chapter 1, the researched topic was the perception of information security risks within AMI in the energy sector of Norway. And the purpose of the interview investigation was to identify these perceptions, and thus provide data to enable the study to answer RQ 3.

2) **Design:** To fulfil the purpose of the study, different methods can be used to obtain the intended knowledge. This stage answers the *how* of the investigation: What methods will enable the investigation to best fulfil the purpose defined in stage 1. Design involves the planning of procedures and techniques to be used, where moral implications of the investigation are considered as well. Within this research study, the method chosen was SSI, as the question it seeks to answer is of exploratory nature, i.e., exploring a question that has not been investigated extensively. As a methodology, SSI is flexible by combining both structured and unstructured elements, with some open-ended questions that allow for probing of answers, and some set questions with closed answers. This setup potentially ensures both reliable and comparable data, while allowing to ask elaborative and probing questions to gain more specific insights and clear up potential

misunderstandings. However, such a design also entails clear disadvantages depending on how the flexibility is used. The validity of the interviews can be reduced if the probing strays too far from the predetermined set of questions, making the comparison and analyses challenging. Another aspect is the bias that can be introduced, such as researcher and response bias [74]. By asking questions that lead the answers in a specific direction, and the subjects giving what they think are the desired answers, sources of error are introduced. In this study, the comparison and analyses are both based on a set amount of closed-ended and structured questions to ensure the ability for comparison, and a set number of open-ended questions to provide deeper insights. By adhering to this structure, the validity can be enhanced; however, this also depends on the quality of the questions developed. The interview was divided into a structured and semi-structured part, where both were conducted in the same setting. The closed-end questions were given in the structured part of the interview, and developed in the form of a questionnaire, focusing on ranking different elements related to experience with information security in AMI, and the concepts of risk, consequence and likelihood. The semi-structured part consisted of more open-ended questions, designed to enrich the structured questions and provide a basis for deeper reflections.

Using the recommendations from the research study's supervisor, handbooks such as [80], and published research such as [17] and [81] as inspiration and guidance, an interview guide was developed. The overarching principles in this development were inspired by [17] and were as follows: (i) Utilize questions that are answerable by individuals with different technical background and expertise, (ii) Open enough to catch trends, ideas and phenomena, (iii) Specific enough to provide insights in the perceived state of AMI security, and (iv) The interviews must be time-efficient and not exceed one hour. The interview guide is enclosed in Appendix A in an English (A1) and a Norwegian (A2) version. It was tested on fellow students and a few selected participants from two different distribution network companies and adjusted based on their inputs. An application was then submitted to the Norwegian Center for Research Data (NSD[35]), which included the interview guide and invitation letter containing the consent form. In this application, a data handling plan was created to ensure compliance with regulatory requirements when handling organizational and PII from the interview subjects. The PII included names, contact and background information, written and audio transcripts from interviews, and was primarily used for communication with the subjects. The written report from this research study was sanitized where all PII and organizational identifiable information was removed. This stage also included scheduling the interviews in collaboration with the coordinator at each organization. The interview subjects were chosen based on the sampling procedure explained in Paragraph 3.2.2.1.

3) **Interviewing:** The interviews were conducted over two months, in February and March 2023, utilizing the interview guide consistently. All interviews were conducted in Norwegian except for one that was conducted in English. The transcripts were produced in the native language. As the interview subjects and organizations were spread at different locations throughout Norway, most of the

[35] Norsk Senter for forskningsData (NO)

interviews were conducted as virtual meetings utilizing the online conferencing platform Microsoft Teams. This required the interviewer to prepare the interview stage in greater detail to build rapport with the interview subject. The main objective here was to give the interview subjects an introduction to the interviewers and to build a connection on common subjects. This was also eased with the use of two interviewers with a clear separation of duties, where one was assigned the role of leading, being fully present in the interview setting and a more attentive listener. The other interviewer would take the role of secretary, handling the technical aspects and ensuring compliance and adherence to the interview guide. An important aspect when building the rapport was to disarm the potential sensitivity in the topic of the interview. This was done by clarifying the compliance to the non-disclosure agreement both interviewers are bound by as officers in the Norwegian Armed Forces, and the consent form both parties have agreed upon. Further on this was to underline that the interview was focusing on a topic that does not warrant the disclosure of sensitive information, i.e., PII or classified information. The interview session was digitally recorded through Teams for later transcription, as the built-in transcription functionality produced erroneous results. System audio was recorded as well as a backup if the platform-recording was faulty. All digital recordings were stored on NTNU's OneCloud-solution, where each student has separate account and storage.

4) **Transcribing:** The digital recording from step 3 was processed through the *Dictate from Audio*-feature in Microsoft Word to produce digital transcriptions of the interviews in their native language. The transcription was sent to the specific interviewees for corrections, a final validation and approval to be included in the study. The digital recordings were deleted after submission and approval of the research study in accordance with the NSD approval (Appendix C).

5) **Analyzing:** The topic and purpose developed in stage 1 formed the foundation for the analysis of the interview transcripts from stage 3 and 4. This involved utilizing appropriate modes for analyzing the interviews. The crucial aspect in this regard is to have a set method planned in stage 2 when designing the interview guide, and to be able to integrate it into the interview itself. By clarifying or testing the interpretations during the interviews, a part of the analysis is done in the interview situation itself, easing the later analysis by providing confirmed or corrected interpretations.

   The data collected in the semi-structured part was analyzed using qualitative thematic analysis and coded utilizing the integrated coding approach as described in [82] by Cruzes and Dyba. Thematic analysis is a mode for systematic analysis of qualitative data, comprising identifying themes and coding the data based on the themes, and further interpreting the created thematic structure by looking for commonalities and patterns [83]. Integrated coding entails utilizing both inductive (data driven) and deductive codes (concept-driven or codes prepared in advance) [79, 82]. This approach enabled the use of an existing framework with categories, while still allowing development of new codes and categories. Thus, if new concepts would emerge, the integrated coding scheme would allow for both inductive and deductive coding. The framework for the coding process was the deductive categories developed in the SLR.

The scheme was operationalized by giving each section of data an inductive meaning code when concepts emerged as the data was analyzed. Meaning code was chosen as the key mode to the inductive coding of the material produced in stage 4. This mode of coding involves affixing one or more keywords to segments of the transcripts to enable compilation of codes. The keywords are based on inductive empirical coding or data driven coding, meaning that the keywords often use notions found in the data and attempt to be as close as possible to the empirical evidence. The study chose a meaning-centered mode for inductive coding as it was more concerned with what was said (i.e., treating the transcripts as reports), rather than the linguistic form by which meanings are conveyed (i.e., treating the transcripts as accounts). The meaning codes were then grouped into clusters before meaning condensation was applied to turn longer statements into briefer ones, aiding in identifying the essence in the statements.

The used integrated coding approach provided, through thematic analysis, a mode for comparison between the findings in the SLR and SSI, which ultimately enabled the study to answer RQ 3.

6) **Verifying:** At this stage, the validity, reliability and generalizability of the findings from analysis are determined by various methods [79]. Reliability and validity concern the objectivity of the knowledge obtained through the selected method. More specifically, validity concerns whether the method investigates the intended problem statement. In the context of this research study, the interview study was conducted in accordance with the topic and purpose defined in the RQs and further refined in stage 1 above, i.e., to investigate perception of information security risks within AMI. Reliability in this context concerns the consistency of the findings, both across the body of interviews conducted, but also concerning to what degree the findings are reproducible, e.g., at different times and by different researchers. In this study, a total of 27 interviews were conducted, which produced a thematic diverse array of findings. The different subgroups where internally compared for consistency, where the subgroups were formed based on organizational level, organizational size and organizational type. Generalizability in this context concerns whether the findings are applicable to other situations or subjects. A common objection to interview studies in this regard is the low number of subjects in the sample. However, this can to some extent be mitigated by using appropriate sampling strategies, producing representative samples in the interview study. Another approach is the analytical generalization described by Brinkmann and Kvale in [79]. This approach involves using rich descriptions of the interview methodology and process, with the aim of enabling a reasoned judgement regarding the degree of transferability of the findings from this situation to another situation. The background and methodology chapter aim at providing a sufficiently rich description of the process and methodologies and serve as a foundation for arguments presented in the analysis and discussion chapter about the generalizability of the findings.

7) **Reporting:** The last stage revolves around how the research study communicates the knowledge acquired through the interviews. This involves reporting the methods used and the findings obtained in an accepted scientific format, taking ethical aspects into account, and producing a comprehensible product [79]. An important consideration in this regard is that the quality of the report considerably

affects the validity and reliability of the interview report. The methodology chapter therefore seeks to provide concrete, reasoned and rich descriptions of the chosen methodology. Further, the findings are reported in a format which enables comparison with the findings in the SLR, together with rich contextual information concerning the interview findings. In terms of ethical aspects, the main consideration was the anonymization of interview subjects and their organizations, both in a privacy context, but also to mitigate potential response bias. Response bias in this context is how external expectations can influence how the interview subjects respond, e.g., they are influenced by what they assume their organization or higher management want them to communicate. Anonymity will to a certain degree reduce such expectations and can aid in producing more genuine answers and reflections.

3.2.2.1 Sampling procedure

In survey research with an exploratory nature, it is important to choose a sample that can be representative of the population the study wants to draw inferences from [74]. A narrow or incomplete sample will not make it possible to generalize the findings to a wider body of the population.

To achieve a significant and representative sample of interview subjects, the study targeted three general levels within the stakeholder organizations, from strategic, through tactical and down to the operational level. This provided subjects with abstract and concrete experience in information security and AMI integration, i.e., providing the study with the perspectives of different functions and levels. These levels were also approached in the complete chain of stakeholders in the energy sector of Norway, from energy regulatory authorities, actors in the distribution network and end-users/consumers. Ensuring representation of different organizational sizes was also sought, based on the findings of Skotnes in [67] and the effect of organizational size on the perception of risk. A total of 27 subjects were interviewed, with a distribution between organizational levels and company sizes as described in Table 3.6.

Organizational level		DSO			AMI vendor (equipment, service and operator)	Power vendor	Other (Industry organizations, industry SME)	End-user	Regulatory authority	Total	
		Small (<15k)	Medium (>15k-100k)	Large (>100k)							
Strategic	Male	1	1	2	-	1	-	2	1	8	10
	Female	-	-	-	-	-	-	-	2	2	
Tactical	Male	-	2	-	-	1	1	3	1	8	10
	Female	-	1	-	-	-	-	-	1	2	
Operational	Male	1	1	1	2	-	1	-	1	7	7
	Female	-	-	-	-	-	-	-	-	-	
Total		2	5	3	2	2	2	5	6	27	

Table 3.6 Demographic profiles of interview subjects

The described sampling aspects imply a stratified purposeful sampling strategy. This aims at ensuring a heterogenous sample in terms of sizes of and levels within the organizations. This strategy is useful to highlight subgroups and enables comparisons between them [74].

3.2.2.2 Data analysis - Coding and tabulations

Integrated coding was used as the main approach to analyze the translated transcripts. The deductive framework and categories were developed during the SLR, and also inspired by scientific literature identified during the work with the background chapter, and as such they are concept driven.

When the initial inductive coding approach was utilized in the analysis, it was based on the ability to categorize the interview subjects' perceived information security risk picture from the transcripts. This entailed meaning coding based on the empirical data in the transcripts as the concepts emerged, and as such was data driven. The coding process was conducted using HyperRESEARCH Qualitative Research Tool Ver 4.5.4 software. The meaning codes with clear relations where then grouped together to form compiled codes to reduce the overall number of inductive codes. At this stage, the relevance of the data was continuously reviewed regarding the RQs, and at each iteration some information was deemed irrelevant and consequently omitted. After the inductive coding was completed, the data from the compiled codes was clustered and condensed under the categories concerning perception of risk in the deductive framework and the identified main themes. The compiled inductive codes formed the main structure of the analysis in Section 4.2.4. Further, the result from the analysis was discussed in relation to theory in Chapter 5, where the main themes and the tabulation of compiled inductive codes in the framework constitute the structure in Section 5.2. In Section 5.3, the compiled inductive codes were compared to the deductive codes from the SLR in the established framework to form the basis for the comparative analysis.

The integrated approach ensured that the data were coded and settled into categories in the framework to describe the perception of information security within AMI. These categories enabled a comparison with the findings from the SLR, and subsequently aided in answering RQ 2 and 3.

3.2.2.3 Validity and reliability of the semi-structured interviews

In a qualitative research study, obtaining validity and reliability entail using somewhat different methods compared to quantitative research.

- **Validity**

  Validity can be divided into internal and external validity, as described earlier. The internal validity was sought to be achieved by using the acknowledged 7-stage method for SSIs from Brinkmann and Kvale in [79], and applying appropriate statistical analysis such as descriptive statistics on the structured part of the interview. The findings from the SSIs where also compared to findings from similar research studies (reviewed in Chapter 2) prior to discussing the problem statement and drawing conclusions. This approach was chosen to ensure the external validity of the findings in the study. The external validity is also affected by the generalizability, as described earlier in stage 6 *Verifying,* i.e., the chosen sampling strategy, and the use of analytical generalization concepts also sought to further strengthen the validity of the SSIs.

  A considerable threat to the overall validity of the SSI is how the participants may have been restricted in sharing information and knowledge concerning potentially sensitive subjects within critical infrastructure organizations. In a Norwegian context, the Power Contingency Regulation and §6-2 (Section 2.2.1.2) defines information that can be used to affect functions relevant to the energy supply as sensitive energy information and subject to strict regulations regarding sharing and publication. This may have caused the participants to withhold or refrain from elaborating on specific knowledge regarding risk factors in AMI. This was mitigated by refraining from probing into technical details regarding risk factors to avoid having participants revealing sensitive and classified information and to concentrate on functional descriptions.

- **Reliability**

Reliability in this context is similar to validity, described in stage 6 *Verification,* but is further elaborated here for both the structed and semi-structured part of the SSI. The evaluation of the quantitative data collected in the structured part of the interview was performed by calculating the internal consistency using the Cronbach's Alpha tests in the IBM SPSS Statistics Ver 29.0.0 software. The closed-end questions concerning ranking of risk, consequence and likelihood (see Appendix A1 - Interview Guide English, part 1, Ranking of risk elements) gave a Cronbach's alpha value of α = 0.778 for risk, α = 0.891 for consequence and α = 0.923 for likelihood. An $\alpha \geq 0.9$ indicates an excellent internal consistency according to [84], but this can also indicate redundant questions. The risk in this regard is deemed to be acceptable, as the structured part is used as a supplement to the semi-structured part. Further, $\alpha \geq 0.8$ and $\alpha \geq 0.7$ implies a good and an acceptable internal consistency, respectively, according to [84]. Further, to test if there are statistically significant differences between the different organizational levels, a one-way analysis of variance (ANOVA) was conducted using IBM SPSS Statistics. The ranking of risk, likelihood and consequences based on the 7 incidents were tested on the different organizational levels (strategic, tactical and operational) with the result tabulated in Table 3.7 below.

		N	MEAN	SD	P/F/F-critical
Risk	Strategic	10	2,63	0,21	0.11/2.39/3.40
	Tactical	10	2,95	0,27	
	Operational	7	2,29	0,34	
Consequence	Strategic	10	3,26	0,29	0.74/0.30/3.40
	Tactical	10	3,08	0,54	
	Operational	7	3,31	0,47	
Likelihood	Strategic	10	2,45	0,33	0.76/0.28/3.40
	Tactical	10	2,73	0,33	
	Operational	7	2,43	0,30	

Table 3.7 One-way ANOVA test

Table 3.7 shows that perceptions of risk, consequence and likelihood all have a p > 0,05 with F values within F-critical. Based on this, the study does not find any difference between the organizational levels.

In terms of the overall SSI and the semi-structured part, Brinkmann and Kvale describe reliability in qualitative research as the degree of trustworthiness and consistency of the methods used and the findings obtained [79]. Using SSIs as a method, reliability concerns both the interviews themselves, the transcriptions and the analysis conducted. To ensure reliability in the interview setting, the study strived to use neutral questions to avoid bias by influencing the subjects' responses. A combination of close-ended and open-ended questions were used, with flexible follow-up questions prepared in advance. To further enhance reliability, all interviews were recorded and transcribed as described in stage 3 and 4 and finalized before conducting data analysis. In the analysis of the data, Leedy in [74] describes how expectations and bias from a single researcher can

affect the codes assigned, and thus contaminate the reliability and affect the interrater reliability[36]. This was mitigated by coding the data from the semi-structured part individually between both researchers. However, enhanced interrater reliability could have been achieved by utilizing more than two individuals to assist in the coding process. By increasing the number, the study could have better assessed the consistency in the coding, and thus better documented the reliability of the coding scheme. However, due to time constraints, this was not a feasible option. Another element that could potentially affect the reliability, is the language used in the interview setting. All interviews were conducted in Norwegian except for one conducted in English. The native transcripts were then coded using HyperRESEARCH, where both meaning codes and summaries were written in English to comply with the format of this research study. This may have led to loss of distinctions or misinterpretations; however, this was sought to be mitigated by validating the coding and summaries between the researchers.

3.2.3 RQ 3: Comparative analysis

With this question, the study sought to identify potential overlaps or divergence between the focus and information security risk factors identified in literature and the attitudes and perceptions of the stakeholders of AMI in the energy sector of Norway. By utilizing the identified information security risk factors from RQ 1 and the results from RQ 2, a comparative analysis was conducted to highlight and explore the differences. This was operationalized by comparing the compiled inductive codes from the SSI to the deductive codes from the SLR in the framework established from the SLR. The study further discussed the areas of divergence in the framework between literature and actors based on theory.

The information and findings from the comparative analysis will be summarized and presented in Section 5.3.

3.2.4 RQ 4: Addressing divergences

In this question, the study seeks to answer if potential divergence between literature and stakeholder perception of information security risks needs to be addressed and bridged. Further, it will propose methods or solutions that can aid in reducing and addressing divergence to create a more aligned focus and effort in information security work in the energy sector.

The proposed methods for addressing divergence are mainly based on an analysis of the last three questions in the SSI, revolving around the subjects' perception about potential solutions to current challenges and how roles and responsibilities can be handled in the energy sector. The methods will be summarized and discussed in Section 5.4.

3.3 Validity and reliability of the chosen methods in general

The ability to evaluate and assess the reliability and validity of the results obtained within different research designs are of crucial importance. They will reflect the level of potential errors in the results, and substantiate the methods chosen, the results and the conclusion. Within this study different approaches will be used to substantiate a credible and trustworthy research effort, and both validity and reliability will be described with the measures to increase both.

[36] Interrater reliability concerns "the extent to which two or more individuals provide identical judgements" [74, p.313]

3.3.1 Validity

Validity concerns the likelihood of meaningful, exact and dependable outcomes from the chosen approach, and how the approach can address the RQs and the defined problem area. Different measures or strategies can be applicable for different approaches. In the context of the qualitative approach, [74, p.106] describes strategies that can be applied, as opposed to internal and external validity often used in quantitative research. It argues that there are different views on the applicability of internal and external validity when conducting qualitative research, and often terms like "quality, credibility, trustworthiness, confirmability and interpretive rigor" are used instead [74, p.106]. The strategies proposed in the same chapter are: "*Extensive time in the field", "Analysis of outliers and contradictory instances", "Thick description", "Acknowledgement of personal bias", "Triangulation of data", "Respondent validation"*, and "*Feedback from others"*.

The work with the thesis was conducted over a span of eight months part time and gave the authors ample time to obtain in-depth knowledge and experience within the research area. As such, *"Extensive time in the field"* can to a certain degree be covered, where the information and knowledge obtained had time to mature and be challenged throughout the research. *"Thick description"* will be obtained by describing the situations sufficiently rich enough so that the readers are able to draw their own conclusions from the presented methodology, data and analyses. *"Acknowledgment of personal bias"* will be obtained by reflecting and describing the researcher´s own personal beliefs and attitudes, and how these can affect the observations and interpretations. *"Respondent validation"* will be obtained by letting the interviewees validate the transcripts and findings from the semi-structured interviews, and to ensure that they are sufficiently anonymized in the report.

3.3.2 Reliability

Similarly, reliability can be handled by using the same strategies as with validity. Especially "Analysis of outliers and contradictory instances", "Acknowledgment of personal bias", "Extensive time in the filed" and "Thick description" will aid in enhancing the reliability of qualitative studies. By focusing on these strategies throughout the conducted research steps, the study aimed to increase the reliability of the obtained results.

To counter the inherent human trait to look for patterns and consistency, "Analysis of outliers and contradictory instances" was used as a mindset during the collection and analysis of the data. By continuously challenging such predispositions, the study was to a greater extent forced to mature the findings by seeking out answers to such cases.

"Extensive time in the field" was to a certain extent covered by the duration of the thesis, and the ability to visit 2 different stakeholders at strategic, tactical and operational level gave the authors time with subjects within the sector.

To further enhance the reliability, the thesis focused on giving a sufficiently rich explanation with "Thick descriptions" regarding how the methods were employed within the literature review, the interviews, analysis and conclusions.

During the work with the thesis, the authors actively tried to identify any biases by self-reflection. This entailed using different methods in different stages of the research, such as during data collection and analysis/conclusion. In the collection phase, where interviews were conducted, the authors aimed at creating a form of internal consistency reliability by using different questions revolving around the same specific subject to see if

the interviewees were giving consistent answers. In the analysis phase, the authors went through several iterations of interpreting the data collected in the analysis, where different methods for representation were tested to determine which of them could present the findings in the most holistic and objective manner.

3.4 Ethical considerations

In research, most ethical aspects involves protection from harm, informed consent of participation, right to privacy and the researcher's academic integrity and honesty [74].

During the initial work with this research study, the authors studied the NSD guidelines for handling of data and PII in relation to academic research, concerning imposed compliance requirements. NSD further referred to the Norwegian Personal Data Act, where the requirements for handling, storing and processing of PII related data are explicitly explained. According to the Act, all research that entails processing, storing or otherwise handling PII, are required to apply to the relevant authority prior to collecting data. This study subsequently applied to NSD prior to starting the interview phase; the approval is attached in Appendix C.

The invitation to the interview including the informed consent form was specifically formed based on the ethical aspects, and is attached in Appendix B. It included information about the study, how PII is handled, how the right to privacy is adhered to, and that the study was based on voluntary participation. The informed consent form was reviewed in person with each participant during the start of each interview session in order to resolve potential issues the subjects might have regarding participation, data handling or PII. The form was not signed in paper, but the consent was explicitly asked for and the answer was subsequently recorded digitally through Teams and system audio.

The study aggregates a significant amount of data and information regarding a critical infrastructure, and thus may contribute to highlighting vulnerabilities and potential exploits for malicious actors. However, the level of detail is sought to be held at a functional level, not describing the specific technical and organizational challenges in detail.

All data collected through interviews, such as transcriptions, notes, and the research report were sanitized to anonymize the subjects and their respective organization prior to publication/submission. All data and information concerning the research study were stored according to relevant regulations regarding PII.

4 Data analysis

The chapter will first present the findings from the SLR and contributes to answering RQ1. The SLR will identify the most prevalent vulnerabilities, threats, consequences, their likelihood and assessment of risks according to the identified body of literature. The findings are presented in summaries where content is compared, and their limitations described. The findings are also presented in tabulated form according to the classification scheme in the SLR to provide an overview of the findings. Secondly, the SSI is presented and analyzed, and contributes to answering RQ2. The SSI will identify the participants' perception of vulnerabilities, threats, consequences, their likelihood and assessment of risks. The findings from the SSI are presented as summaries of the compiled inductive codes.

4.1 Data analysis literature review and theoretical framework

In this section the study will give an overview of the current state and focus of information security in AMI according to the literature. The aim is to give a structured synthesis and provide insights and interpretations of the vulnerabilities, the threat landscape and the potential impacts from attacks.

4.1.1 Scope

The scope of the review is to give a structured overview of recent research on information security challenges within AMI. The impacts and consequences of exploits will be based on the effects on the system and its end-users, together with the extended CIA-triad (CIAPI3A). In terms of areas of focus, it will consider the complete infrastructure, from the endpoints to the management and business network of the DSO. Due to the fast pace in ICT development and the recent nation-wide deployment of AMI in Norway, the study has incorporated research conducted within the last 10 years, and excluded research conducted prior to this.

According to [20, p.6-9], CIA is what is considered the industry standard for information security, describing the utility of information. These characteristics have since been deemed inadequate to describe and catch the meaning of information security due to a limitation in scope and the pace of development in ICT. The addition of Privacy, Identification, Authentication, Authorization and Accountability to the triad provides a more holistic set of processes and distinctive characteristics that conceptualize information security of today (CIAPI3A). The characteristics will be utilized when exploring the vulnerabilities, threats and impacts regarding information security within the AMI. They will to a greater extent express the common characteristics of information and its utility as an asset to the stakeholders. Several of the above-mentioned characteristics are crucial within AMI as part of critical infrastructure, specifically from the perspectives of safety and security. But in the electrical grid, both availability and integrity are considered critical to ensure a safe and reliable distribution of power. As described in [14], the loss of integrity may lead to compromise of system functionality and false data being inserted, resulting in safety critical incidents in the grid. Similarly, the loss of availability of the system or specific parts of it, can result in interrupted or denied delivery of power, and delaying or severing the communication within the power

grid. However, from a privacy and customer point-of-view, confidentiality may to a certain extent be equally important in a data-driven society. If confidentiality of information and data within AMI is breached, privacy-related and sensitive information may be exposed or stolen.

4.1.2 Classification scheme

There exists a wide range of topics within research on critical infrastructures and the concept of SG, focusing on different aspects or technologies. The introduction, implementation and operation of AMI is such a topic, where information security is one of the researched aspects. Both the initial search and the SLR revealed a research trend focusing on one or more of the different systems and layers constituting AMI: the HW (such as the SM, the DC, the HES and MDMS), the data produced and processed (such as data from SM and DC to HES and MDMS), the communication network (such as the wired and wireless communication and the different channels used within AMI), and AMI as part of the SG and other critical infrastructures. Within the different layers, the information security vulnerabilities and challenges are often highlighted and evaluated against the potential effect on all or parts of the CIA-triad and its extended characteristics. The research effort on information security in AMI has been extensive, and many review papers have been published throughout the years. Some focus on specific security aspects, like Yaacoub et al. [85], where the security of PLC communication is evaluated, identifying vulnerabilities from the physical layer to the application layer, and how different attacks can exploit the vulnerabilities. Further, in [86] by Husnoo et al. and [87] by Reda et al. investigate False Data Injection (FDI) threats and attacks in the SG and the AMI and provide overviews of attacks and threats tied to different vulnerabilities in the system. Asri et al. in [88] analyzed the impacts of DoS and DDoS attacks in AMI, focusing on flooding attacks and firmware and software vulnerability attacks. As a last example, Bou-Harb et al. in [89] take an extensive look at the security in wireless communication infrastructure in AMI, with a specific focus on mechanisms between the end-user and DSOs in AMI.

As such, the identified research trend will, in the course of this SLR, be used as a classification scheme to structure and refine the data extraction, synthesis and write up of the review. Both the initial review and the identified research trend detail a focus on different areas in AMI, containing both similar but also aggregated and unique sets of security challenges and common and distinct attack vectors. Figure 2.5 visualizes the scope and classification scheme used in the SLR, focusing on three distinct areas or layers in AMI, listed below:

1. The distributed HW (including SM and DC)
2. The communication channels
3. AMI at system level (including HES and MDMS)

4.1.3 Definitions of the most common threats and attacks from literature

The threats and attacks described are categorized according to the layer they affect and its vulnerabilities. Similar to the information and cyber security terminology defined in Section 2.1.2, they are mainly drawn from the ISO Online Browsing Platform's Terms & Definitions[37] , the IEC Electropedia[38], and the NIST Computer Security Resource Center's

[37] https://www.iso.org/obp/ui#home
[38] https://www.electropedia.org/

glossary[39] with their accompanying standards. An important note is that an attacker can exploit several vulnerabilities and launch several types of attacks, depending on the intentions. This can entail using one attack type to lay the ground for other types of attacks to reach the intended goal, and can be illustrated by an attack tree, as described in [90] by Tøndel et al.

Denial of Service (DoS) and Distributed DoS (DDoS) concerns the prevention of authorized entities from accessing resources or services they are eligible for, or to delay the access by affecting system operations [91]. For example, an attacker may send a large number of packets (flooding) from a single system (DoS) to an entity to deny access to the AMI network. In DDoS, a similar effect is obtained by utilizing several compromised systems to flood the target entity's resources or bandwidth with packets [92]. These actions mainly affect the availability objective in information security and are considered active attacks.

Eavesdropping, sniffing and interception in the context of cyberattacks, refers to the unauthorized interception of electronic communications or emanations in order to gain access to sensitive information [93]. Sniffing is used in the context of network traffic, intercepting communication to decode protocols, and examining headers and payloads for information. These attacks can breach the confidentiality in AMI, depending on the security measures implemented (e.g., encryption), and are considered passive attacks. For the sake of simplicity in this study, eavesdropping is used as the collective term.

False Data Injection (FDI) and data modification/tampering are data-centric attacks, where FDI is a concept originally introduced in the domain of the SG. In essence it means the compromise of readings from sensors, devices and databases in the SG (e.g., SMs, PMUs), and unauthorized modification of the readings to introduce hidden errors in the state estimation of the SG [94]. Based on this definition, in the context of SG and AMI, FDIs are used as a collective term for FDIA and data modification/tampering where applicable.

Man-in-the-Middle (MitM) is a common designation for attacks that enable the attacker to be placed between two communicating nodes in a network in order to intercept and/or alter data or signaling in the communication [95]. This can be used both for active and passive attacks, depending on the attacker's intentions and main goal, e.g., eavesdropping (passive) and FDI (active).

Replay attack is defined as a form of masquerade attack, where an attacker can replay previously intercepted messages between two authorized entities to masquerade as the sender [96]. For example, in AMI the attacker could intercept an authenticated message between SMs and the AMI network, and replay the message several times, potentially causing the network to process the same data multiple times or causing the SM to take unwanted actions.

Repudiation is the denial of involvement in or responsibility for all or part of an action by one of the participants involved in the action [95]. In the context of digital communications and AMI, repudiation refers to the ability of a party to deny having sent or received a particular message or having taken a specific action. It is the opposite of nonrepudiation, which is an important aspect for maintaining the integrity of the AMI system, and for ensuring compliance with legal and regulatory requirements.

[39] https://csrc.nist.gov/glossary

Impersonation, spoofing and masquerading are variants of the same type of attack, used to gain unauthorized access to data, information or computer systems and networks. Spoofing refers to the action of disguising oneself as another entity (e.g., resource or user) [91], in order to gain access to data, resources or information. Masquerading is quite similar, but here the attacker can also hide their identity (e.g., behind a router). Impersonation is a more concrete type of spoofing, where the attacker disguises themselves as another user. For the for the sake of simplicity in this study, spoofing is used as a collective term.

Sybil attack involves creating multiple forged identities to impersonate several identities at once within a network [97]. The purpose is to achieve an undue advantage by gaining the majority of influence in the network. For example, using a single node to operate many active fake identities (Sybil identities) simultaneously within a peer-to-peer network.

Time Synchronization Attack (TSA) is a cyberattack that focuses on timing information at the physical and data link layer. These attacks can target devices and functionality, including phasor measurement units and wide area protection, monitoring, and control. Within the SG these attacks aim to disrupt the exact timing data that are essential for vital processes in the AMI, such as event location estimation and fault detection, as described in [13].

Session hijacking is an attack combining MitM and spoofing, where an attacker places themselves between two legitimate nodes after authentication exchange between the two, and subsequently impersonates as one of the legitimate nodes to control the session data exchange [98].

4.1.4 The concept of risk in SM and SG

In the context of the problem statement and the defined research questions, the main task was initially to identify the most prevalent vulnerabilities, threats, impacts and information security-related risks in AMI. Both risk and information security risk are defined in standards and described in Section 2.1; it consists of several aspects which need to be uniquely identified, as they have internal dependencies for the outcome of the calculation of and the description of risk in specific cases. Figure 4.1 visualizes the different aspects. The valuable assets will have to be identified with their exposure and interfaces (forming the attack surface), together with their inherent or inherited vulnerabilities. Further, the threats that can take advantage of the asset and their vulnerabilities will need to be identified, along with their threat actors, their motive, capacity, and intent or goal. By doing this, the impacts of an effectuated threat (an attack) can be described. The next step in calculating and defining risk is to use the function of likelihood and impacts. Based on the abovementioned elements, a systematic risk assessment can be performed.

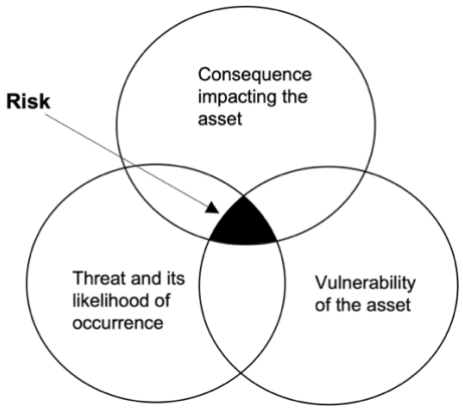


Figure 4.1 The relations between elements of risk

The comprehensive literature search revealed an abundance of academic material related to different risk concepts in AMI, SG and RQ1. The material identified and reviewed in general concerned vulnerabilities, threats and attacks, based on different classification methods [1, 99, 100], and how to handle incidents by proposing tools and frameworks and outlining how these can be used to identify, protect and detect vulnerabilities, threats and attacks [13, 101, 102]. However, a significant part of the research body does not consider or explain the aspect of likelihood when risk is described and assessed, neither by subjective nor objective analysis. This is also valid for consequences, which often are described as impact towards the defined security objectives or in overarching terms. This may be due to the fact that likelihood and consequence are to a large extent dependent on the individual system, and how its components, protocols and communication are configured [90]. The material extracted from the body of research included in the study then considers to a large extent functional descriptions of the vulnerabilities, threats and impacts to the security objectives and the SG. However, by deriving elements from the material indirectly related to the concept of likelihood, the study identified to a limited extent how likelihood is viewed in academic literature. In a Norwegian context, [42] conducts a risk assessment of a generic implementation based on regulatory requirements regarding functionality and expected operation.

In Norway, the Regulation on settlements describes the different functional requirements of the SM and AMI together with security requirements as described in Section 2.2.1.1. In addition, both the Power Contingency Regulation (Section 2.2.1.2), the Personal Data Act (Section 2.2.1.3) and the Electricity Meter Regulation (Section 2.2.1.4) further describe information security requirements for the implementation and operation of SMs and AMI. These regulations and requirements are designed so that they oblige the DSOs and AMI operators to provide an acceptable level of risk in terms of information security. However, to obtain an acceptable level of risk, the requirements need to be fulfilled and implementations continuously updated to keep up with the ICT development and the threat landscape that is continuously evolving. And as with all measures taken in terms of information security, there will always be residual risk.

4.1.5 Identified security challenges in HW

The security challenges in the HW layer of AMI are largely based on the distributed nature of the system, with its endpoints (SMs) and communication routers (DCs). It does not include the HW-layer challenges at the HES and MDMS, which are placed within the control center of the DSO or AMI operator, and thus largely inside a protected and controlled environment. However, it is also vulnerable for different types of threats,

mainly due to its connectivity to other systems in the corporate enterprise, its platform and the humans operating the system. In terms of research on the security aspects of HW identified in the SLR, there are numerous efforts conducted on the subject as part of research on information security in AMI or the SG. The findings from the SLR on HW security challenges are tabulated in Table 4.2.

4.1.5.1 The smart meters

The SM are at the boundary of AMI, placed at the endpoints close to the end-user of electricity. In a Norwegian context, they are the responsibility of the DSOs, but is also the point where their responsibilities end. From the HAN-port and outwards to the customer-domain, the responsibilities lie within each customer regarding information security and the equipment connected. The SM consists both of its HW components and its interfaces towards the end-user environment, the AMI-communication chain, and interfaces for technical maintenance. The following research has described to a varying degree vulnerabilities, threats, likelihood and impacts, and thus some of them are projecting partial risk assessments.

In [1], the different components and interfaces within a SM are described in terms of vulnerability, threats and impact, but the likelihood of threats or threat actors are not described. It focuses on how physical or cyber access to the SM with its different components and interfaces creates several possibilities for an attacker to conduct HW/FW/data interception and modification which can impact the confidentiality by interception, the integrity by modification, and the availability by interrupting or blocking commands to/from the SM. A SM is usually equipped with tampering detection mechanisms, which could potentially mitigate some of the threats described as cyber or physical access, however the work of [103] states that such mechanisms can be circumvented with sufficient resources and dedication.

Further, in [103], Liu et al. describe attacks on the SM using a threat model based on analyses of the data flows in a SM. It considers both physical and cyberattacks and divides each attack-type into attacks on data or commands. However, it considers a cyberattack on SM as the more likely of the two, where FDI attacks affecting the consumption data in the physical memory of SM are the most common type of attacks. Such attacks are often used in combination with other attack types which enable the FDI, e.g., by using DoS to exhaust the bandwidth and cause disconnection, followed by injection of malware to write to or read the physical memory of the SM. The paper does not specifically describe vulnerabilities, the impacts towards the security objectives, the likelihood of threats exploiting vulnerabilities, nor does it evaluate risk.

In [104], Al-Sammak et al. briefly describe HW-attacks in the SM, where both the physical access and the access to network interfaces can be used to affect FW, SW and stored data on the device. The paper does not specify the types of attacks which can manifest the threats, and further does not describe impacts or likelihood of threats exploiting the physical access to SM. The threats and vulnerabilities are similarly described by Bendiab et al. in [105], that in this article are linked to the compromise of confidentiality, integrity, availability and privacy. Energy theft and data theft are further described as prominent impacts to the AMI, where energy theft is considered as the most considerable challenge, due to the financial impact.

In HW, the physical access to devices gives an attacker several vectors that can be exploited. [106] describes in addition the possibilities utilizing the JTAG-interface on HW to extract both FW, hard-coded credentials and data from devices. It briefly describes

how this enables further exploitation of memory vulnerabilities to reach the intended target of FW, credentials or data in the devices. It does not consider the likelihood, nor does it give any risk descriptions of the vulnerabilities.

The work of [107] describes AMI as a cyber-physical system, and describes the physical threats to SMs based on the physical accessibility to the systems, and also describes the threat arising from an exposed supply chain. These threats may enable an attacker to affect the components in the device (replacing them with malicious components), FW and SW, and data/commands stored or sent to the device. The research does not describe the likelihood and gives only a superficial description of potential impacts in AMI as ranging from breach of privacy to cascading failures in the AMI. However, it claims the risk of HW tampering is high, both due to the vast opportunities in the supply chain, and the potential physical access to the devices in the field.

Both the SM and DC are described in [100] by Foreman et al. in terms of their attack surface, where the interfaces outwards and the physical access to the devices are considered the main surfaces for compromising the devices and their communications locally. The paper does not consider likelihood or impacts in specific, and thus it does not provide a risk evaluation of the devices or the AMI system. Similar descriptions are given in [108] and [109] in terms of vulnerabilities and threats, but Ancillotti et al. in [108] also provide a description of how trust systems can be used to identify and weigh risks, however without providing risk evaluations and assessments of the vulnerabilities and threats identified.

The work of Line et al. in [42] provides a similar description as [100] of vulnerable vectors by the physical access and the interfaces at the SM but conducts in extension an overarching risk assessment of a general implementation of AMI in the Norwegian context, based on different incidents at all levels of AMI. Threats at the HW-level are considered as targeted tampering and manipulation of HW with the intention of theft of data or affecting functionality (breaker) causing denial of power, and/or locally produced and stored data causing corrupted data or blocking/hindering measurement for financial gain. In terms of risk assessment, the likelihood of targeted attacks is described as a combination of the number of affected end-users and DSOs, and the complexity of the attack. The likelihood is deemed to increase if targeting several end-users, while increased complexity will reduce the likelihood. Similarly, the severity of consequences increases based on how extensive integrity of measurement data is affected and the number of end-users experiencing denial-of-power conditions due to triggered breaker functionality. This produces a risk matrix as tabulated in Table 4.1, where risk is considered as a function of severity of consequence and likelihood (both 5-point scales). The table shows the matrix for the identified incidents in both HW (id 1, 3-8, 14-16, 18, 20, 22-23) and system level (28-29,31). Incidents at the communication channel are not specifically assessed, and the matrix in the article also included unwanted non-malicious technical errors not assessed in this study. The colors indicate the level of risk of incidents, with black as high risk (severe consequences), grey as medium risk (unfortunate consequences), and white as low risk (no major consequences).

		Severity of consequence				
		Not serious (1)	Less serious (2)	Serious (3)	Critical (4)	Catastrophic (5)
Likelihood	Highly likely (5)					
	Very likely (4)					21
	Likely (3)	17	1, 9, 11, 19, 25	10	6, 12, 13, 22, 24, 26, 27	8, 23, 28, 29, 30, 31
	Possible (2)	2	5, 14	7		
	Unlikely (1)	16	3	4		

Table 4.1 Risk matrix AMI, adapted from [42]

In [43], both the interfaces and the physical access, and how resource constrained the distributed devices are, are considered as the vulnerability surface. This is largely based on economic and scale-of-distribution considerations but gives way to additional vulnerabilities that threats can exploit. Especially the buffer overflow is considered a significant threat exploiting the constrained nature of SMs, whereas the communication interfaces can be used to launch masquerading attacks and send malicious commands to trigger breaker functionality. Similarly, physical access can be used to interfere with the devices to affect the FW or stored data. The impacts are described as ranging from local or widespread denial-of-power, instability in the operation of SMs and theft of power. The likelihood of the threats exploiting the vulnerabilities is not considered, and the paper does not conduct risk evaluation or assessments. However, it highlights how the widespread use of the system, and the introduction of a more diverse set of system-vendors, contribute to an overall increased risk to AMI.

The identified vulnerabilities in [101] by Wei et al. are similar to those in [43] by Shokry et al., but a somewhat wider range of threats is described here, such as meter spoofing and energy fraud attacks by extracting the identification credentials from the SM, authentication attacks by extraction authentication details from SM memory, FDI attacks by injecting malicious data or FW on the SM, and DoS attacks by overwhelming the communication links or tampering with the routing tables. The impacts are described as 1) making the SM incapable of responding to requests and disconnecting the meter from the network (DoS), 2) theft of power by authentication and FDI attacks, and 3) causing instability in billing and grid operation by FDI attacks. The research does not consider the concept of likelihood regarding the vulnerabilities and threats, and thus does not conduct a risk evaluation or assessment.

In [102], the potential for follow-on attacks after a node (SM) compromise is briefly described, enabling impersonation, FDI, replay and repudiation attacks. These attacks can target the communication channels, other devices and the head-end system, creating substantial impact. However, the research does not describe the exploited vulnerabilities, how the attacks can be performed, and does not evaluate likelihood or risk in any regard.

Threat modelling and the use of STRIDE and Attack Tree is explored in [90], where Data Flow Diagrams (DFD) and STRIDE are used to identify the SM interfaces for communication and maintenance as vulnerable entry points. In addition to using Attack Trees to describe how an attacker could go about to attack identified assets, they show how threat modelling could provide a valuable input to risk assessments by identifying entry points and threats, the assets in the system, and how an attacker could attack the assets based on different paths and threats. The research identifies threats based on a specific system and specifies how evaluation of likelihood and consequence are dependent on the particular system under study, and does not provide such evaluations, nor risk assessments.

Husnoo et al. in [86] narrows the focus by conducting a survey exploring FDI threats in active distribution systems. It classifies FDI threats according to their attack targets, where AMI communication networks, SMs and the distribution control center are identified as vulnerable targets. The vulnerabilities are not explained in detail, but the discussion revolves around the physical access to devices, the use of publicly available and shared communication channels and insecure communication protocols. The threats to SMs are categorized based on their target in SMs: 1) Energy profile attacks by MitM FDI to reduce own consumption. This is done by injecting false data into the SM, but also into the least possible number of neighboring SMs to reduce the discrepancy. 2) Load profile attack by privacy attack to infer the power consumption of home appliances. This is done by extracting reactive power data, capturing the essential characteristics and enabling identification of appliances. 3) Disruption of energy consumption data attack by false load attack to reduce the energy bill. This is done by switching the load off synchronized with the sampling rate of the SM. Lastly, 4) SM energy generation data attack by short-term FDI. Here, false data is injected in the SM or at generator buses to increase the readings of generated energy. In general, FDI attacks target integrity, corrupting data at rest or in motion within SM and the communication channel. The degradation of the integrity of data can, in the long run, with sufficient volume of compromised data, impact the reliability and stability of SG by affecting operational decisions in the system. However, the article does not describe impacts in detail, nor likelihood of threats and vulnerabilities, and does not evaluate or assess risk.

4.1.5.2 The DCs

The DCs act as a bridge in the communication channels, depending on the communication architecture of the AMI. They link the SM and HES/MDMS together and support the flow of data and commands between the entities in the network. Like the SM, the DC consists of HW components and communication modules for SM and HES/MDMS communication, in addition to interfaces for technical maintenance. The following identified research works have described to a varying degree vulnerabilities, threats, likelihood and impacts, thus projecting both complete and partial risk identification or assessments.

[104], [105], [107] and [100] describe the vulnerabilities and threats to DCs as similar to SM, but also how attacks on DCs could have a potentially more extensive impact as single collectors serve as routers in the network, serving multiple SMs and the HES/MDMS.

In [42] a risk assessment is conducted for incidents also concerning DCs, where manipulation of data and functionality (breaker) are considered. It does not describe specific exploited vulnerabilities, but it is assumed as similar to that for SMs. The assessment in Table 4.1 shows that targeted manipulation of data at DC is considered a high risk, considered likely with critical severity. Similarly, the targeted manipulation of the breaker is a high-risk incident, considered likely with catastrophic severity (based on the potential to affect many end-users).

4.1.5.3 Summary of HW challenges

As a summary, the SM and DC in AMI are vulnerable to a variety of threats that can impact the security objectives, but with limited description of likelihood of threats and attacks exploiting vulnerabilities, except for one article conducting a risk assessment on a generic implementation in a Norwegian context. The identified security challenges of HW are tabulated in Table 4.2:

Vulnerabilities	**Threats**		**Attack descriptions**	**Impact towards CIAPI3A objectives**	**Impact towards AMI**	**Likelihood description**	**Risk evaluation or description**
Not described in specific:	Not described in specific:	Jamming (DoS):[108]	Not described in specific for threats: [43] [101]	Not described in specific: [103] [104] [106] [108] [102] [42]	Not described in specific: [103] [104] [107] [108] [102] [109]	Not described in specific for threats: [1] [103] [104] [105] [106] [43] [101] [102] [109] [86]	Not described in specific for threats: [1] [103] [104] [105] [106] [107] [101] [102] [109] [86]
Accessible interfaces: [1] [103] [104] [105] [107] [100] [108] [43] [101] [90] [109] [86], [42]	HW/FW/SW/data modification: [1] [103] [104] [105] [106] [107] [43] [101] [102] [90] [109] [86] [42]	Buffer overflow (DoS):[43]	Physical tampering or connection: [1] [103] [104] [105] [100] [108] [101] [102] [90] [109] [86] [42]	Confidentiality: [1] [105] [107] [43] [101] [90] [109]	Theft of data: [1] [105] [100] [42]	(Observation) High likelihood of HW tampering due to physical access: [107]	(Proposal) The use of trust systems to determine risks and give weight to risks: [108]
Accessible internal components: [1] [100] [108] [43] [101] [109] [86] [42]	HW/FW/SW/data interception: [1] [103] [105] [100] [102]	Flooding (DoS):[101]	Remote attacks via cyber: [105]	Integrity: [1] [105] [107] [43] [101] [90] [109] [86]	Theft of power: [1] [105] [100] [43] [90] [86] [42]	Likelihood is dependent on the individual system: [90]	(Observation) Increasing numbers of connected devices increases the risk: [43]
Resource constrained HW: [103] [104] [105] [43] [101] [102]	HW/FW/SW/Data extraction: [100] [101] [103] [104] [105] [106] [107] [108] [102] [90] [109] [86]	Routing table poisoning (DoS):[101]	Interception in supply chain: [105] [106] [107]	Availability: [1] [105] [107] [43] [101] [90] [109]	Denial of power: [1] [100] [42]	[42] Likelihood for targeted attacks is described as combination of the consequence in terms of number of affected units and the complexity of the attack.	(Proposal) The importance of risk assessments to determine security posture: [43]
Design-flaws: [103] [104] [105]	Modification of commands: [103] [104] [105] [106] [107] [42]	Replay: [102] [109]	Physical tampering - connection via JTAGs: [106]	Privacy: [105] [107] [43]	Financial loss: [105] [101] [86]		(Proposal) The use of threat models (e.g., STRIDE, Attack Tree, DREAD) can be valuable input to risk assessments: [90]
Hard-coded credentials: [106] [100]	Injection of malicious code: [103] [104] [105] [107]	Repudiation: [102]	Social engineering: [107]	Identification:	Bricking of device: [1] [105] [43]		(Proposal) PRA can be used for SG: [108]

Insecure communication protocols: [106] [86]	Injection of false data (FDI): [103] [105] [106] [108] [43] [101] [102] [109] [86]	Impersonation: [102] [109]	Local wireless network attacks: [100] [108] [101]	Authentication: [107]	Unreliable operation of device: [106] [43] [101] [86] [42]		[42] Conducts risk assessment of a generic implementation in a Norwegian context, producing a risk matrix for selected incidents.
Memory errors: [106]	Eavesdropping: [105] [108]	Elevation of privileges: [90]	Serial bus attacks: [100]	Authorization:	Cascading failures: [107]		
Exposed supply chain: [107]	APT: [105]	MitM: [109] [86]	False load attack: [86]	Accountability: [109]	Loss of system visibility: [100]		
Lack of tampering mechanism: [102]	Spoofing: [106] [109]				Unreliable operation of grid: [100] [101] [86] [42]		
					Disconnection from network: [101] [42]		
					Consequences is dependent on the individual system: [90]		

Table 4.2 Identified challenges in HW layer of AMI

4.1.6 Identified security challenges in communication channels

The security challenges in the communication channels are based on the communication medium used and the technology applied in the medium. The flexible network architecture of AMI may combine a variety of communication media (wired and wireless) and technologies (e.g., PLC, DLS, fiber optics, Wi-Fi, WiMAX, cellular and ZigBee). In terms of research on the security aspects of the communication channels identified in the SLR, there are numerous works on the subject as part of research on information security in AMI or the SG, but also considerable research focusing specifically on the communication channels. The findings from the SLR on security challenges in the communication channels are tabulated in Table 4.5.

Al-Sammak et al. in [104] look at the different communication media and technologies that can be used in the AMI network, and how different technologies can be used based on the network topology. It identifies several threats that exploit the access to the medium (wired or wireless) at different points in the communication channel to affect the traffic (data and commands) and the interconnections themselves. The most common threats are identified as DoS, MitM, sniffing, malware injection, eavesdropping and masquerading. The described threats are not linked to impacts toward the security objectives or described in terms of likelihood, however the risk level for network attacks is claimed to be increasing due to the availability of attacker tools to access the different communication media. Similarly, [105] accounts for the same overarching threats, and also describes the impacts towards the security objectives and to AMI as a system, where denial-of-power is considered the most severe impact. In an overall manner, it also describes theft of power and data as considerable impacts, AMI communication as a significant attack vector and APTs as a severe threat.

The work of both [1] and [103] lacks specific descriptions of vulnerabilities in the communication channels but [1] describes the potential for vulnerability discovery by reverse engineering of components and FW. Further, it looks at the attack vectors in the communication channels and describes different threats that may intercept, inject or block data and commands in the channels, affecting the security objectives and impacting the AMI as theft of data and power, denial of power and disruption of the grid. However, it does not describe the concept of likelihood nor does it conduct a risk evaluation or assessment of risk. [103] has focused on the threat of FDI, by injecting malicious code or data, but lacks descriptions of likelihood and specific impacts towards security objectives and AMI. Further it does not detail any risk evaluation or assessment for the system.

Old and weak communication protocols are to some extent explored in [106], where vulnerabilities in DNP3, IEC 60870, ModBus can be exploited to affect the communication channel and the transferred data and commands. It argues that even if there are efforts to encrypt communication in the power industry, there are still segments utilizing old protocols with poor cryptographic and authentication protection. These vulnerabilities can be exploited by FDI and spoofing of signaling and commands. The work does categorize the impacts of threats in terms of breached security objective or consequences to AMI but does not describe risk in terms of likelihood or consequences.

The research conducted in [13] is a survey on cyber security threats in the SG, where AMI is one of the more central communication infrastructure. It classifies threats according to both security objectives breached and the network layers but does not

describe the exploited vulnerabilities specifically. The access to the wired and wireless media and the use of internet-based protocols and public solutions are examples of overarching vulnerabilities. The research proposes both Probabilistic Risk Assessments (PRAs) and Attack Graphs as tools for risk assessments, but in terms of PRA the main drawback is the lack of statistical data on events to calculate likelihood. Further, it outlines the importance of risk assessments as an important precaution for SG and AMI security, but does not provide one itself, as it does not describe likelihood or consequences in detail.

The communication channel can be used to target different elements in the distributed parts of AMI, but in [110], Wei et al. target the control center and HES/MDMS by delaying and blocking communications and commands from the control center, following its reaction to either a Load Redistribution or FDI attack. The study shows the vulnerability of the system to composite attacks carried out in tandem, and the effectiveness of targeting the control center rather than the distributed elements. The study does not describe how single attacks are enabled, but rather focuses on the composite effects. Further, it does not describe the likelihood, and does not evaluate or describe the risk of composite attacks. In contrast, [107] does not specify a target, but looks at individual types of threats and their countermeasures, specifically DoS, MitM and data integrity attacks in the communication channel. However, it does not categorize the threats into security objectives or impacts to AMI or SG, and subsequently does not perform a risk evaluation.

[100] investigates the attack surfaces in the communication channel but gives only a general overview of the surfaces presented by the wired and wireless communication technology. It also describes how inherent vulnerabilities in communication protocols (such as American National Standards Institute (ANSI) C12.22 and Smart Energy Profile (SEP) 2.0) can be leveraged to attack AMI as a system or the individual distributed devices. It does not consider likelihood or impacts in specific, and thus does not provide a risk evaluation of the devices or the AMI system. Similarly in [108], a general overview of vulnerable surfaces is given, based on the use of open network architectures and publicly available communication standards. However, it does not consider likelihood or impacts in specific, and thus does not provide a risk evaluation of the devices or the AMI system. [101] also considers the use of publicly available networks and technologies and considers the communication network as one of the two most prominent attack surfaces with inherent vulnerabilities. It gives a more detailed list of potential threats capable of exploiting the communication networks, however in an overarching manner. It also gives a brief introduction to potential impacts to security objectives and to the AMI as a system, but does not provide descriptions of likelihood, and thus does not conduct a risk evaluation or assessment based on the vulnerabilities, threats and impacts.

The ANSI C12.22 is further investigated in [61], which looked at the inherent vulnerabilities in the protocol specification, and what threats could exploit these. In general, the discovered vulnerabilities pertain to the Extended Protocol Specification for Electronic Metering (EPSEM) logon service, security service, read service and resolve service. These could be exploited to create DoS scenarios by operator lockout and routing table poisoning, FDI by routing table poisoning, masquerading to enable operator lockout, and data theft due to flawed password storage. This was conducted by sending crafted EPSEM service requests to devices on the communication channel. The study did not consider impacts to AMI as it considered the specification of the protocol and not a

specific implementation of it. Consequently, it did not provide an evaluation of likelihood and risk.

Like [100], the work of Hossain et al. in [60] also looks at the inherent vulnerabilities in protocols but looks specifically at ModBus RS-485 and its lack of basic security mechanisms such as authentication and encryption. This makes the SM and the communication architecture susceptible to injection threats and attacks with the aim of compromising the SMs. This can be obtained by sniffing, DoS (jamming), spoofing and FDI based on low-cost intelligent attacking tools. Like [100], it does not consider likelihood or impacts of the threats and vulnerabilities in specific, and thus does not evaluate or assess the risk.

Shokry et al. in [43] takes a holistic look on AMI and the security challenge by describing threats and impacts based on the different vulnerabilities that the threats are exploiting. This is conducted by considering the hardware, communication and data layer of AMI, describing vulnerabilities in the layers, the threats that can potentially exploit these, and the accompanying impacts to security objectives and AMI. In communication it considers the vulnerability in using publicly available and shared communication networks, the use of common and accessible technology, the use of insecure protocols and how the remote updating of the distributed devices can be exploited. The threats exploiting the wireless nature and vulnerabilities in protocols or security posture of the network are considered as session hijacking and MitM with FDI, with the aim of modifying commands, data, FW or SW. The impacts are briefly described in terms of security objectives and AMI; however, the study does not consider the likelihood of vulnerabilities being exploited by threats, and thus does not conduct any risk evaluation or descriptions.

False data injection attacks in the SG are explored by Reda et al. in [87], where they also describe AMI as a central hub in the communication network of the SG. It categorizes threats into attack models, attack targets and attack impacts, where the communication channels of AMI are considered a prominent target and one of the most vulnerable attack surfaces of the SG. The impacts are based on how FDI attacks can affect the SG and the power grid, and in the case of AMI and SM, the impact to the secure operation and reliability of the power grid is considered based on how injections in the communication channel can potentially cause overload scenarios and forcing the grid to work outside of acceptable limits. Further, it can cause energy theft by altering measurements, and customer privacy violations by accessing customer data. However, the study does not conduct likelihood evaluations on the described threats and vulnerabilities, and thus does not conduct risk evaluations or assessments. [86] has a similar focus on FDI, but considers all active distribution systems, and does not confine itself in the survey to the SG. The article briefly describes the vulnerabilities as the publicly available and shared communication channels and some inherent weaknesses in the used communication protocols used. The communication networks specifically, but also the SM and the distribution control center are identified as potential targets for FDI threats, as their vulnerabilities exposes data to FDI and other types of threats. In terms of the communication networks, the article further defines the data packets sent between SMs and the distribution control center, and the integrity of communication messages as targets. The threat towards the integrity of communication messages is described as MitM short-term FDI, where short-term indicates the period for disruption of integrity. The threat towards data packets in transit is described as a puppet DoS attack, where the aim is to reduce the packet delivery rate. This is done by flooding the puppet node with malicious routing requests to exhaust the bandwidth and deplete the resources of

the targeted node. The impacts of both threats are similar to those of general FDI attacks, by degrading the integrity of data in the communication channel. This can further impact the reliability and stability of AMI and the grid by affecting the operational decisions in the system. The article does not describe the likelihood in terms of the defined vulnerabilities and threats defined and does not evaluate or assess risk.

Like [87] and [86], the work of Asri et al. in [88] focuses on a single family of threats, namely DDoS. The described vulnerabilities concern faults in network protocols or applications, and in the infrastructure design itself, enabling DoS conditions. The family of DDoS threats described in the study are flooding and vulnerability attacks. Flooding is divided into SYN, UDP and ICMP flooding and exploits the vulnerabilities in communication protocols, where the aim is to drain resources from the target when responding to requests. A DDoS attack concerns vulnerabilities and faults in protocols or applications at the target network, where malicious packets exploit these in order to exhaust its resources, e.g., triggering increased CPU utilization, memory demand and general system braking. The simulated attack was a UDP flooding attack towards the DSO server simulating the MDMS (collecting metering data and handling billing) and was able to force the server to drop all packets and disconnect from the AMI-network, which further brought down the power production. This was due to the prerequisite in the simulation that the power production was directly linked to the demand and purely based on AMI data. However, this prerequisite in the simulated network is unrealistic in a Norwegian context, as production is not dependent on AMI-data to conduct load forecasting and immediate adjustments in production. The direct connection of MDMS to the internet is similarly unrealistic, however the MDMS is reliant on the HES for routing of AMI-data, which has an interface towards public infrastructure or otherwise available communication channels. It is presumed that this interface is similarly vulnerable to DDoS attacks as shown in the simulated tests in the study. Regarding risk concepts, the study does not evaluate the likelihood of the described vulnerabilities and threats, and consequently does not provide a risk evaluation or assessment.

Compared to [87] and [88] and their focus on specific threats, Benmalek et al. in [111] looks at the authentication security objective in regard to securing communication between entities in AMI and analyzes the threats seeking to breach this objective. To meet all of the security requirements described for AMI (confidentiality, integrity and availability) and provide a secure communication channel, the entities in the network needs to ensure a mutual authentication. The vulnerabilities are dependent on the implemented authentication schemes implemented; however, a general concern is the resource constrained environment of the distributed elements in AMI (such as SMs and DCs). The potential computational overhead, latency and general resource-intensive aspects of authentication puts constraints on what scheme can be selected and how it is implemented. This will again entail trade-offs between providing sufficient authentication and protection against the other types of attacks. The main types of threats affecting the authentication objective are defined as MitM (interception, FDI, replay), impersonation, insider, unknown key share and DoS (flooding and vulnerability) attacks. MitM concerns the interception of data and information (e.g., consumption data from SMs), which are then modified or replayed, before being forwarded (e.g., to HES/MDMS). Impersonation as described in the article concerns physical identity theft, e.g., in the value chain of AMI data in order to gain access to SM-data or privacy related information. Unknown key share attacks are based on how cryptographic keys are shared between communicating entities in the network and their perception of the distribution. For example, a key may be distributed amongst SMs and DC, where each SM perceives the key to be unique

between themselves and the DC, while the DC perceives the key to be shared between themselves and other entities other than the intended SM. The different threats seek to affect the authentication objective but may impact other security objectives depending on the motive, intent and resources. The impact towards AMI is not described in specific, but, based on the types of attack and how they can breach the different security objectives, it is evident that they may impact grid stability and reliability of the SG by affecting consumption data, event information, commands and the real-time requirements of AMI-applications. There is also the potential for economic impacts on both the consumer and SG-operator (e.g., DSOs) by affecting billing information (based on consumption data) and price signaling (by affecting Demand-Response (DR) management). The study does not evaluate the likelihood of threats exploiting the vulnerabilities within the different authentication schemes, and thus does not provide an assessment or evaluation of risk.

An overarching exploration of threats is conducted by Abdullah et al. in [102], where the reliance on publicly available communication technology is considered the main cause of vulnerability in the communication channel. It briefly describes what is denoted as internet-based threats, highlighting eavesdropping, FDI, MitM, DoS, replay and repudiation attacks, but does not describe how the threats can be effectuated in specific. Impacts based on the threats are similarly overarchingly described as affecting the secure and reliable operation of the power gird, how the leakage of customer data enables profiling and traffic analysis, and how congestion of the communication delays or blocks data and commands. The research does not evaluate the likelihood of the described vulnerabilities and threats described, and consequently does not provide a risk evaluation or assessment.

The use of threat modelling and the STRIDE and Attack Tree technique in [90] identifies the communication channels and the communication between SMs and between SM-HES as vulnerable entry points. Based on the entry points in the communication channels, corresponding threats that could utilize the entry points to reach the attacker goals are described with overarching immediate consequences for AMI and the security objectives. But, as the article highlights, the evaluation of likelihood and consequence are dependent on the particular system under study, and as such the article does not provide evaluations, nor risk assessments. Similarly, the work of Haider et al. in [112] use STRIDE together with DREAD for threat modelling, focusing on wireless attacks in AMI. The research identifies the vulnerable entry points for such attacks as HES, SMs, third party equipment and maintenance personnel, and maps the entry points to STRIDE categories based on the five most common wireless threats that can affect them (DoS, DDoS, MitM, de-pseudonymization and FDI attacks). Further, [112] utilizes DREAD modelling to perform a risk analysis by ranking the risk of each of the identified threats into the categories of damage, reproducibility, exploitability, affected clients and discoverability. Each threat is given a value between 1-3 in each category and based on the sum of all of its categories, each threat is then rated as low (5-7), medium (8-11) or high risk (12-15). The table is reproduced in Table 4.3. The method does not evaluate the likelihood of each threat and does not fully explain the concept of risk as a function of likelihood and impacts.

Threats	Damage potential	Reproducibility	Exploitability	Affected clients	Discoverability	Total	Ranking
DoS	2	2	2	2	2	10	Medium risk
DDoS	3	3	2	3	3	14	High risk
MitM	2	2	2	1	1	8	Medium risk
FDI	2	1	2	2	2	9	Medium risk
De-pseudonymization	2	3	1	3	1	10	Medium risk

Table 4.3 DREAD risk ratings [112]

As [90] and [112], Akkad et al. in [113] utilizes STRIDE modeling to create a threat model for the SG and AMI. The study is one of the most recent studies regarding security challenges in the SG and AMI, which explored the information security challenges in the information flow in AMI and SG communication networks. By developing a security model for an IT-enabled SG, the article identified the access points in SG, where SMs and AMI communication network were two of seven access points which were most likely to be exploited in attacks. The specific vulnerabilities of the access points were not analyzed, but the article considered the use of IP-based communications as a significant contributor, making them more susceptible to a wide array of threats. The threats identified through threat modeling were mapped to the different access points, where the mapping was based on the functionality, operations and systems present at the access point and how the threats could affect the components and interconnections at the access point. The most prevalent threats for SMs were spoofing, eavesdropping/traffic analysis/MitM, replay, data tampering, DoS and malware injection. The AMI communication was found to be vulnerable to identical threats as SMs, but and in addition to SQL injections and FDI. The impacts to security objectives were also identified, where confidentiality is affected by eavesdropping/traffic analysis/MitM, integrity by replay, data tampering, malware and SQL injection and FDI, availability by DoS, authorization and authentication by spoofing, and non-repudiation by FDI. However, the impacts on security objectives and requirements of the different identified threats identified are ultimately dependent on the intent, motive and resources of the attacker. Finally, the study does not evaluate the likelihood of the described vulnerabilities and threats described, and consequently does not provide a risk evaluation or assessment.

However, in the work of Mrabet et al. in [114], risk is indirectly assessed as a function of likelihood and consequence and produces a matrix for the identified threats is provided. The article takes the attacker's perspective when exploring potential vulnerabilities and the associated threats, and describes threats to AMI and SG in terms of the attack cycle (a version of the cyber kill-chain). The first step in the cycle is reconnaissance, where threats include traffic analysis and social engineering, which seeks to obtain credentials and map out the network under scrutiny. This stage is often followed by scanning threats, which can actively investigate the network to discover the network structures and its entities with addresses and ports available. Both reconnaissance and scanning mainly impacts the confidentiality of data and information on the network. Next, exploitation threats seek to take advantages of the discovered vulnerabilities in the AMI and the SG to gain control over networks, entities and/or data at rest or in motion. Exploitation will affect different security objectives depending on type, objective and motive of attacker: Availability is affected by DoS, jamming, MitM, popping the HMI,

masquerading. Confidentiality is affected by MitM, popping the HMI, masquerading. Integrity is affected by MitM, popping the HMI, masquerading, and integrity violations (FDI). Accountability is affected by popping the HMI and masquerading. The last step, maintaining access, further seeks to maintain a permanent access to networks or entities, data and information, and can be used to launch future attacks. Regarding security objectives, the article distinguishes between regular IT systems and SG systems in terms of prioritization, where in the SG the prioritized order is availability, integrity, accountability and confidentiality. Thus, breach of availability is defined to have a high severity, while breach of confidentiality and privacy is deemed to have a low severity or consequence. Likewise, the likelihood of each attack is defined based on the attack complexity and the exposure of the vulnerability/attack vector. As an example, the Stuxnet is described as having a high degree of complexity and requires significant resources to execute, thus it is deemed to have a low likelihood of being performed. The article presents the function of likelihood and severity as a risk matrix, visualized in Table 4.4. It does not necessarily discriminate between different systems and entities in the SG when describing vulnerabilities and threats, but based on the high-level description of them, they are considered valid within the AMI communication channels, and to some extent the HW in the network such as SM and DCs.

		Severity of attack		
		Low	**Medium**	**High**
Likelihood	**High**	• Traffic analysis • Privacy violations		• Virus, worms, trojans • DoS • Popping the HMI
	Medium	• Social engineering • Scanning	• MitM	• Backdoor • Jamming • Masquerading
	Low			• Replay

Table 4.4 Likelihood and severity matrix of threats [114]

Similar to [114], the work of Line et al. in [42] conducts a risk assessment using risk as a function of likelihood and severity of consequence of specific incidents. However, the article does not specifically describe incidents for communication channel, and as such produces a risk matrix for HW and system level incidents as tabulated in Table 4.1. In terms of vulnerabilities, the incidents and scenarios described in the study utilize different communication technologies but do not describe the specific vulnerabilities within those threats could exploit. On a general level, the study mentions how the use of commercial devices and the interconnectedness makes AMI vulnerable to regular ICT- or internet-related threats, and how 3rd party communication infrastructure makes AMI vulnerable to attacks on this party. The threats described as targeting communication are both targeted (DoS, malware, eavesdropping, traffic analysis, interception and manipulation of data) and non-targeted (DoS, malware), but only exemplified relevant threats in each category are provided and the operationalization of the threats is not described. Targeted attacks in this regard are considered as either physical or remotely conducted through interconnections, but with some types requiring specific knowledge and competence on the targeted system. The non-targeted attacks concern regular ICT threats, caused by both malware and automated tools with a variety of motives, but not necessarily with the intention of affecting AMI. In relation to impacts of attacks, they are briefly described based on the examples of both categories of attacks: How DoS conditions (e.g, by malware or attacks on 3rd party) may cause loss or delay of measurement data, potentially affecting settlements and grid operation. How privacy violations can be caused by eavesdropping, interception and traffic analysis of data. And lastly how manipulation of data can cause corrupt data, affecting grid operations. The

impacts on the security objectives are not specifically stated, but the article states how the protection of ICT systems revolves around securing the CIA-triad.

The reconnaissance and scanning threat step in the attack cycle described in [114] can be conducted by the use of open-source tools in the SG and AMI. This is explored by Ackley et al. in [99] where Shodan is used to find connected SG and AMI devices (SMs and DERs) on the internet by using tailored search queries. The article shows how exposure to the internet and poor security implementations make such devices vulnerable to a variety of attacks, both active and passive. By not protecting the devices from enumeration in Shodan (e.g., by using VPNs), they will be visible in the tool, and with insufficient security, an attacker can perform passive attacks as part of the reconnaissance and scanning phase or active attacks in the exploitation phase of the attack cycle. In passive attacks, the attacker may read status information (network configuration, power status and maintenance options) to obtain an overview of the device and the network. In active attacks, the attacker may change configuration settings on devices (change password, upload malicious FW/SW or inject false data) to affect their or the network's performance, such as locking the operator out or bricking the device. The impacts on the security objectives and AMI are not described specifically, but the reading of status information and changing configuration settings or injecting data can affect confidentiality, integrity and availability. The article does not describe the likelihood, impacts nor does it evaluate the risk, however it is a readily available tool with a continuously updated database of devices, making it very likely to be used by malicious actors with an intent and motivation to target the SG and AMI.

The SG-perspectives of OT, IT and AMI are explored in terms of threats and countermeasures by Kim et al. in [109], where threats to AMI and the communication channel and architecture are described, together with threats to AMI HW. The main threats in the communication channel are characterized and described superficially in terms of the security objectives they breach and how they can be implemented, as the study focuses more on the countermeasures for the different threats. The study does not evaluate the likelihood or consequences of the threats and does not provide a risk evaluation or assessment. In addition, the study does not seem to consider the integration of IT, OT and AMI and their interconnections, thus it does not describe how vulnerabilities can be inherited and the possibility for threats to influence several systems at once.

The communication technologies used in HANs and NANs are explored by Bou-Harb et al. in [89], which describes the different vulnerabilities and the associated threats within the networks. The vulnerabilities are the inherent properties of the technologies and the medium they use, which can be exploited by common threats to the AMI (spoofing, replay, DoS, MitM, traffic analysis, eavesdropping, FDI and session hijacking). The study does not consider likelihood and describes briefly impacts to both security objectives and AMI. Further, it does not evaluate or assess the risk of the different vulnerabilities and threats.

The use of Machine Learning (ML) techniques is explored by Mirzaee et al. in [115], which analyzes how Adversarial Machine Learning (AML) can be used to impact ML techniques used in AMI and the SG for attack detection, load forecasting and energy pricing. The two main classes are poison and evasion attacks, both of which aim at misleading ML algorithms used in AMI and the SG. This is done by either injecting wrong inputs or parameters or by modifying the training samples to distort the training system

or mislead the algorithm to make a wrong decision. Further, Mirzaee et al. also describe the common threats and vulnerabilities inherited from the wireless communication technologies used in AMI and the SG, and briefly discuss how the resource constrained environment of the devices in the network (e.g., SM and DCs) produces dilemmas in what security measures to implement. This is evident with the introduction of defensive ML techniques, which are resource-intensive in terms of computational and storage requirements. In a separate section, the article also considers privacy threats in AMI and the SG and defines 3 classes of threats: 1) personal information leaks, where an adversary can extract private information from network traffic, potentially leading to password or location disclosure, eavesdropping and sniffing of network packets, 2) identity theft, by impersonation, masquerading and spoofing, and 3) social engineering by phishing attacks. The impacts for both conventional attacks and privacy attacks are categorized according to the security objective they breach, whereas AML is not categorized according to security objectives, but according to the ML affected service. The article does not consider likelihood in relation to the vulnerabilities and threats described, and thus does not evaluate or assess risk.

The use of PLC as a communication channel in the SG and AMI is explored by Yaacoub et al. in [85], which aims at describing the vulnerable aspects of different PLC technologies and standards and analyzes the entailing threats. The focus lies on reviewing the technologies from a cyber security perspective, and describes threats based on signal interception, interruption and injection issues, and networking issues. However, there are no clear descriptions of the specific vulnerabilities within each technology or standard, as the article is more focused on the threats targeting the described issues and the impact they have on the security objectives defined for PLC. The impacts toward the AMI and the SG are not described in any detail, and the article does not discuss the likelihood, nor does it conduct any evaluation or assessment of risk regarding the vulnerabilities and threats.

As an outlook to future communication channels and architectures, Borgaonkar et al. in [116] analyzes the 5G security specifications (from 3GPP) in terms of security aspects affecting the use of 5G as a communication network within SG and AMI. The paper highlights the inherent properties in wireless communication as vulnerable to threats arising from fake base stations, e.g., IMSI catching, where an adversary can intercept traffic and signaling to conduct geolocation and create DoS conditions (exhaust resources on the devices caught). Further, the Mobile Edge Computing Host (MECH) with its interfaces towards the Radio Access Network (RAN) and the SG control center (such as HES) introduces vulnerabilities to the SG and AMI, as MECH is exposed to third-party applications hosted within and at risk from user plane attacks. The threats and vulnerabilities are overarchingly described, while impacts, likelihood and evaluation of risk are not considered in the article. However, the article provides a glimpse into some of the future challenges for information security in the communication infrastructure of the SG and AMI if 5G is utilized as a communication carrier.

4.1.6.1 Summary of challenges in communication channels

As a summary, the communication channels and the network infrastructure in AMI are vulnerable to a broader set of threats compared to the HW but haves similarly limited descriptions of likelihood of threats and attacks exploiting vulnerabilities. However, 2 studies, [114] and [112], conducts a limited risk assessment of the identified vulnerabilities, using the concepts of likelihood and consequence. Additionally, observations are made, and recommendations proposed on models and techniques for

evaluating likelihood and conducting risk assessments. The identified security challenges in the communication channels are tabulated in Table 4.5:

Vulnerabilities	**Threats**		**Attack descriptions**	**Impact towards CIAPI3A objectives**	**Impact towards AMI**	**Likelihood description**	**Risk evaluation or description**
Not described in specific:	Not described in specific: [100]	APT: [105]	Not described in specific for threats: [106] [110] [107] [108] [43] [101] [87] [102] [90] [112]	Not described in specific: [103] [104] [106] [100] [102] [60] [61] [112] [116] [99] [42]	Not described in specific: [103] [108] [102] [109] [60] [89] [61] [116] [113] [85] [99]	Not described in specific for threats: [1] [103] [104] [105] [106] [110] [100] [108] [43] [101] [87] [102] [109] [60] [89] [61] [115] [112] [88] [116] [111] [113] [85] [99]	Not described in specific for threats: [1] [103] [104] [105] [106] [13] [104] [110] [100] [108] [43] [101] [87] [102] [109] [60] [89] [61] [115] [88] [116] [111] [113] [85] [99]
Accessible communication interfaces: [1] [103] [104] [110] [107] [87] [112] [116] [99] [42]	FW/SW/data modification: [1] [104] [105] [106] [13] [107] [43] [90] [114] [116] [113] [99] [42]	Traffic analysis: [13] [102] [89] [115] [114] [113] [42]	Remote attacks via network: [1] [103] [104] [105] [100] [109] [60] [89] [61] [115] [88] [116] [111] [113] [85] [99] [86] [42]	Confidentiality: [1] [105] [13] [110] [107] [108] [43] [101] [87] [90] [109] [89] [115] [114] [111] [113] [85] [86]	Consequence is dependent on the individual system: [90]	Likelihood is dependent on the individual system: [90]	(Observation) Increasing numbers of connected networks increases the risk: [43]
Publicly accessible and shared communication media: [1] [103] [104] [105] [13] [110] [107] [108] [43] [101] [87] [102] [90] [109] [89] [112] [114] [88] [116] [85] [99] [86] [42]	FW/SW/data extraction: [103] [90]	Replay: [13] [107] [102] [109] [89] [115] [114] [111] [113] [85]	Interception in value chain: [1] [111]	Integrity: [1] [105] [13] [110] [107] [108] [43] [101] [87] [90] [109] [89] [115] [114] [111] [113] [85] [86]	Theft of data: [1] [105] [100] [43] [87] [90] [115] [114] [42]	(Observation) Lack of historical data and statistical examples: [13]	(Proposal) The importance of risk assessments to determine security posture: [43] [85]
Publicly available technology: [107] [110] [100] [108] [43] [101] [87] [102] [109] [89] [115] [112] [114] [116] [86] [13] [42]	FW/SW/data/signal interception: [1] [107] [43] [109] [89] [112] [114] [116] [111] [85]	Repudiation: [102] [90]	Social engineering: [13] [115] [114] [111]	Availability: [1] [105] [13] [110] [107] [108] [43] [101] [87] [90] [109] [89] [115] [114] [88] [111] [113] [85] [86]	Theft of power: [1] [105] [100] [101] [87] [115] [114] [86]	(Observation) Most attacks are of wireless nature: [112]	(Proposal) The use of threat models (e.g., STRIDE, Attack Tree, DREAD) can be valuable input to risk assessments: [90]
Insecure communication protocols: [105] [106] [13] [100] [90] [60] [89] [61] [88] [86]	Modification of commands: [103] [104] [106] [43] [90]	MitM: [1] [104] [105] [13] [110] [107] [108] [43] [101] [102] [109] [89] [115] [112] [114] [111] [113] [85] [86]	Wireless attacks: [1] [103] [104] [105] [100] [43] [109] [89] [115] [114] [116] [86]	Privacy: [105] [108] [115] [114] [111] [85]	Denial of power: [1] [105] [106] [100] [43] [101] [42]	Likelihood is a combination of attack complexity and the exposure of the target: [114]	(Observation) The availability of attacker tools increases the overall risk levels: [104]

Insecure authentication protocols/mechanisms: [104] [90] [111]	Injection of malicious code (inc malware): [104] [105] [114] [113] [85] [42]	Load drop: [13]	Coordinated attacks: [13] [110] [86] [42]	Authentication: [109] [115] [114] [111] [113] [85]	Financial loss: [105] [115] [114] [111] [86] [42]	[42] Likelihood for targeted attacks is described as combination of the consequence in terms of number of affected units and the complexity of the attack. Does not assess likelihood of incidents in the communication channel specifically.	(Proposal) PRA can be used for SG: [13] [108]
Insecure encryption protocol/mechanisms: [104]	Injection of false data (FDI): [1] [103] [104] [105] [13] [110] [107] [43] [101] [87] [102] [109] [60] [89] [61] [115] [112] [111] [113] [99] [86]	Load redistribution: [110] [87]	Insider: [43] [111] [85]	Authorization: [115] [113]	Bricking of device: [1] [105] [43]		Models risk of threats with DREAD: [112]
Insecure protocols in general: [105] [107] [43] [114] [85]	Eavesdropping: [103] [104] [13] [107] [102] [89] [115] [112] [114] [113] [85] [42]	Masquerading: [104] [105] [13] [43] [61] [115] [114]	Intercepting authentication: [114] [111]	Accountability: [109] [115] [114] [113]	Unreliable operation of communication and devices: [1] [104] [43] [101] [90] [115] [112] [114] [86] [42]		Models risk of threats as combination of likelihood and severity in risk matrix: [114]
Lack of authentication: [106]	Spoofing: [1] [104] [105] [106] [13] [43] [101] [90] [109] [60] [115] [113]	Time sync: [1] [13] [109] [114]	Spoof GPS information: [1] [13] [109] [114]		Disruption of grid: [1] [104] [110] [100] [43] [101] [115] [114] [42]		(Proposal) The use of attack graphs to identify attack paths most likely to succeed: [105] [13]
Resource constrained HW/ network: [100] [102] [90] [115] [114] [111]	Sniffing: [1] [104] [13] [109] [60] [115] [85]	Impersonation: [105] [43] [109] [115] [111]	Malware runs malicious code: [104] [105] [114] [88] [85] [42]		Cascading failure: [87]		[42] Conducts risk assessment of a generic implementation in a Norwegian context, producing a risk matrix for selected incidents. Does not assess incidents in the communication channel specifically.
Complexity of network: [100] [115] [88] [99] [86]	(D)DoS: [1] [103] [105] [110] [108] [43] [101] [102] [109] [89] [61] [115] [112] [116] [111] [113] [99] [42]	Sybil: [85]	Connected as a hub in network: [1] [104] [105] [13] [110] [107] [108] [43] [101] [102] [109] [89] [115] [112] [114] [111] [85] [86]		Loss of system visibility: [100]		

Long life-time expectancy: [100]	Jamming (DoS): [13] [60] [115] [112] [114]	Session hijacking: [43] [101] [89]	Exploiting known vulnerability in SW/OS: [114] [88] [85] [99] [42]		Unreliable operation of grid: [87] [115] [112] [114] [111] [86] [42]		
Remote updating: [43]	Flooding ((D)DoS, inc teardrop): [103] [104] [13] [107] [90] [89] [112] [114] [88]	De-pseudonymization: [101] [112]	Using bot networks: [88] [85]		Disconnection from network: [88]		
Vulnerable defensive ML techniques: [115]	Routing table poisoning: [107] [108] [43] [61] [112]	Disaggregation: [101]			Physical damage to equipment: [106]		
The IT-nature of the network: [88] [113] [99] [13]	Vulnerability exploit (DoS inc malware): [90] [88]	Latency and geolocation: [115] [116]			Real-time communication: [13] [111]		
Data-intensive nature of AMI: [88]	Wormhole (DoS): [13] [85]	ML poisoning: [115]			Balance between power generation and demand: [13] [115] [112] [114] [86] [42]		
Insufficient cyber hygiene: [99]	Blackhole (DoS): [115] [85]	ML evasion: [115]			Electricity market and price signaling: [87] [90] [115] [111] [86]		
	Sinkhole (DoS): [85]	Scanning (vulnerability, IP, ports): [114] [99]					
	Buffer overflow (DoS): [13] [114] [85]	Popping the HMI: [114]					
	Smurf (DoS): [13] [114]	False base stations: [116]					
	Puppet (DoS): [13] [115] [114] [86]						

Table 4.5 Identified challenges in the communication channels of AMI

4.1.7 Identified security challenges at system level

This area will look at the most prominent challenges at system level and within the end of the AMI-chain at HES/MDMS. Challenges at this level have potentially more far-reaching consequences with its control of the infrastructure and the distributed elements in the network. In the context of the SG and depending on how AMI is realized and implemented, shortfalls at the AMI system level could affect the whole SG, while at the same time being the one of the most vulnerable components in the SG.

The HES and MDMS are placed within the premises of the DSOs or the AMI operators, and thus haves an increased level of protection both physically and logically compared to the distributed elements of AMI. As described earlier in Section 2.1.4, the MDMS is utilized as a central module from which where other backend applications and systems fetches relevant data from. These interconnections pose potential vectors for malicious users to exploit, both remotely by cyber attackers and locally by insiders. The potential impacts arising from controlling and exploiting AMI at the system level are substantial compared to the distributed elements and may be a more attractive and effective vector to affect the CIA of the AMI, and to affect the rest of the SG.

The work of [105], [100], [101], [42] and [43] describes how the exposure of the HES/MDMS in the distribution control center and its interconnections in the corporate WAN together with the IT-nature and IP-based communication makes it vulnerable to regular internet-based threats. In addition, [105] describes briefly the threats of malware hopping between computing platforms, exploiting the same interconnections between the systems. [43] further takes into the account the possibility of insiders at the distribution control center, thus being a considerable threat. With the exception of [42], none of the research describes the concept of likelihood concerning the vulnerabilities and threats, and thus does not provide a risk evaluation or assessment.

Line et al. in [42] conducts a risk assessment using risk as a function of likelihood and severity of consequence of specific incidents, producing a risk matrix populated shown in Table 4.1. The article describes three targeted incidents at system level with the manipulation of data and breaker functionality and theft of data (cryptographic key), with a catastrophic level of severity due to the reach extent of the consequences. These can be operationalized through remote attacks exploiting the interconnections and IT-nature at system level, but also by using insiders. Insiders in this regard constitutes a formidable threat actor, which may inject malware, manipulate data, commands or control mechanisms, or provide access or information to external threat actors. As described in Section 4.1.5.1 in conjunction with Table 4.1, the article assessed the risk of the three incidents as high based on the level of severity (catastrophic due to potential number of end-users and DSOs affected) and the likelihood being assessed as likely. The likelihood is affected by both the potential number of affected users and the perceived complexity of the attack and is thus a combination of different assessments based on the authors' competence, insights into the technical details, and experience.

The threat to privacy by de-anonymization is analyzed by Tudor et al. in [117]. The work investigates how the granularity of reported consumption data and the timespan of data stored by the DSO affect the ability of an attacker to re-identify individual SMs and consumers from a large dataset of consumption traces (generated by SMs). The vulnerability lies with the increased volume of data communicated and stored at the DSOs, and the use of different frequencies in reporting, where consumption data has a

relative low frequency and grid operational data has a relative high frequency. By matching the datasets and considering the granularity of the data and the timespan of storage, it is evident that a higher granularity in consumption reporting and longer timespans for storage make it easier to re-identify the individual customer, thus making the datasets vulnerable to de-anonymization. This will impact the privacy of the individual customer as a significant amount can be identified simply based on their consumption. The impact to AMI is not discussed in specific, but a breach of privacy will most likely impact the consumers' trust in the system, and considering privacy legislation like GDPR, could cause substantial fines to the DSOs. In terms of likelihood, the article does not evaluate the likelihood concerning vulnerabilities and threats, and thus does not provide a risk evaluation or assessment.

Attacks on state estimators by corrupted SM data is explored by Husnoo et al. in [86], where FDI is performed on a closed-loop Conservation Voltage Reduction (CVR) in an unbalanced 3-phase distribution network integrated with DERs. CVRs are used in active distribution networks incorporating DERs as an efficient method for reducing distribution voltages, thus enabling energy and demand reductions for consumers while still maintaining power quality, i.e., above the minimum operating limits. The threat described in the article considers maliciously changing the SM measurement data used for CVR, to provoke incorrect CVR solutions at system level. The attack is performed by using Mixed Integer Linear Programming (MILP) to compute malicious SM measurement data which are injected into the communication and fed into the CVR, with the goal of increasing the 3-phase active power flow at a substation. The impact from the attack is a corrupted CVR solution, which increases the feeder voltage profile and the total 3-phase active power flow, in addition to voltage violations below the minimum voltage limit in some of the nodes in the grid. This can further cause breakdown in connected electrical devices. The threat is theoretically described, and the performance of the attack is simulated in a lab and is not necessary a realistic scenario. Based on this, an evaluation of likelihood and risk is out of scope for the study.

The work of Komninos et at. in [118] takes a holistic look at the SG and describes challenges that could affect the SG and AMI entities and cause impacts at the system level. Several vulnerabilities and attack vectors are analyzed in relation to HES and MDMS, where creative attacks could impact the security objectives and AMI as a system. The vulnerabilities outlined at this level revolve around how security is implemented at the distribution control center and the management systems. This includes weak platform configuration, where insufficient security policies and general poor cyber hygiene can entail excessive access rights, insufficient authentication and authorization mechanisms and weak password policies. Further, the availability of grid and system information in publicly available sources enables an adversary to passively reconnoiter and map out the system with legal means. Coupled with open-source intelligence tools such as Shodan, a vulnerability analysis can be conducted as a part of the reconnaissance phase of the attack cycle. And as HES and distribution control center are mainly IT-based networks, they are also victims of regular IT-vulnerabilities, such as SW flaws. The threats to the system are here divided based on the intentions of the attacker, such as whether they want to steal data from the server, control or take down the server, or affect the input data to the system. The main goal is either to obtain information about the system or to gain access. Stealing data can be conducted by using open-source intelligence tools and insiders to access the system by using social engineering and exploiting poor platform configuration and cyber hygiene. These steps enable further attacks to control or take down the servers, such as the injection of

malware which can modify or delete system files, conduct message fabrication and modification (e.g., Load Shedding (LS) priorities), control SM communication and functionality, and creating DoS conditions. It can also include attacks against the measurement-data from SMs at the MDMS used as input in state estimation for the grid. The threats described will impact different security objectives depending on the intent, motive and resource of the attacker, and each threat is not specifically categorized according to breach of objective. In general threats aiming at stealing data from or controlling or taking down the server will impact confidentiality, integrity, availability, authentication, and authorization. Attacks against measurements aim at affecting the integrity and availability of the data. When considering the impacts to the system, they are potentially severe and widespread due to the level of access and controllability from the control center. The article uses the FIPS 199 impact level assessment criteria, where all threats described at this level fall under the category moderate or high impact, but as mentioned earlier, depending on the motives and intentions of the attacker. Moderate is described as having a significant adverse effect on the operations, assets, or the individuals, meaning significant degradation of the ability to perform its primary functions, significant damage or financial losses, or significant harm to individuals. In the high impact category, the impacts are considered severe or catastrophic. Regarding the likelihood of threats exploiting specific vulnerabilities, the study does not evaluate or calculate likelihood, and thus does not evaluate or assess risk in any regard.

4.1.7.1 Summary of challenges at system level

The challenges at system level and within the distribution control center are more connected to how the infrastructure at the control center is realized and the interconnected nature of the network at this level. The IP-based communication between entities further adds to the challenges, making it potentially vulnerable to the vast list of internet-based threats. Similar to HW, the identified literature has very limited descriptions of likelihood of threats and attacks exploiting vulnerabilities, but with some generic observations and recommendations, applicable for all information systems, and described earlier for HW and communication channels. The identified security challenges at system level are tabulated in Table 4.6:

Vulnerabilities	Threats		Attack descriptions	Impact towards CIAPI3A objectives	Impact towards AMI	Likelihood description	Risk evaluation or description
The IT-nature at system level: [105] [100] [43] [101] [118] [42]	Injection of malicious code (inc malware): [105] [118] [42]	Injection of false data (FDI): [86] [118]	Not described in specific for threats: [100] [101]	Not described in specific: [100] [42]	Not described in specific: [101]	Not described in specific for threats: [105] [100] [43] [101] [117] [86] [118]	Not described in specific for threats: [105] [100] [43] [101] [117] [86] [118]
Insufficient security policy and cyber hygiene: [43] [118]	APT: [105]	Scanning (vulnerability, IP, ports): [118]	Remote attacks via network: [105] [43] [118] [42]	Confidentiality: [105] [43] [101] [117] [118]	Theft of data: [105] [100] [43] [117] [42]	[42] Likelihood for targeted attacks is described as combination of the consequence in terms of number of affected units and the complexity of the attack. Assesses the likelihood of manipulation of data and breaker functionality and theft of data (cryptographic key) as likely.	(Observation) Increasing numbers of connected networks increases the risk: [43]
Interconnected systems: [105] [100] [43] [101] [42]	Regular internet-based threats: [100] [43] [101] [118] [42]	Eavesdropping: [118]	Malware runs malicious code: [105] [118] [42]	Integrity: [105] [43] [86] [118]	Theft of power: [105] [100]		(Proposal) The use of attack graphs to identify attack paths most likely to succeed: [105]
Data-intensive nature of AMI: [117]	HW/SW/data modification: [43] [101] [86] [118] [42]	MitM: [118]	Insider: [43] [118] [42]	Availability: [105] [43] [118]	Denial of power: [105] [100] [43] [118] [42]		(Proposal) The importance of risk assessments to determine security posture: [43]
Distributed system state estimation: [86] [118]	Modification of commands: [105] [43] [42]	Traffic analysis: [118]	Load redistribution attack: [86]	Privacy: [117]	Disruption of grid: [100] [43] [42]		[42] Conducts risk assessment of a generic implementation in a Norwegian context, producing a risk matrix for selected incidents. Assess the risk as high for modification of data and breaker functionality and theft of data (cryptographic key)
	HW/SW/data extraction: [105] [100] [43] [117]	Replay: [118]	Exploiting known vulnerabilities in SW/OS: [118] [42]	Authentication: [118]	Trust in system: [117]		
	De-pseudonymization: [117]	(D)DoS: [118] [42]	Connected as a hub in the network: [118]	Authorization: [118]	Unreliable operation of grid e.g., LS and DR operation: [86] [118] [42]		
	Disaggregation: [117]	Impersonation: [118]	Open-source intelligence: [118]	Accountability: [118]	Loss of system visibility: [100]		

Table 4.6 Identified challenges at system level AMI

4.1.8 Summary of SLR

The SLR has given an overarching overview of the vulnerabilities, threats, impacts, and to a limited extent assessed risk to AMI. The analysis shows a considerable research effort and focus on the HW, the communication and the data within AMI.

As described in Chapter 1 and 2, AMI provides the DSO with considerable flexibility and potential to optimize the operation of the grid. This enables the reduction of margins by frequent measurements and continuous state estimations to improve the balance in the grid and in forecasting generation and distribution requirements (e.g., through better load balancing and shedding). However, the complexity and interconnectedness introduce new vulnerabilities and open up for other types of threats, where a complete overview of the systems and its assets, and the interdependencies within AMI and dependencies between other critical infrastructures can be challenging to obtain.

The findings from the different levels in AMI are described in the previous sections, but an important observation is the threat from compound and coordinated attacks. As described in [14] and found in [13], [110] and [86], threats can be realized as attacks both in the physical and the cyber domain via direct or indirect communication and connections. And can occur as single incidents or as compound, combined and highly coordinated attacks. Wei et al. in [110] specifically look at how different compound and coordinated attacks increase the efficiency and the impacts to AMI, and additionally how threats targeting the DSO control center provide more utility to the attacker compared to threats targeting the distributed elements.

4.2 Data analysis interview

4.2.1 Introduction

This chapter is organized in line with the questionnaire and the identified compiled inductive codes developed during the data analysis of the interviews. To preserve anonymity, each interviewee is referred to as participant and their organizational affiliation is referred to as the type of actor they are in AMI to preserve anonymity. The interview was combined in a structured part (questionnaire) and a semi-structured part, thus yielding both quantitative and qualitative data to be analyzed.

4.2.2 Interview demographics

A total of 27 interviews were conducted. The participants mainly consisted of representatives from DSOs (37.0%) and the regulatory authorities (22.2%). Among the participants, 10 (37.0%) were working at the strategic level, 10 (37.0%) at tactical level, and 7 (26.0%) at operational level. All participants perceived they had some knowledge of information security related to AMI, where nearly half of the participants (48.2%) perceived they had a proficient level of knowledge. An overview of the interview demographics is given in Table 4.7.

Variable		**Frequency**	**Percentage**
Actor	DSO (DSO#1-10)	10	37.0%
	AMI service and equipment vendor (AV#1-2)	2	7.4%
	Power vendor (PV#1-2)	2	7.4%
	End-user (E#1-5)	5	18.5%
	Regulatory authority (R#1-6)	6	22.2%
	Other (Industry organizations and SME - O#1-2)	2	7.4%
	Total	27	100%
Organizational level	Strategic	10	37.0%
	Tactical	10	37.0%
	Operational	7	26.0%
	Technical	0	0
	Total	27	100%
Proficiency level information security AMI	Expert (10)	1	3.7%
	Proficient (7-9)	13	48.2%
	Intermediate (4-6)	8	29.6%
	Low (1-3)	5	18.5%
	None (0)	0	0
	Total	27	100%

Table 4.7 Interview demographics

4.2.3 Structured interview

This chapter presents the results from the questionnaire distributed as the structured part of the interview. The collected data are mainly quantitative in nature and are presented through tables, while qualitative data are obtained through the semi-structured interviews. The analysis of the obtained data obtained will be conducted integrated with the analysis of the semi-structured part of the interview, where the data will be used as a supplement when applicable.

The following sections present the initial analyses of the data. The data was analyzed and tested using basic descriptive statistical methods supplied by IBM SPSS Statistics 29.0.0 software. The arithmetic Mean (M) with standard deviation (SD) was calculated to determine the degree of perceived risk, consequence and likelihood of specific

information security incidents[40]. Analyses were also conducted to compare different groups: The participants working at the different organizational levels (i.e., strategic, tactical and operational), and the participants working within different actors. The data was also analyzed and tested for internal consistency using Cronbach's alpha and variance using one-way ANOVA test, which are presented in Section 3.2.2.3.

4.2.3.1 Perception of likelihood, consequence and risk related to incidents

The participants were asked to rate the degree of risk of 7 potential information security incidents. Risk was explained as a function of the likelihood of the incident occurring and the consequences of the incident. A 5-point Likert-scale was used to rate the degree of risk and consequence: (0) Unknown, (1) Very low, (2) Low, (3) Medium, (4) High, (5) Extreme. A similar 5-point Likert-scale was used to rate the degree of likelihood: (0) Unknown, (1) Very unlikely, (2) Unlikely, (3) Possible, (4) Likely, (5) Very likely.

Based on the descriptive statistics and the calculated arithmetic mean for risk, consequence and likelihood, the study was not able to find any patterns in the responses when comparing the organizational levels and the type of actor in AMI. When comparing the ranking of risk with the variable *"Proficiency level information security in AMI",* it shows that in general participants with a perceived low level of proficiency consider the risks to be higher ($3.00 \leq M \leq 4.00$, medium) compared to the other proficiency levels ($2.00 \leq M \leq 3.00$, low). However, this pattern did not occur when comparing the ranking of consequence and likelihood with the same variable.

Further, when analyzing risk, consequence and likelihood with the entire population sample as a whole (N=27), the study was not able to identify any particular patterns and clear relations between how consequence and likelihood were rated and how they would form the rated perception of risk. Table 4.8 presents the comparison between the three, where risk by definition should be evaluated as a function of likelihood and consequence. Targeted cyberattacks are here perceived with both the highest consequence ($3.00 \leq M \leq 4.00$, medium), likelihood ($3.00 \leq M \leq 4.00$, possible) and risk ($2.00 \leq M \leq 3.00$, low).

Incident	Conseq.		Likelihood		Risk	
	M	**SD**	**M**	**SD**	**M**	**SD**
Unauthorized manipulation of data and equipment through the communication channels	**3.22**	1.188	**2.44**	1.050	**2.63**	0.884
Unauthorized access and modification of hardware and its locally stored data (equipment and components, firmware and software)	**3.11**	1.396	**2.15**	1.134	**2.56**	1.050
Inadequate/non-existing availability of data within AMI (e.g., consumption measurements, control signals, commands to units, events and alarms etc.)	**2.93**	1.174	**2.93**	1.238	**2.48**	0.893
Unauthorized access to data and information produced in the AMI (violation of data confidentiality)	**2.74**	1.059	**2.70**	1.103	**2.67**	0.961
Unauthorized modification of data and information produced in the AMI (violation of data integrity)	**3.37**	1.149	**2.44**	1.050	**2.67**	0.877
Targeted cyberattacks	**3.85**	1.134	**3.04**	1.344	**2.93**	1.269
Untargeted cyberattacks	**3.04**	1.126	**2.52**	1.087	**2.52**	0.975

Table 4.8 Comparison of consequence, likelihood and risk

[40] The incidents are based on the most prevalent vulnerabilities and threats identified in the SLR. The participants were asked to rate the degree of risk, consequence and likelihood, using a 5-point Likert-scale.

The study conducted a similar comparison with the organizational levels, comparing consequence, likelihood and risk. However, the comparison presented in Table 4.9 did not provide any significant patterns as when analyzing the population as a whole. Targeted cyberattacks are here perceived with both the highest consequence, likelihood and risks by all the organizational levels, but with different ranking. Strategic level rates the consequence as medium ($3.00 \leq M \leq 4.00$), likelihood as possible ($3.00 \leq M \leq 4.00$) and risk as low ($2.00 \leq M \leq 3.00$). Tactical level rates consequence (medium) and likelihood (possible) in a similar manner, but rates risk as medium ($3.00 \leq M \leq 4.00$). Operational level rates the consequence as high ($4.00 \leq M \leq 5.00$), likelihood as unlikely ($2.00 \leq M \leq 3.00$) and risk as low ($2.00 \leq M \leq 3.00$).

Both Table 4.8 and Table 4.9 may show that the concepts of likelihood, consequence, and risk in information security, when subjectively evaluated in different steps, may not necessarily give a consistent connection between the three. This also depends on the participants' understanding of the concept of risk as briefly explained in the introduction to the questions.

Incident	Strategic (N=10)			Tactical (N=10)			Operational (N=7)		
	Conseq.	**Likelihood**	**Risk**	**Conseq.**	**Likelihood**	**Risk**	**Conseq.**	**Likelihood**	**Risk**
Unauthorized manipulation of data and equipment through the communication channels	3.40	2.50	**2.90**	3.10	2.60	**2.90**	3.14	2.14	**1.86**
Unauthorized access and modification of hardware and its locally stored data (equipment and components, firmware and software)	3.20	2.00	**2.50**	3.30	2.40	**3.10**	2.71	2.00	**1.86**
Inadequate/non-existing availability of data within AMI (e.g., consumption measurements, control signals, commands to units, events and alarms etc.)	3.00	2.70	**2.40**	2.50	3.10	**2.80**	3.43	3.00	**2.14**
Unauthorized access to data and information produced in the AMI (violation of data confidentiality)	2.90	2.50	**2.50**	2.30	2.90	**2.90**	3.14	2.71	**2.57**
Unauthorized modification of data and information produced in the AMI (violation of data integrity)	3.30	2.40	**2.50**	3.50	2.50	**3.00**	3.29	2.43	**2.43**
Targeted cyberattacks	3.80	3.00	**2.90**	3.70	3.30	**3.30**	4.14	2.71	**2.43**
Untargeted cyberattacks	3.20	2.30	**2.50**	2.60	2.70	**2.50**	3.43	2.57	**2.57**

Table 4.9 Comparison of consequence, likelihood and risk across organizational levels

4.2.3.2 Perception of factors affecting information security in AMI

The participants were asked to rank factors that could positively affect the level of information security within AMI. A 4-point Likert-scale was used to rank how prominent the factor is: (5) Most prominent, (4) 2nd most prominent, (3) 3rd most prominent, (2) 4th most prominent and (5) 5th most prominent.

They were also asked to rank factors that could inhibit a further integration and development of AMI. A 4-point Likert-scale was used to rank the how negative the factor is: (5) Most negative, (4) 2nd most negative, (3) 3rd most negative, (2) 4th most negative, (1) 5th most negative.

Based on the descriptive statistics and the calculated arithmetic mean for factors affecting positively and negatively, the study was not able to find any particular patterns in the responses when comparing the type of actor in AMI. The study therefore analyzed the factors by comparing the different organizational levels and with the entire population sample as a whole (N=27).

Ranking of factors positively affecting security:

When analyzing the ranking of factors that could positively affect information security with the entire population sample (N=27), the study showed that standardized technical solutions is what is perceived amongst the factors to influence the security the most. Similarly, improved benefit arrangements and better cost allocation are perceived to have the least influence. The result is tabulated in Table 4.10.

Factor	M	SD
Standardized technical solutions are established	**4.07**	.874
Increased cooperation and knowledge sharing amongst the stakeholders in AMI	**3.48**	1.189
More precise guidelines and regulations are developed and implemented	**3.19**	1.210
Guidelines for deployment and integration of solutions are adopted (Best practice)	**3.07**	1.269
Benefit arrangements and better cost allocation for investments are implemented for the stakeholders in AMI	**1.19**	.483

Table 4.10 Ranking of factors positively affecting security in AMI

The study also conducted a comparison between the different organizational levels, ranking the different factors that could positively affect the level of security in AMI. The comparison showed discrepancies between some of the levels without any particular pattern. However, all levels considered benefit arrangements and better cost allocation to be the least important amongst the factors. The operational level perceived increased cooperation as the most prominent factor, whereas the strategic and tactical levels perceived standardized solutions similarly. The result is tabulated in Table 4.11.

Factor	Strategic (N=10)		Tactical (N=10)		Operational (N=7)	
	M	SD	M	SD	M	SD
Standardized technical solutions are established	**3.70**	0.823	**4.60**	0.699	**3.86**	0.900
Increased cooperation and knowledge sharing amongst the stakeholders in AMI	**3.50**	1.269	**3.10**	1.101	**4.00**	1.155
More precise guidelines and regulations are developed and implemented	**3.20**	1.317	**3.30**	1.252	**3.00**	1.155
Guidelines for deployment and integration of solutions are adopted (Best practice)	**3.50**	1.354	**2.80**	0.919	**2.86**	1.574
Benefit arrangements and better cost allocation for investments are implemented for the stakeholders in AMI	**1.10**	0.316	**1.20**	0.632	**1.29**	0.488

Table 4.11 Comparison of factors positively affecting security across levels

Ranking of factors negatively influencing information security:

When analyzing the ranking of factors that could negatively affect security with the entire population sample (N=27), the study showed that lack of knowledge is what is perceived amongst the factors to influence security the most negative. Similarly, the current distribution of roles, responsibilities and governance is perceived to have the least negative influence. The result is tabulated in Table 4.12.

Factor	M	SD
Lack of knowledge and expertise within AMI stakeholders	3.81	1.331
Costs	3.11	1.311
Immature technology	3.07	1.412
Insufficient regulations and guidelines (in terms of quality and specificity)	2.78	1.502
The current distribution of roles, responsibilities and governance within the AMI and the energy sector of Norway	2.22	1.121

Table 4.12 Ranking of factors negatively affecting security in AMI

The study also conducted a comparison between the different organizational levels, comparing the different factors that could negatively affect the level of security in AMI. The comparison showed discrepancies between some of the levels without any particular pattern. However, all levels considered lack of knowledge and expertise within AMI stakeholders to influence security most negatively amongst the factors. The result is tabulated in Table 4.13.

Factor	Strategic (N=10)		Tactical (N=10)		Operational (N=7)	
	M	SD	M	SD	M	SD
Lack of knowledge and expertise within AMI stakeholders	**4.20**	0.789	**3.30**	1.567	**4.00**	1.528
Costs	**3.00**	1.633	**3.00**	1.247	**3.43**	0.976
Immature technology	**3.40**	1.174	**3.20**	1.476	**2.43**	1.618
Insufficient regulations and guidelines (in terms of quality and specificity)	**2.60**	1.506	**3.10**	1.449	**2.57**	1.718
The current distribution of roles, responsibilities and governance within the AMI and the energy sector of Norway	**1.80**	0.789	**2.40**	1.506	**2.57**	0.787

Table 4.13 Ranking of factors negatively affecting security in AMI

4.2.4 Semi-structured interview

This chapter presents the results from the semi-structured part of the interview. The semi-structured part generates qualitative data which were analyzed using inductive meaning coding and thematic analysis, as described in Chapter 3. The relevance of the data was continually evaluated against the research questions during coding and analysis. This led to a total of 8 compiled inductive codes which form the structure of this chapter:

1) Initial perception on the concept of cyber risk
2) Cyber risk in operation of AMI
3) Cyber SA
4) Likelihood
5) Prevalent threats
6) Prevalent vulnerabilities
7) Prevalent consequences and impacts
8) Enablers and challenges

Based on the data from the categories, three main themes emerged after the analysis concerning perception of risk amongst stakeholders of AMI: *Perceptions of risk*, *influencing factors*, *and information security focus.*

The participants were asked a set of questions relating to information security and risk, with the intention of exploring their attitudes and perception of the most prevalent challenges. The questions were paired with a set of probing questions, enabling the study to also dive deeper into the answers and the participants' perception of the concepts of vulnerabilities, threats, and risks.

4.2.4.1 The initial perception of the concept of cyber risk in AMI

All participants were initially asked what they think when cyber risk in AMI is mentioned. When answering this question, the participants had different approaches to answering, providing a wide range of answers. There was no clear distinction between the actors or their organizational level in this regard. A summary of the main factors is given below:

Cyberattacks on the communication channels, distributed HW or the management systems at DSO level is highlighted by 11 of the participants initially as what they consider cyber risk to AMI is.

"Cyber risk are attacks…" was a prevalent opening theme; none of the participants evaluated likelihood of the mentioned attacks without probing questions. The focus was on the different attack vectors a malicious actor could use, such as the supply chain, the physical access to distributed HW in the infrastructure, the communication channels, and the management systems at system level.

Impacts were similarly highlighted by 16 of the participants; impacts to the power delivery to customers was the most prevalent, causing denial of power conditions. The impacts focused initially on the direct impacts within the system, such as unauthorized access to functionality, and how it could affect the services provided. One participant raised the concern that the consequence and impact dimension is not well understood, and as such causes significant uncertainty when it comes to defining risk levels and what is acceptable residual risk.

Vulnerabilities were mentioned specifically by 10 of the participants, but with varying focus. The most prevalent were the inherited vulnerabilities from the supply chain, and

the IT-nature of HES and management systems. However, the same participants did not evaluate threats that could leverage these vulnerabilities.

Threats were not mentioned specifically in the initial answers, but 2 of the respondents referred to the general heightened level of threat due to the current international security situation, and how this would also mean an increased cyber-threat level to the AMI as well. Further, one of the respondents states how the threat landscape is continuously evolving, challenging the situational awareness of the AMI actors.

Likelihood was generally not considered by any of the participants, as threats were similarly not considered.

Security objectives where only considered specifically by 2 of the participants, highlighting cyber risk as the attack on and breach of confidentiality, integrity or availability of the information system and data within AMI. Privacy of data was only mentioned by 2 different respondents, who saw breach of privacy as the other main risk to AMI beside the breaker functionality.

Attacker goals and main target were considered by 8 participants as accessing the management systems and HES at the DSO or AMI operator to control operations at the top level. This is based on the perception that the distributed elements are secure and that the IT-nature at system level with its accompanying vulnerabilities and threats makes it a more promising target with higher utility.

Risk is often considered only in terms of general attacks, vulnerabilities or impacts, and the participants do not evaluate threats or likelihood when giving their initial perception of cyber risks in AMI. As such they do not necessarily follow the common definition when evaluating cyber risk as defined in Section 2.1.

4.2.4.2 Cyber risk in operation of AMI

The operation of AMI as a system will incur risk in terms of exposed vulnerabilities, threats seeking to take advantage of the vulnerabilities, causing impacts to the system and the services it provides.

The participants were in the structured part of the interview asked to rank risk, likelihood and consequence of a set of potential incidents. The findings from the initial analyses in Section 4.2.3.1 show no particular patterns between different groups analyzed. By tabulating the ranking as shown in Table 4.14, it is clear that the low-risk perception was the dominating one. However, in each incident there were those who ranked the same incident as either high or extreme.

Incident	Very low	Low	Medium	High	Extreme	Unknown	Total
Communication channel	2	11	9	5	0	0	27
HW	4	10	8	4	1	0	27
Loss of availability	0	15	7	4	0	1	27
Loss of confidentiality	1	14	6	5	1	0	27
Loss of integrity	2	10	10	5	0	0	27
Targeted cyberattacks	1	6	7	10	1	2	27
Untargeted cyberattacks	2	14	8	1	2	0	27
Total	12	80	55	34	5	3	189

Table 4.14 Risk perception for specific incidents in AMI

The semi-structured interview provided further insights into this ranking, where the participants reflected up on risk within different elements of AMI and the system as a whole.

The distributed HW and communication channels are not mentioned by the participants as a significant risk factor as they are perceived as relatively secure. When challenged, 6 participants (from DSO, AMI-vendor and power vendor) argue that the system as implemented is secure due to the substantial assessments and the testing conducted prior to operationalizing it. This led to the detailed and thorough information security requirements as described in Section 2.2.1. However, as two participants from DSOs (DSO#7 and 8) put it, this depends on being compliant with the regulation as a minimum. And even so, there will always be residual risk which needs to be accepted or mitigated. The same 6 participants also noted that even though they consider the HW as secure, security can never be guaranteed.

In addition to being considered secure, the use of the distributed HW and communication channels as attack vectors (such as the SM) is also considered an unrealistic scenario. The resources and effort needed to obtain access are too high compared to the gain of accessing individual HW and its locally stored FW and data. The current requirements in regulation, such as the Regulation on Settlements §4-6, states that the compromise of a SM and/or its communication with HES/MDMS shall not compromise other SMs, their communication with HES/MDMS or the HES/MDMS itself. By being compliant with this requirement, the potential gain from compromising a single device is limited and as such can be considered high cost and low reward for a potential attacker.

The physical access to SM and DCs was mentioned by 10 of the participants as a risk factor, but deemed acceptable with the current mitigation measures, such as locked cabinets and other physical and logical tampering mechanisms. However, 2 participants (AMI-vendor and DSO) mentioned how the lack of safe disposal requirements and access to HW on the open market may pose a potential threat by enabling easy and low-cost vulnerability discovery on HW and FW. An adversary could obtain HW directly from the AMI-vendor or purchase used devices online to reverse engineer the devices and conduct vulnerability discovery in relative safety before engaging the network with exploits. The availability on the market was briefly tested by the researchers by searching common online marketplaces such as Finn.no (Norwegian) and Amazon.com, where two of the most common SMs in Norway were found available for sale by third parties.

The use of distributed HW and the communication channels in AMI, when considering SM and DC, are not considered a realistic or particularly suitable surface of attack, but the SM has nevertheless functionality that can be exploited by attacks at system level within the HES and MDMS of the DSO or AMI operator. The main factor contributing to an overall increased risk perception of the AMI as a system is the breaker functionality in all SMs. 19 participants from all the different actors and organizational levels mention this as one of the main contributors to increasing the risk level of AMI. However, this functionality is not seen as a particular high-risk factor looking at the individual SM and exploiting it locally at the SM or through the DC. The impact is only local to the end-users and the likelihood for HW attacks is considered low. On the other hand, when attacking the system level with the aim of controlling functionality in the infrastructure, exploiting the breaker functionality can potentially cause more widespread and severe impacts such as denial of power scenarios for large groups of end-users.

The risk level in HW and communication is also reflected in the structured interview where the mean risk is ranked low ($2 \leq M \leq 3$), which is also overall reflected in the interviews with participants regardless of organizational level or actor. However, when comparing both likelihood and consequence, the connections between the two is not necessarily reflected in the risk, as seen in Table 4.8 and Table 4.9.

AMI at system level

The most prevalent risk factors addressed by the different actors and organizational levels are the breaker functionality implemented in the SMs and the risk of theft of data. These factors can be considered impacts caused by different types of threats and are considered the risk factors with the highest consequences, but with low likelihood (unlikely).

Both are mentioned as risks connected to exploits targeting the system level and are not considered risks at the distributed level due to the limited impacts obtained by attacking SM or the communication channels. The regulatory requirements on the design of the infrastructure and the HW and how it is implemented are considered to significantly restrict the effect of compromising individual communication channels or HW, and thus offering limited payoff to potential attackers.

- **Breaker functionality**

  The breaker functionality is mentioned by 19 of the participants (from all actors and levels) as the most prominent risk at system level based on the potential severe impact a denial-of-power attack could have on the end-users and the potential financial impact to the DSOs. In terms of likelihood and consequence, the participants rate the consequence as high based on the dependency the modern end-users have on a reliable and predictive power delivery. Exploits of the breaker functionality can also be conducted at end-user level, attacking the individual SM or DC, but gaining only local impact within an NAN. Attacks at this level are thus considered unlikely and with low gain for potential attackers. The security implemented through the design of the topology and mitigative measures is considered to further restrict the impact but pending on compliance with regulatory requirements as described in Section 2.2.1. Successful breaches would then confine the attacker to the individual SM or DC, not being able to pivot into neighboring SMs or DCs or affecting their communication. The participants further describe system level access via the DSOs corporate network systems and their IT-surface as the most likely and prominent attack vector for

pivoting in to the MDMS and HES to exercise control over functionality such as the breaker. The IT-nature, the interconnectedness and IP-based communication make the corporate networks susceptible to both common internet-based threats, and targeted attacks tailored to the specific system, functionality or data within the distribution system and AMI it is targeting. However, as the consequence is perceived as high, the likelihood is inversely perceived as low. This assumes that the systems at this level are hardened and within the corporate firewalls and protective measures. 7 of the participants (DSO#4, DSO#6, DSO#7, DSO#9, O#1, R#3, R#4) further explain how the design of the management system and the separation of duties concerning control of the breaker functionality would prohibit attempts to perform mass-disconnections, both in terms of restrictions on the number of disconnections per day and at a single instance. Additionally, the system is not necessarily designed for mass-communications, where updates and commands are not broadcasted. However, 2 participants (PV#1, DSO#7) later point out how the design of the control mechanisms for the breaker functionality can vary in implementation, and that in most cases the mechanisms are SW-based. This implies the possibility to circumvent the controls logically and possibly disable restrictions in terms of mass-disconnections.

The breaker functionality in itself raises the level of risk to AMI, due to the potential severe consequences it represents, making AMI a more attractive target. Pending on the attacker resources, motives and goals, the system level can be a more feasible vector for impacting the functionality of AMI in general and the breaker in particular.

- **Theft of data - Breach of data confidentiality, integrity and availability**

Breach of the security objectives of the data within the infrastructure is similarly perceived as the other most prominent risk within AMI. However, different objectives are valued, where impacts towards the integrity of data for financial and grid operation are highlighted as the most important.

Confidentiality, integrity and availability of data can be affected by a wide range of threats mentioned by the participants, such as FDI, data extraction, eavesdropping, and traffic analysis. Table 4.15 shows how 18 different participants perceive the risk of breach of confidentiality, integrity and availability, and what they focus on in this regard. The risk to data exists both in the distributed infrastructure and the communication channels, but as for the breaker functionality, the system level is perceived as the most likely entry-point in order to maximize the utility for the attacker, causing the most severe and widespread impact.

The breach of the security objectives for data represents different impacts, where the most prominent described by the participants is the potential for financial impact by tampering with data or injecting false data in management systems at the MDMS or HES, targeting the handling of the data stored there. The interconnectedness, the integration of IT and OT and the IT-nature of the system level are mentioned as factors enabling different avenues of approach to reach the system level.

	Integrity of data			Confidentiality of data		Availability of data
Objective	Financial impact	State estimation	Other	Privacy and profiling	Big data analysis	Financial impact
Data tampering and FDI	DSO#10, DSO#3, DSO#5, AV#2, R#1, R#2 DSO#7, DSO#9, DSO#6, O#1-2, E#2-4	O#1, DSO#5	E#1, R#2			AV#2
Data extraction					DSO#3, R#5, PV#1	
Eavesdropping				DSO#4, R#1, E#1-3, DSO#2		
Traffic analysis				E#2-3		
DoS						AV#2, DSO#4, DSO#7

Table 4.15 Most prominent risks data

In terms of likelihood and consequences, the consequences are, similarly to breaker functionality, rated high, but when compared, the breaker functionality is considered to be causing more severe impacts due to the immediate physical effects. The financial impacts do not necessarily restrict themselves to the DSO and end-users, as the tampering of data at DSO or AMI operator can have the potential to affect market operations (R#2) or a reliable operation of AMI (DSO#5, O#1). However, a compliant organization should have mechanisms in place to be able to correlate data and adjust discrepancies and thus discover a breach of data integrity. In terms of privacy related challenges, a breach of confidentiality is considered to have minimal impacts as most of the participants consider the data to contain limited privacy related information. However, as pointed out by PV#1 and described in Section 2.2.1.3, consumption data within the AMI is considered PII on its own and as such needs to be protected against threats such as eavesdropping and traffic analysis. Three actors (PV#1, DSO#4 and R#3) express concern in this regard how GDPR will impact the AMI and the operators if a breach of data confidentiality occurs at system level where data is aggregated. Significant fines and a considerable financial and reputational strain on the operator could be the result.

The likelihood for successful breach at system level is in overall considered to be unlikely based on the implemented security controls and mechanisms at this level. Both the HES and MDMS are placed within the corporate network where logging, patching and updates are put into the system and regularly revised. However, several of the participants express how likelihood on a general basis can be challenging to calculate, due to both the lack of historical data (DSO#3 and E#1) and the uncertainties regarding the factors affecting the likelihood (AV#1, R#4 and R#5). They perceive it as low based on the consensus that the system has been thoroughly surveyed and audited by both external and internal organizations and considered as one of the most secure AMI-implementations in the world. The outlier in this regard is the end-users (E#1-3), who consider a successful breach at system level to be likely to very likely in the form of targeted cyberattacks. This is based on a general perception of risk towards Norwegian critical infrastructures, where the energy sector

is a prominent target for nation state actors. They perceive Norway's role as a considerable supplier of resources to Europe and a reduced threshold for conducting cyber operations to substantially increase the likelihood for attacks; it is only a matter of time before they are able to breach the system.

Summary of risks in operation of AMI

The participants perceive the overall risk to AMI both at distributed and system level as low, where the level of consequences and likelihood vary depending on the level. The perception is based on what appears to be a consensus about the initial work and audits of both the individual components and the system, creating what is perceived as one of the most secure AMI implementations.

The consequences at the distributed HW and communication channels are overall perceived as low based on the implemented security measures, with a similarly low perception on likelihood for successful attacks. It is also considered an unrealistic attack scenario due to the limited gain and potential extensive use of specialized knowledge and resources to be able to create a breach at this level.

At system level, the consequence is considered to be considerably higher due to the ability to reach the entire infrastructure below the HES and to exercise control over or affecting data and commands within the system. The IT-nature and the interconnectedness at this level also provide natural and common vectors for adversaries aiming at pivoting into the systems from the corporate WAN. However, due to being within the corporate WAN, it is also considered to be better protected and under constant scrutiny, as it is considered the most attractive target within AMI. The likelihood is nonetheless considered to be higher when compared to the distributed elements, but at the same time generally considered to be unlikely. The outliers in this regard are 3 of the end-users, who perceive the likelihood to be likely and very likely, using the argument that the Norwegian energy sector is an attractive target combined with a lowered threshold for attacks. When the consequence and likelihood is combined, the participants still consider the main risks as low, with the end-users still as outliers, considering the risk both as high and extreme.

4.2.4.3 Likelihood

The assessment of likelihood is considered by several participants as a challenging task, being bound by several uncertainties. It is also often divided into two separate assessments, looking at the likelihood for attempts and likelihood for successful attacks. Further, several participants describe how uncertainties distort and make assessments of likelihood challenging. DSO#3 and E#1 explains how the lack of historical data and statistical examples concerning threats, threat actors, attacks and consequences distort the assessment. The uncertainties in the factors affecting the likelihood are further described by AV#1, R#4 and R#5, who point at how nation state actors may pose a significant threat, as they potentially have the resources, knowledge and motive to attack the energy sector in general and AMI in specific. But as there are no clear methods to assess their capabilities and potential in e.g., targeted cyberattacks, coupled with the complexity of AMI, the likelihood of such attacks is difficult to assess.

As for cyber risk, the participants were in the structured part of the interview asked to rank the likelihood of a set of potential incidents. The findings from the initial analyses in Section 4.2.3.1 show no particular patterns between the different analyzed groups. By

tabulating the ranking as shown in Table 4.16, it is clear that the unlikely and possible likelihood perception were the dominating ones.

Incident	Very unlikely	Unlikely	Possible	Likely	Very likely	Unknown	Total
Communication channel	2	8	12	3	0	2	27
HW	5	11	5	4	0	2	27
Loss of availability	0	6	12	4	3	2	27
Loss of confidentiality	0	8	12	4	1	2	27
Loss of integrity	2	8	12	3	0	2	27
Targeted cyberattacks	0	2	13	6	3	3	27
Untargeted cyberattacks	1	10	9	5	0	2	27
Total	10	53	75	29	7	15	189

Table 4.16 Perception of likelihood for specific incidents in AMI

The likelihood for attempts is perceived as rising both on a general basis due to the pace of ICT development and changes in the threat landscape with development of new tools and capabilities, and specifically due to the current security environment in Europe as of today. 17 participants from all actors assess the likelihood for attempted attacks to increase in general, where AMI may be targeted specifically, but most prone to be affected as part of attacks towards the general energy sector of Norway. The international security situation is perceived to have lowered the threshold for cyber warfare by nation states, where some of the participants (DSO#3, DSO#7, DSO#9, R#2) state how they initially expected more incidents targeting critical societal functions as the Ukraine conflict escalated in spring 2022.

The likelihood for successful attacks is perceived differently as the participants factor in the different security mechanisms and compliance with regulatory requirements for information security in AMI and the energy sector in general.

- **The distributed HW and communication channels**

  The distributed elements are perceived as limited in potential value compared to the resources required to successfully exploit HW and communication. It is generally not considered a risk factor, with both low likelihood and consequences. Compared to the system level and its susceptibility to IT-threats, the likelihood is considered lower at the distributed HW and communication channels (DSO#1-4, DSO#6, DSO#9, O#1, AV#2, PV#2, R#2). However, there is a mixed perception on likelihood for successful attacks when participants elaborate further on the distributed elements alone (deemed unlikely by O#1-2, AV#2, PV#2, DSO#1-2, 4, 6-10; deemed in the range possible to likely by E#1-4, DSO#5, PV#1). Several participants refrain from describing the likelihood on a general basis (R#5-6), while others (R#4, AV#1, DSO#3) preferred to use the term real risk as opposed to likelihood.

  The exposure and physical availability of the distributed HW and communication channels are by 3 of the participants (PV#1, DSO#3 and 5) considered to increase the likelihood of attacks, both directly and indirectly. DSO#3 mentions that both HW and communication technologies are available on the open market, as there are no apparent safe disposal and licensed buyer requirements. This will provide ample possibilities for vulnerability discovery and attack development, allowing for

significant reconnaissance and weaponization, and thus increasing the chances of success. Similarly, PV#1 describes how publicly available information further exposes the distributed elements for reconnaissance, where the use of AI and attacker tools for aggregating information can be used to enhance and speed up the cyber kill chain. Further, DSO#5 describes how the prevalence of AMI may similarly increase the likelihood of both attempted and successful attacks. This assumes that increased use and focus on a system will lead to more exploration and attempts at breaking the different elements.

When comparing the HW and the communication channels in terms of likelihood in Table 4.16, 15 participants rate the likelihood of threats in the communication channel to be possible to likely, while only 9 rate the HW similarly. During the interviews, there were few participants (only DSO#2 and PV#2) that made a specific distinction between HW and communication in this regard.

- **AMI at system level**

The system level is generally perceived as the most attractive target within AMI. The participants identify HES, MDMS and/or the connected corporate network as part of the system level, where interconnections between the systems enable data transfer between systems handling different tasks and services.

In contrast to the distributed elements, the system level is considered a more likely target for attempts, but the general perception is still considered to be overall unlikely in terms of successful attacks. The DSOs and AMI-vendors state that they are continuously under attack, both targeted and untargeted, but most of them have been stopped at an early stage, not causing impacts to the delivery of power or to the AMI in itself. Some participants (R#1, 4-5) state that the system level to a certain extent can be considered as any other interconnected IT-system, susceptible to reconnaissance, probing and attempts for breach due to the nature of the systems and its connections. However, there were only 3 participants who described the likelihood of breach at system level as likely to very likely (E#1-3). The outliers in this regard stem from their perception of the system level being an attractive target where all connections and data are terminated, increasing the impact that a breach at this level could have. Coupled with its IT-nature, it is perceived to be susceptible to regular internet-based threats, both targeted and untargeted.

4.2.4.4 Cyber SA

All participants were asked how they assessed their SA for cyber-threats, vulnerabilities and risks, and what factors could potentially influence or change their perception.

- **Cyber SA – A joint effort**

In terms of overall cyber situational awareness, 22 of the participants (from all actors and levels) explicitly stated that they felt confident with their level of knowledge and competence. At the same time, 19 of those expressed that with the current threat environment and pace in development they were dependent on their own organization and the collaboration with others to maintain at a sufficient level, both in terms of general awareness and AMI-specific awareness of vulnerabilities and threats. Two of the participants (DSO#1 and 3) explained that it is not necessary to have the complete and detailed picture, but simply enough to be able to ask the right questions within their own organization. The remaining participants were divided

between trust towards others, such as the DSOs and regulating authorities) for providing a secure system, while a few stated their lack in AMI-specific knowledge and therefore considered it to be low. The common factor for those were engagement in management of AMI or energy sector governance at a strategical level as just one of several areas of responsibility.

The participants provided several reasons for as to why a joint effort is necessary. Firstly, AMI is considered a complex and distributed system with a mix of different infrastructure- and HW-solutions at the different levels of AMI, making asset management challenging. Further, the value chain is equally complex, with a variety of actors providing services, handling and processing data, requiring close cooperation, coordination and division of responsibilities. Lastly, the difference in resources and capabilities between the different actors and the ability to sustain information security vigilance and compliance with the regulatory requirements may create a suboptimal class divide between organizations. The smaller organizations may not be sufficiently equipped to have a persistent and sufficient focus, and rather aim for compliance and nothing more. These factors inhibit to a certain degree individual organizations and actors to obtain a complete overview of the potential vulnerabilities and threats AMI as a system is susceptible to, entailing the need for a joint effort between the actors for obtaining a more holistic and shared SA.

The participants described several factors that would affect the level of joint effort in building a shared cyber SA. One of the key factors considered by 15 of the participants is knowledge and knowledge sharing both internally and externally. By fostering internal focus and awareness groups and their ability to share the knowledge within the organization, a more specialized and directed focus could be obtained, tailored to the needs of the organization. These groups are again dependent on external collaboration and sharing of knowledge, which can be achieved using industry organizations (such as CERTs) and established fora for security related information (such as FSK[41]). A consistent perception amongst the majority of the participants is that information sharing within the AMI domain is key to enhancing the overall security for all. New knowledge and insights in how partners work with information security will help build a more complete picture and affect the SA of challenges in energy sector and AMI related information security challenges. New knowledge can be in the form of threat assessments and information on development in threat actor's capabilities, changes in the international security situation affecting the energy sector and information security, and the uncovering of missed vulnerabilities or zero-days.

Some participants (5 DSOs and 3 from regulatory) also highlight the use of external and internal audits as a tool to enhance awareness and get a snapshot of the current status within the organization. External audits can provide a refreshing point of view and aid in enhancing the focus of the individual organizations subject to regulation. Similarly, the participants pointed out how internal audits and reviews conducted on a regular basis provided a more constant focus on the security posture. If the results from audits in a suitable format can be shared, according to some of the participants (2 DSOs and 1 AMI-vendor), it will aid in building trust between the actors and further enhance the common SA and security posture.

[41] Forum for Informasjonssikkerhet i Kraftbransjen (NO), Forum for Information Security in the Power Industry (EN)

- **Cyber SA - Incidents in AMI**

In terms of specific and instant impacts to the cyber SA of the individuals, 15 participants from all actors and levels pointed out the occurrence and knowledge of incidents affecting AMI and the different stakeholders in AMI as a significant factor. Incidents would force them to re-evaluate and re-assess their knowledge and SA and focus their attention. Some of the same participants further elaborated on how the lack of incidents can reduce the focus over time and lead to a state of complacency, where simple compliance with regulation can be considered as good enough.

Few of the participants had any knowledge of incidents affecting AMI in Norway or abroad. The only concrete example considering incidents in Norway is the hacking of VOLUE[42], a company delivering a variety of services and products to DSOs and AMI-vendors. Three participants (R#1, PV#1, DSO#6) brought this up as an incident in Norway, however they were all unsure if the incident had any impacts towards AMI or its actors. In addition, several others (6 participants from all the different actors) expressed knowledge of incidents abroad affecting operation centers and SCADA-systems in the energy sector but were unsure of the details and accuracy of the events. As 2 participants (E#2 and AV#1) pointed out, incidents would not necessarily be published due to potential loss of reputation and trust.

Three other participants (O#1, E#2 and AV#1) also highlighted various academic work and events, such as hackathons and proof-of-concept experiments exploiting both HW and communication channels. 1 event featured HW found in the Norwegian implementation, where all attempted attacks were unsuccessful. The other events briefly mentioned featured equipment and systems from other countries not necessarily comparable to AMI in Norway but provided proof-of-concept for attack methodologies and vulnerabilities.

- **Cyber SA - Information security focus**

The information security focus within the different actors seemed to be affected by several factors. Several of the participants stated that it could be challenging to decide what to base the focus on.

International security situation. With the lack of incidents and cases threatening information security in AMI, a sense of complacency can occur. However, 17 of the participants explained how the current security situation in Europe and a perceived lowered threshold for nation state actors to engage in cyber operations affected how they viewed the level of risk and threat to critical infrastructure in general and the energy sector in specific. Specifically, the DSOs and AMI operators had been required by the regulatory authority to exercise increased vigilance and imposed additional measures to be prepared for an expected increase in malicious activity towards the energy sector. However, several of the same participants also stated that this increased focus had already been in place since the start of the Ukraine-conflict in 2014 and the incidents in its power grid. The lowered threshold is perceived to increase the likelihood for attempts, but most of the participants were unsure of the capabilities of such actors and the consequences they may produce. One participant (PV#1) expressed a concern about the general knowledge regarding consequences in a complex and interconnected system like AMI when the residual risk is accepted. A

[42] https://energiteknikk.net/2021/07/volue-tar-tap-pa-30-40-millioner-etter-hackerangrep/

nation state actor is assumed to have both the capabilities and resources to breach a system if needed, where the residual risk may create significant consequences not accounted for in the initial risk assessments.

The technological development and the race between attackers and defenders were also highlighted in conjunction with the international security situation. 10 of the participants pointed out how the development in attacker tools and capabilities, and the introduction of new technologies would shape their focus on information security and their perception of risk. New technologies will impact both the possibilities for the defenders to develop better and more effective solutions for protecting information and information systems, but they similarly could introduce new vulnerabilities and vectors, and thus need to be sufficiently scrutinized before implementation. Similarly, new attacker tools and methods will change the threat landscape, requiring a continuous focus and assessment of the security posture.

Collaboration and regular information exchanges between the actors is further defined as a significant driver for building up and maintaining an appropriate focus. The smaller and medium sized DSOs (such as DSO#4, DSO#9) point to collaboration between the DSOs, but also through fora and CERTs (such as KraftCERT[43]) and with the service providers. Actor collaboration is expected to enhance the actors by updating each other on challenges and solutions. One participant (R#3) mentioned such collaboration as simply word of mouth between the actors after supervision by authorities. Such low threshold collaboration and communication could aid the others in adjusting their operations and measures to be more in line with both the regulations and to reassess their posture and need for measures. Some DSOs (DSO#3, 8-9) also mentioned collaboration and information exchange towards the AMI operators and vendors both in terms of regular communication but also in requirements as a crucial element to ensure a sufficient focus on information security.

The regulatory authority (RME and NVE) contributes to the above-mentioned collaboration and information exchange by facilitating arenas for information exchange. 10 of the participants point to how the regulatory authorities' collaboration with the actors in the work with guidelines and requirements instill ownership to the challenge of securing AMI and the energy sector. By involving and communicating with the actors both during audits and in various fora, the DSOs in particular perceive the current regime as an appropriate method to control their focus. The requirements in regulations also provide a mandatory focus on their own, based on both national and international legislation and best available techniques and practices. However, several actors (R#1 and 4, PV#1, AV#1) highlight that the requirements will only provide a minimum standard for information security. Following and incorporating what the guidelines entail will provide a more adapted and secure system and organization, but this will also incur additional costs for the organization. This cost is not necessarily something the actors see the immediate effect of, as several actors (R#1, DSO#5, 6, 7 and 10) state how information security does not directly generate revenue. This can further lead to the perception that compliance is good enough. In this regard, 2 of the participants (DSO#4 and 10) call the regulations on information security a necessary evil, and as something they, to a certain extent, feel is exaggerated.

[43] KraftCERT is an independent CERT for the energy and petroleum sector, https://www.kraftcert.no/no/#om

Personal interests and company resources is further described as what drives the focus beyond compliance. 7 of the participants (R#2-3, O#2, PV#1, DSO#3, 5 and 9) state how personal interests drive several of the companies (as considered by them) in the forefront of information security in AMI and the energy sector. Two of the participants (O#2, PV#1) also state that they believe that personal interest to a larger extent than company size drives the information security focus. However, to be able to maintain the interest, the organizations need to allocate resources and personnel to the task. The larger DSOs and AMI operators thus have an advantage in this regard, as expressed by 13 of the participants. They have the resources and capabilities to both build and retain competence and a persistent focus on information security and are considered as some of the drivers. Some participants also highlight that this will also benefit the smaller organizations, as the Norwegian implementation of AMI consists of a limited set of operators and vendors, using a small selection of SMs. Any changes or updates conducted by the larger operators can then potentially trickle down to the smaller actors struggling to be level with both regulations and guidelines. Several of the smaller and medium sized DSOs (DSO#6, 8-10) also point out how they and similarly sized organizations in the energy sector have limited resources, competence or capabilities to have a persistent and sufficient focus. One actor (DSO#9) states that this is to a certain degree mitigated by creating alliances handling AMI-operations (such as the SORIA-project[44]).

Power delivery and associated functionality has traditionally been the focus of the DSOs as explained by several of the participants (PV#1, DSO#3, 8 and 10, R#4-6). This entails a focus on delivering a service (energy) coupled with the functionality to control, measure and adapt the service. In this focus, the availability of power and integrity of data are considered to be the most important, where the main objective is to make the systems work with the intended functionality to adhere to their obligation to supply energy[45].

- **Cyber SA - Information security focus within the actors**

The end-users' focus on information security in AMI as perceived by the other actors is generally explained to be low (DSO#4-5, R#1-2 and 4). The customers are focused on the power delivery and reliable and persistent energy services, however 4 participants from DSOs and regulatory authority point to a few end-users where the focus lies with privacy related matters and the threat from traffic analysis and profiling. These end-users are often other critical infrastructures concerned with how their consumption pattern and data can be aggregated to reveal sensitive information. One of the end-users (E#1) explains this general low focus amongst end-users related to lack of knowledge, accountability and perception of low impact. Actors that are not accountable for security, coupled with a perception of low impact when breached or with a low level of knowledge of the system will most likely have a low interest.

The DSOs are perceived to have a mixed focus and interest in information security amongst the participants. Some of them (DSO#2 and 5, R#2, O#2) state that they think in general the DSOs have a low focus on security in AMI, but with a divide between the distributed and the system level. DSO#2 and 5 further explain that there

[44] SORIA is the largest AMI alliance in Norway created by 29 different DSOs and currently responsible for 840.000 metering points.
[45] § 3-3 in the Energy Act of Norway.

is a naturally higher focus on the system level and the IT-based architecture, as it is considered the most prevalent vector for attacks. Although the focus is generally considered to be low, it is also assumed to be varying between the different DSOs, largely depending on the personal interests within the organizations and the allocated resources. The level of outsourcing and closeness to the operation of the systems is brought up by 3 participants (DSO#5, R#2, O#2, PV#2) as an additional factor affecting the focus, as some actors rely on their service providers to provide security and is believed to become complacent after a while.

However, almost all participants point out that the interest is present with all DSOs, enforced by choice or by regulation. A significant part of the participants (12) nevertheless state that the interest and focus is increasing, where one of the main driving forces is seen as the larger DSOs with the in-house resources, competence and interest in the subject.

The AMI vendors and operators are perceived slightly different compared to DSOs. Four participants (R#1 and 2, O#1, AV#1) point out how they are offering a service or products to be bought, and in this regard security and compliance can be seen as a competitive advantage. At the same time, the vendors have an inherent interest in protecting their products and intellectual property rights. Further, both O#1 and AV#1 state that security needs to be an inherent property of the vendors in order to meet the requirements from the DSOs and to survive in the market.

At the same time, some participants (R#1 and 3, DSO1 and 9) also point to the lack of diversity amongst HW and service vendors and operators in Norway. The small number of AMI-vendors and operators in Norway reduces the options for the DSOs and creates to some extent a vendor lock-in. However, at the same time the lack of diversity in HW and operators can make patches and updates requested or required by one DSO available to other and possibly less resource-capable DSOs. DSOs with the resources and competence to challenge and set the standard towards the vendors may lead to a trickle-down effect to other DSOs operating under the same vendor.

The different participants elaborating on the vendors and operators (DSO#1-2, 5, 8-9, O#1, AV#1-2, R#1-3) perceived a varying level of information security focus amongst the operators and vendors, but the common denominator was similar to that of DSOs, i.e, that the interest is present. Two participants (O#1 and AV#1) point out how the focus is driven by the requirements set by the customers (the DSOs) in order to comply with regulations. At the same time, one participant (DSO#8) also describes how the lack of resources and competence can to a certain degree affect the product and the level of security implemented, despite the interest and focus within the vendors and operators.

4.2.4.5 Prevalent threats

When the participants described information security risks, threats and vulnerabilities in the context of AMI and the energy sector in Norway, threat actors and their target, motivation and goal are often mentioned in the same context.

- **Threat actors**

Two prevalent threat actors are mentioned as the most likely actors with the capacity, resources and motivation to target the AMI. This can be both with the

purpose to affect AMI or as a method to gain further access or cause cascading effects into other critical infrastructures.

Nation state actors are highlighted by 17 of the participants (from all actors and levels) in the context of descriptions of threats and vulnerabilities. Several of the participants describe how the capabilities of state actors are perceived to be significant and refer to the annual Norwegian national threat evaluation stating that state actors are able to breach most systems. However, the motive and utility of breaching AMI are also pointed out to be unclear by some of the participants (DSO#9, R#5, AV#2). The AMI is not necessarily considered an attractive target (AV#2, DSO#3, O#2, R#5-6, R#1), as there may be other and less resource demanding vectors that can be utilized to affect the energy sector. However, as described by R#1, the nation state actors may choose to lay dormant and wait for increased utility than to reveal themselves and their capabilities now.

In terms of motive and goals, other participants (DSO#2-3, DSO#7, R#6, AV#1) also point out that attacks on AMI can be considered as another strategic tool for adversaries. The goal can be to affect the national security situation in Norway, and to destabilize and affect the trust in society, by attempting to or conducting successful breaches of AMI. However, most of the participants describe other vectors or parts of the energy sector, such as energy generation and production, as a more likely and attractive target in this regard, with increased utility for the attacker and more severe consequences.

Insiders or unfaithful employees are further indicated as another significant threat actor by 13 of the participants, often in conjunction with nation state actors. Several of the participants mention how nation state actors can utilize insiders (or spies as O#1 describes it) or unfaithful employees to gain foothold on the inside of DSOs' operation centers and other critical functions within the energy sector. O#1 and PV#1 highlight how this can occur both within the energy sector directly, but also within the value chain, e.g., at service providers and equipment manufacturers.

The most recent example, however not directly related to the energy sector or AMI, was described by O#1, where an alleged nation state actor had infiltrated Norwegian universities. The participant further draws the line to the energy sector and explains how this would be a potentially less resource demanding and accessible solution to gain foothold for further traversal to the intended targets. Such threat actors can also lie dormant within the organization, and then spring to life based on indicators or by command.

The motivation for insiders is indicated by 2 of the participants (PV#1, O#2) to be related to motives of financial, discontentment or political nature. Employees that are compromised or simply spear phished to act as an unconscious proxy does not necessarily have a malicious motivation, similar to employees that are threatened into compliance. Nonetheless, they can all provide a nation state actor with backdoor or inside access.

- **Threats**

Several overarching and general threats are described by the participants, where the most prominent and concrete concerns HW, SW, FW and data manipulation and tampering, and the threat from reconnaissance.

Manipulation and tampering causing impacts to the integrity objective in AMI was indicated by the participants as the most prevalent threat. This concerns affecting data in motion and at rest, but also the FW, SW and HW in operation and in the value chain.

The integrity objective is indicated by 19 of the participants as one of the most important features within AMI, as most of its current operations and functionality is based on the processing of correct and reconciled data (e.g., measurements and performance data) and signaling (e.g., commands and alerts). However, both data and signaling and the FW, SW and HW processing and storing the data and signaling are susceptible to a variety of threats targeting the integrity of the elements.

Several participants (PV#1, O#1, E#2-3) also mention how manipulation and tampering can occur in the supply chain of both vendors of FW, SW and HW, where backdoors can be integrated and HW components tampered with or swapped. Threats within the supply chain can have severe and widespread impacts if the adversaries are able to affect the mass-distribution of FW, HW and SW. Further on this, R#2 mentions specifically a concern regarding the lack of sufficient authentication between vendors and DSOs when FW is distributed. The trust between long-term partners can affect the authentication process of FW as their partnership is considered sufficient for validating the integrity of products.

Manipulation of data for financial impact is described by other participants (O#2, DSO#5 and 7, E#4, R#1) where data can be manipulated when at rest and in motion at the distributed elements, e.g., through crime-as-a-service solutions. However, this is considered to be an unlikely scenario by most participants with limited impact outside the individual end-user. However, as pointed out by R#1, if adversaries are able to affect the integrity of measurement data for larger quantities of end-users, the financial impact could be more severe for the DSO, and additionally affect the trust in the system.

The most severe and considerable threat pointed out by most of the participants (19) is the manipulation and tampering with data and commands related to functionality and the operation of the AMI. This can be obtained by several methods. The most prevalent is how access through system level attacks can give control over or enable the manipulation of the communication to the distributed elements. One participant (PV#1) describes briefly how the breaker functionality is regulated by SW-based control mechanisms at some DSOs, and further implies that this then is possible to circumvent or breach. Further, signaling between HES and the distributed elements could be intercepted and false data or commands can be injected through common MitM-attack to trigger erroneous functionality. O#1 also highlights the potential for bricking of SMs, where the breaker functionality is engaged permanently. However, the risk of this threat being successful is considered acceptably low by O#1 to not warrant immediate actions.

In addition to financial and breaker functionality impacts, manipulation and tampering may also affect the operation of AMI and the distribution network through state estimations. Two of the participants (O#1 and DSO#5) point to how the integrity of data is important for a reliable operation of the grid. By conducting false data injection at system level or within the communication channel, the DSOs can obtain an incorrect estimate of the status in the grid concerning load and end-user status, causing operational decisions to be made on the wrong basis.

Reconnaissance was considered both as a precursor to manipulation and tampering, but also a considerable threat due to the current international security situation. 12 of the participants indicate this as a considerable concern and threat, where some of the participants perceive this to some extent unintendedly being facilitated by the energy sector and authorities. This happens in the form of publicly available sources providing detailed information of the energy sector, such as overviews of infrastructure. PV#1 further points to how the use of OSINT-technologies coupled with artificial intelligence can be a considerable threat in terms of aggregating openly available information. Simple tools such as Shodan and ChatGPT can be daunting in terms of their ability to conduct reconnaissance as part of the cyber kill chain. Some participants (E#1-3, DSO#2,4 and 5) also consider traffic analysis when elaborating on the threat from reconnaissance.

Almost all participants perceive a lowered threshold for attempts, but at the same time evaluate it as unlikely for threats to successfully breach their systems. Further, some of the participants (R#4, E#2-3, PV#1) state how the use of reconnaissance and mapping of the infrastructure and systems in the energy sector lay some of the foundations for successful and targeted attacks. With the current international security situation, reconnaissance activity is perceived to most likely increase as a preparatory measure for nation state actors. This may equip them in case of a conflict or to be used as an input for strategic operations affecting the national security situation in Norway.

Traffic analysis and profiling was pointed out by some participants (E#1-3, DSO#2,4 and 5) as threat towards the confidentiality in general and the privacy in specific of the end-users. By intercepting communication and analyzing the data and signaling, a concern is that adversaries may be able to profile end-users and their operations. They highlighted the risk for other critical infrastructures of being mapped out and exposing their operations and infrastructures to adversaries employing MitM attacks and passively intercepting traffic within the communication channel.

Further, 3 of the participants (DSO#4, R#2, PV#1) also underlined such threats towards the regular end-user. An expected increase in data and the aggregation of data will increase the potential in identifying the individual user and their consumption, challenging the GDPR and privacy for the end-user. This may again cause substantial financial impacts towards the DSOs in case of a breach of privacy.

Targeted attacks are indicated by some participants (PV#1-2, AV#1, R#4-5) as considerable factors in the semi-structured interview. This threat involves highly tailored attack-methodologies, as AMI is considered a complex and distributed system, with different communication technologies and HW throughout the infrastructure. The system level with HES and MDMS is, however, considered more similar to a regular IT-system, with all the vulnerabilities and attack vectors common in IP-based networks. In this regard, the participants describe how the system level is experiencing regular attempts to breach their defenses, however they mostly appear to be untargeted and general in nature.

The participants elaborating on targeted attacks, further point out that the most likely threat actor capable of exercising targeted attacks are nation state actors. They are perceived to both have the resources, competence and knowledge to tailor methodologies and tools to be able to breach the security mechanisms in the AMI. But as 1 participant (AV#1) also underlines, there are significant uncertainties related

to their potential, consequently making it challenging to evaluate the significance of the threat and its likelihood for successful breach.

4.2.4.6 Prevalent vulnerabilities

The most prevalent vulnerabilities pointed out concerned both organizational and technical matters and different types of assets, both intangible and tangible.

- **Value chain and markets**

The value chain for HW, FW and SW in AMI consists of a few vendors and service providers, which again rely on different subcontractors with their own value chain. All actors operate in the open market, offering their services to a wide variety of alliances, AMI operators and individual DSOs.

Several participants (PV#1, R#2, DSO#8, O#1) stressed the importance of having a functional communication and to enforce control and conduct audits at their suppliers and service providers. This can be a considerable task as the value chain with all the subcontractors who represent potential vectors for attack may be stretched out across the world. The value chain in a Norwegian context is regarded as exposed in terms of few numbers of vendors and the open tender competitions required by law. Several participants (PV#1, O#1, AV#1, DSO#8, E#1-2) underline how it can be vulnerable for attempts to manipulate and tamper HW, SW and FW produced. Adversaries can address a long supply chain and target the weakest link in order to weaponize HW, SW or FW. As O#1 states it:

"We're finding it everywhere else. Why shouldn't it be possible with AMI technology?"
O#1

The low number of vendors and SM-types present in the Norwegian market is considered as a cause for both vulnerabilities and strengths. Three participants (PV#1, R#2 and DSO#8) underline how few vendors and types of SMs (3 main types) serves most of the Norwegian metering points and end-users. Attacks or incidents at any of those or their supply chains would then potentially affect a significant number of end-users. At the same time R#2 points out that the fewer vendors and providers an actor must relate to can reduce the number of potentially weak spots and reduce some of the complexity.

- **Dependence on third parties (outsourcing)**

Several of the small and medium sized DSOs have engaged in alliances or outsourced the implementation, operation or servicing of AMI. This is done to both take the strain off their organization and to focus on delivery of energy as their core task. Further, it enables them to follow the pace in development and to better ensure compliance with regulation concerning AMI. The outsourcing takes different forms, where parts or all of the data collection, processing and distribution can be handled by AMI operators and their partners. This can include inhouse solutions within the AMI operators or by using cloud solutions through an AMI operator.

Several participants (9) however indicate this dependence as a potential vulnerability, where the DSOs rely on the AMI operators and vendors to provide security. A thorough and detailed Service Level Agreements (SLA) and data processor agreement are then needed to ensure compliance with regulations, but as DSO#8-9 and O#2 put

it, the DSOs tend to be complacent after a while, and not necessarily follow up as a responsible data controller.

The outsourcing of AMI operations is not only the outsourcing of tasks but also a considerable outsourcing of competence and knowledge. DSO#6, 8 and 9 underline how this competence and knowledge which previously were retained inhouse now are lost from the DSOs, and that they are fully dependent on their providers for operation of the AMI. DSO#9 underlines how the lack of vendor diversity can make it challenging to move from one vendor to another if the quality of services is not met by the provider.

The level of outsourcing can also to a certain extent affect the focus the different DSOs have on information security and how they relate to the regulations and guidelines in this regard. R#2, O#2 and DSO#5 state that the focus may very well be linked to the level of outsourcing the DSO has taken, and thus how close they are to the everyday operation of AMI. They are still the responsible actor in terms of the value chain of data and AMI but may tend to become complacent when more and more of the AMI-related activity is outsourced.

- **Complex systems and their integration**

AMI in itself consists of a multitude of different technologies, connected to other networks at system level. The separation between IT and OT may eventually be erased, both in terms of topology and infrastructure, but also due to increased dependence on smart management and production for an optimal operation of the distribution and production network.

15 of the participants (5 DSOs, 4 regulatory, 4 end-users, 1 power vendor and 1 AMI-vendor) indicate the complexity as a vulnerability within AMI, where a system of systems creates significant challenges in obtaining a holistic overview of all the different vulnerabilities and attack vectors a threat actor could exploit. 3 of the end-users perceive it as a system that has been implemented where the operators do not necessarily know how to operate and manage it securely because of the complexity and extent of the system. This perception is based on mixed experiences with a variety of DSOs of different sizes, where the larger DSOs appear to have a sounder approach to information security and the management of the systems.

Two participants (PV#1 and AV#1) point to how the complexity and interconnectedness make it challenging for the management and servicing of the system, where erroneous or poorly performed updates and changes can create unintended backdoors or cause system errors affecting the different security objectives in AMI. Further, PV#1 also describes how the upcoming integration of IT and OT and the use of AI for optimization will change the flow of data and further complicate who stores, handles and processes the data. The optimization will entail moving information to cloud-environments, shifting data between different providers and locations, and obscure who has control or access to the data. Similarly, in terms of the data flow and its value chain, DSO#2 and 8 also points out how a long and complex value chain with the current implementation and the number of data processors and controllers make access control challenging and require stringent control with access and user management.

Several participants (AV#1, R#1, 5-6, DSO#8-9) highlight in this regard the importance of securing the system through a joint effort between all the different

stakeholders. R#1 and DSO#8 point to how the significant number and the diversity of DSOs and stakeholders coupled with a complex technological implementation create a complex system of systems where nobody has the complete picture of vulnerabilities, threats, and risks. In order to secure the system, they are dependent on each other for detailed knowledge, requiring contributions from all actors within the value chain.

- **Updateability**

ICT and its use are in constant development, where new technologies and possibilities with current solutions are put forward and put in use, both by legitimate and malicious actors. In this regard, AMI as a system containing distributed elements with a limited technical and financial lifespan needs to be built with future requirements in mind and to be updateable.

Two participants (DSO#9 and AV#1) underline how AMI and the communication channels are not necessarily built for mass-communication and distribution of updates and patches. Further, several others (DSO#1 and 9, AV#1-2, O#2) point out that when the distributed equipment is first purchased and implemented, it is largely static and with limited resources and ability to handle updates and additional functionality in terms of security mechanisms. However, as underlined by PV#2, this depends on the requirements put in by the different DSOs, AMI operators or alliances when designing the system.

Further, O#2 and DSO#9 state how updates to the distributed elements are slow due to limited bandwidth, and how it does not necessarily reach all the different SMs at all. O#2 mentions examples with SMs that are never updated due to constrained communication and the number of hops needed to reach the HW. In Denmark, investigations have shown that for a specific SM-vendor (which is also present in Norway, and one of the top 3 vendors) 0.8 to 1.0% of the SMs where never updated.

- **Technical lifespan**

The devices in the distributed elements in AMI can have a considerable lifespan compared to regular IT-systems. The energy sector is generally known for handling equipment with significant lifespan due to both cost and complexity of the systems, and thus handles legacy systems side-by-side with new technologies. The volume and pace with which the AMI-implementation was carried out in Norway incurred substantial costs both in development and implementation. To avoid constant replacements and additional costs, the lifespan was calculated based on both technical and financial predictions on future developments.

However, some of the participants (AV#1, DSO#1, E#4) are concerned that the expected lifespan of HW may be outpaced by the technological development and the threat picture. The lifecycle in terms of development, rollout and operation of AMI can be difficult to change, but vulnerabilities and new forms of threats will emerge and challenge the security of the devices. This will require a constant focus on the security posture of the distributed elements, where DSO#1 mentions the need for constant logging within the infrastructure and updates to the devices. AV#2 also points out that in some cases, depending on the design of the devices, this can also entail the need to either replace modules or the entire device at end-users, incurring substantial costs and time.

- **Knowledge and training**

  AMI as a system of systems has a complex infrastructure, long value chain and a mix of different stakeholders. In order to secure its information and information systems, both knowledge and the right competence are required.

  Some of the participants (O#1, DSO#8, R#2 and 5, PV#1-2) highlight how the lack of competence and specialized knowledge in handling and securing information and information systems is a concern within both DSOs, authorities, AMI-vendors and service providers. Without sufficient competence and understanding of vulnerabilities, threats and risks in information security, decisions may be taken on an erroneous basis and contribute to incomplete and insufficient cyber SA (e.g., regarding implementations of the requirements and guidelines).

  The energy sector has overall a focus on the delivery of energy to the end-users, where the priority has been the availability and integrity of information and energy operations for a reliable and safe generation, transmission and distribution of energy. The smaller DSOs and AMI operators are not necessarily staffed and equipped to understand and handle the requirements in relation to information security. The interest is there, either voluntarily or by regulation, but the lack of resources and competence to understand the implications is to some extent missing. DSO#9 underlines in this regard that the use of alliances and outsourcing of competence mitigates this, but they still need the right competence to set requirements and follow up on their service providers.

  O#1 and DSO#8 also underlines a general concern about the lack of available personnel with competence in information security, but specifically within DSOs, vendors and operators of AMI. The will and interest may be present, but competent personnel will always be in short demand as more systems are digitalized and grow more complex with new functionalities implemented. O#1 states how it is necessary to increase the educational effort on a national level to be able to handle the digitalization of critical infrastructure where both the buyers and the authorities lack the competence to see the implications it brings along.

4.2.4.7 Prevalent consequences and impacts

In AMI and the energy network, the different vulnerabilities and the threats exploiting them can produce a wide range of consequences, both in the digital and physical domain. However, the consequences may vary in degree and duration based on the security mechanisms and the resilience built into the system.

A few of the participants (PV#1 and E#1) highlight that there are considerable uncertainties related to the consequence and impact dimension, as the capabilities and proficiency of some threat actors are challenging to determine. Coupled with varying degree of hardening and implementation of different security mechanisms also mentioned by E#5 further contributes to complicating the picture.

- **Distributed HW and communication channel**

  Most of the participants (19) perceive the consequence at this level as low based on how the system is designed and the limited possibility to traverse between devices at SM and DC level. If the operators and DSOs are compliant with the regulation, a compromised device shall not be able to affect other devices or their communication, and as such will have limited the impact. However, if such compromises can be

automated or are caused by errors in updates or when servicing the devices, the consequence can be more severe. The limited consequences highlighted by the participants could be incidents of local theft of power by injecting false consumption data, and denial of power by manipulating commands locally at the SM or in transit in the communication channel. Similarly, theft of data from SM and through eavesdropping of communication for profiling and extraction of PII where considered, but deemed of low value, as several of the participants perceived the data to have limited PII information, if anything at all. Lastly, the blocking of commands and data were described as a consequence, where both physical tampering and logical denial or disabling of communications could render the AMI-service unavailable to the operators. This was perceived to cause minimal consequences, as the data would still be there (in the SM) and would be sent as soon as communication was restored.

- **System level**

All the participants indicate that affecting the system level will produce the most severe impact. This level with the HES and MDMS acts as the hub in AMI, where commands, data and signaling are controlled. By controlling or affecting functionality such as the breaker, denial of service-conditions can be created for potentially all customers under the HES control.

- **Physical consequences – Denial of power**

By controlling functionality at system level, an attacker can inflict what is considered the most severe consequence within AMI: Denial of power. 20 of the participants perceive this as the most severe impact to both the end-users but also the DSOs as the accountable organization in the operation of AMI. This involves exploiting the breaker within the SMs either at the SM or system level, causing either targeted or widespread impact. By additionally bricking the devices (as explained by O#1 and DSO#2), the duration of the consequence will increase, further adding to its severity.

The breaker functionality is by almost all participants considered as the highest risk factor in AMI and is as such perceived to be closely guarded by both regulations and the DSOs. But as most of the participants agree upon that nothing is 100% secure, they indicate that exploitation of the breaker functionality may be possible, both at device and system level.

- **Loss of availability, integrity and confidentiality of data**

The loss of availability, integrity and confidentiality of data in general do not affect the delivery of energy unless the breaker functionality is targeted and engaged. The energy will still be available at the metering points, but depending on the security objective affected, will have different consequences for the system, the DSOs and the end-user.

Loss of confidentiality is described by some of the participants (DSO#2-4, E#1-3, R#1 and 5, PV#1) where communication can be tapped or intercepted. Further, it can be analyzed for profiling and extraction of privacy-related information or used for big data analytics and marketing purposes, especially on system level due to the volume of data. The loss of confidentiality can also entail substantial financial impacts to the operator or DSO due to the GDPR and how consumption data is considered PII. However, such losses are not highlighted as significant for breaches in the distributed

elements, due to the assumed limited value of information there and how the system-configuration will limit the numbers of affected end-users.

Loss of integrity can be caused by injection of false data and manipulation of FW, SW, HW and data. The main consequence as described by several of the participants (14) caused by loss of integrity is financial impact for both DSOs and end-users. The financial loss can be caused by erroneous or false consumption data being reported, providing a false basis for settlements. O#1 also describes how erroneous or false data can affect the state estimation within the distribution network, providing flawed basis for decisions regarding the operation of the grid.

Loss of availability can have similar causes as loss of integrity, with the addition of denial-of-service attacks at both device and communication channel level. Three of the participants (AV#2, DSO#4 and 7) describe how the loss of AMI data can cause additional financial impact to the DSO. DSO#4 points to how failure to report data to Elhub can incur fines. Further, DSO#7 and AV#2 describe how settlements to end-users may need to be postponed or solved manually, causing temporary financial losses due to average settlements for their customer groups.

- **Societal trust**

If a breach occurs in AMI, several of the above-mentioned consequences can manifest themselves as more or less tangible impacts. Several participants (AV#1, PV#1, R#6, DSO#2, 7 and 9) also describe a more intangible consequence as reduced societal trust in the system.

AV#1 and DSO#9 specifically points to the trust the DSOs and AMI operators have within the society at large, but also the trust between the different actors in AMI, and how crucial it is to uphold this trust in relation to information security. Information security in AMI rests on that the individual actor shall be confident that the delivery they receive from other actors has retained its confidentiality and integrity and is available to them as expected. Any incidents will affect trust and how the different actors relate to each other, possibly incurring financial and reputational loss. AV#1 further describes an example how a lack of trust can lead to reverting or avoiding using updates or patches from a previously compromised provider. This occurs when the actor evaluates the risk from using the patches to be higher compared to the potential vulnerability the patch would fix. As such, a breach of trust could lead to increased levels of risk.

4.2.4.8 Enablers and challenges

In addition to exploring the perceptions on information security vulnerabilities, threats and risks, the study also asked questions and investigated what the different participants see as enablers and challenges for information security.

- **Organizational contributions and challenges**

Information security management and the organization of roles, responsibilities and authority is based on both internationally accepted standards such as the IEC/ISO 27000-series and the regulations and guidelines as described in Section 2.2 and 2.3. The organization of the work with information security in compliance with or with deviations from these creates different contributions and challenges.

Vulnerable due to lack of redundancy in competence: Four participants (DSO#6, O#2, PV#1, O#1) point out how both small and medium sized DSOs have combined several of the roles (such as ICT security coordinator[46], chief security officer and contingency manager) in one individual. This is emphasized by the participants as a significant challenge, where a single individual often is responsible for managing the security in the smaller organizations.

Further, DSO#6 and O#1 also indicate how smaller DSOs are struggling to retain and maintain competence, making it challenging to maintain a persistent focus on information security and the requirements. The size and location are deemed to be significant factors for recruitment in a market with few specialists.

The regulatory authority: NVE (including RME) is considered a significant instigator, both in terms of the supervisory regime and as a facilitator for collaboration and information exchanges by several of the actors (DSO#1-4, 6, 8 and 10, R#3-4 and 5, E#5, AV#1-2, O#1). The DSOs point to the importance of adhering to both regulations and guidelines to obtain a sufficient level of security and describe an interest in improving and working through the challenges being pushed by regulations and guidelines. Some of the participants elaborating on this (DSO#2, AV#1-2, R#3-4) also acknowledge the role that both the authorities and regulations have in driving the engagement for AMI and information security. Without the requirements and supervisions, the actors believe that they would not have been as actively engaged or focused on securing the AMI as they perceive themselves to be as of now.

Several of the participants (DSO#1-4, 6-9 and 10, AV#1-2, E#1 and 4, O#1, R#3-4) highlight the organization and regulation of responsibilities and authorities in AMI and the energy sector as sufficiently described and with duties reasonably placed within different entities. A general perception is that the Norwegian implementation and its organization with the regulatory requirements is one of the most secure and forward-looking implementations of AMI compared to other implementations in Europe and the U.S. AV#1 believes that the groundwork done with the Norwegian implementation has considerably affected the professionalism and focus of vendors and service providers in terms of information security measures adopted into AMI.

However, several of the same and other participants also believe that the organization of roles and responsibilities has considerable room for improvement as described in the next paragraph.

Complex organization: The organization of roles and responsibilities between the different regulatory authorities and further between DSOs and regulatory authorities are perceived by several of the actors as complex and somewhat fragmented (DSO#1-2 and 5, PV#1-2, R#1-2 and 5-6, O#2, E#2). R#1-2 and R#5 note that the organization is functional but fragmented. There are several regulating bodies with specific responsibilities in terms of information security, as described in Section 2.2. For example, NVE regulates the breaker functionality, while RME regulates information security in general for AMI and the energy sector. R#2 and O#2 highlight that the number of authorities creates some confusion amongst the stakeholders (DSOs in specific) about who is responsible for what and which regulations are applicable. O#2 mentions the National Security Act in this regard, and how its

[46] (NO) IKT-sikkerhetskoordinator, a required role in the Power Contingency Act

implementation and enforcement could be used as a template and a potential solution to reduce the confusion within all the actors and KBO-units.

A perceived distance between the regulatory authorities and the DSOs in terms of responsibilities and authority is noted by some of the participants (DSO#5, R#6, PV#1-2). The authorities concerned with regulating DSOs in the energy sector have a wide variety of subjects in all different shapes and sizes, with different competence and focus regarding information security and how to implement regulations and guidelines. The responsibilities are put on the individual DSOs, creating a gap between the DSOs but also between the regulating authorities and the DSOs in terms of capabilities and resources to ensure compliance with regulations. The DSOs seem to be left on their own on how they choose to implement measures to ensure compliance, where the next step is the supervision and auditing by the regulatory authorities. The larger companies with more resources have an advantage in this regard, while the small and medium-sized DSOs are dependent on alliances, industrial organizations, and a trickle down-effect from the larger companies to be level with the regulations.

R#1 and R#6 also point to how the fragmentation is reinforced by the sheer number of subjects, where over 100 DSOs and KBO-units create a formidable task in terms of generating an overview of the status of information security. The joint effort is highlighted as an absolute necessity as no one sits with the complete picture of the status on their own. However, R#1 also underlines that the occasional mix of roles and regulations, as perceived by the actors, is due to the energy industry being considered as one of the more complex systems in the world. There are several different and unique elements that need to pull in the same direction, involving several actors and a mix of interdependencies, necessitating different authorities and mechanisms for control.

Two participants (R#6 and PV#1) also highlight how a complex system with different stakeholders and organizations gives way to suboptimal organization of communication and notification channels. PV#1 points to how actors actively must subscribe to notifications from KraftCERT and other organizations, and states that the bilateral notification between the authorities and the actors has room for improvement. Similarly, R#6 mentions how not all actors are eligible to receive classified information or updates, which may delay or prevent essential and time-critical information reaching the actors.

Regulatory framework shortfalls and vulnerabilities: The regulatory framework as described in Section 2.2 is highlighted by some of the actors (DSO#2,5 and 8, R#2-3, O#2, PV#2) as adjacent to bureaucratic and complex in its organization. The different legal requirements relevant for AMI are placed within several regulations, where DSO#2, R#2 and 3 perceive they should be more centralized and harmonized to streamline accessibility.

In terms of how precise and specific the regulations and guidelines should be, some of the participants argue for both more precise and clear requirements, but also the need to keep regulations from being technology dependent. DSO#8-9 and R#3 indicates how more precise and specific regulations would ease the work of both small and medium sized organizations with limited resources and competence to interpret and understand what is considered partly vague and inconclusive regulations. At the same time AV#1, R#5 and DSO#9 also point to that stricter regulations could

potentially hamper the general development of the system and the flexibility of security measures. As DSO#9 states it:

"We can't become technology-dependent in information security. It has to be system dependent" DSO#9

Industrial and independent organizations are mentioned by some of the participants as important contributors. They act both as advisers in information security compliance and as providers of cyber SA necessary for a secure day-to-day operation of the grid and AMI. When asked about who they see as the driving factors for information security in AMI and the energy sector, KraftCERT (DOS#1, 3, AV#1-2, PV#1-2), FSK (PV#1), NORCICS[47] (DOS#6) and other industrial organizations are mentioned as significant contributors with a strong influence. Their role as independent advisors and supervisory bodies is seen as important in providing unbiased advice in security and operation of information systems in general, and an important notification channel when incidents occur. In specific, KraftCERT with its perceived close cooperation with NSM[48], is mentioned by 6 participants as a key information channel and hub in this regard.

- **Knowledge and education**

Several participants highlight both education and knowledge sharing as a key enabler for both future integration of new technology and functionality, but also as an important factor for improving and further securing the current integration and operation of AMI.

Dilemmas in information sharing are brought up by some of the participants (DSO#3, 6, 10, R#6, E#2, AV#1) as a potential challenge in securing the energy sector and AMI. All of them point to how most companies do not necessarily disclose incidents openly in the sector, which limits the potential to learn from such challenges. This is further elaborated by AV#1 and E#2, who emphasize the potential for loss of reputation when sharing internally experienced short-falls or incidents. This can also affect the level of trust within the sector, as a vendor or service provider with a reported incident can be blacklisted and cause system operators utilizing their equipment or services to roll back or postpone updates or patches. They may choose to live with possible vulnerabilities rather than to let blacklisted vendors or providers access their systems.

Knowledge and knowledge sharing means providing the fora and channels appropriate for disseminating threat knowledge, vulnerability discovery and assessment methodologies. Several participants (E#4, AV#1-2, PV#1, R#2, DSO#8, O#1-2, E#4) deem the ability to share knowledge and findings as essential in building cyber SA and improving the security of AMI and the ICT systems in the energy sector. Several fora and cooperation bodies are already in place supporting the exchange of knowledge, but some participants (DSO#3, PV#1, AV#1-2) point to how these fora can be better utilized. They highlight how the actors need to be present with appropriate personnel with the right competence to actually contribute to these fora. E#4 also points to how such fora with the right personnel and

[47] Norwegian Center for Cybersecurity in Critical Sectors (NORCICS) is a center for research-based innovation hosted by NTNU.
[48] National Security Authority (NSM) in Norway is a cross-sectorial supervisory authority within the protective services in Norway.

competence present can contribute to levelling the playing field for the participants, and further contribute to the joint effort of securing AMI and the energy sector.

This perception is to some degree supported by the structured interview and questions regarding factors that would influence the level of security within AMI in both a positive and negative sense. Here increased cooperation and knowledge sharing amongst participants are deemed as the second most important factor for positively affecting information security. At the same time, the lack of knowledge and expertise amongst actors is seen as the most significant factor inhibiting further integration and development of AMI (Section 4.2.3.2).

Education of personnel in the field of information security is highlighted by 1 of the participants (O#1) as an important factor enabling a secure and reliable grid in the future. This is based on the implementation of new functionality and increased usage of data in AMI, requiring more specialized competence. It is pointed out that there is a shortage of information security knowledge within the industry and amongst the authorities, a view supported by several other participants (DSO#8, R#2 and 5, PV#1-2). As an extension of this, O#1 underlines the need to enhance the recruitment and availability of specialists. Several measures are also proposed to increase the quantity and quality of education. These measures include industry entering into partnerships with educational institutions and providing incentives and support by industry for personnel who are interested in pursuing a career in information security. O#1 focuses specifically on the vendors and service providers in the field of AMI. It is perceived that both the level of knowledge and specialist competence is too low compared to their responsibilities and tasks in the network for securing the infrastructure and data.

- **Future challenges and changes**

The AMI has enabled automation and increased streamlining of the grid with its functionalities and the data produced. Some participants (DSO#3, 7-8, E#4-5, AV#1) also indicate that there is an untapped or unused potential in the system as of today that could further enhance the operation of the grid. But by incorporating more and different types of functionality and extracting and handling more and different types of data, new challenges may arise in terms of information security. All participants were asked about how they view the future changes for information security in AMI, and the answers revealed various perspectives of both technical and organizational nature.

Security mindset and higher requirements: Some participants (O#1, DSO#4-5 and 8, E#2 and 4-5, R#1 and 3) emphasized the need for a more focused technical and organizational security mindset. DSO#8 and E#2 focused on the need for better control and interaction with the value chain, with the introduction of new requirements and more functionality in order to handle the increased digitalization and complexity. Similarly, O#1, E#4 and 5, DSO#5 and 10 highlighted that higher demands on information security might arise with expanded functionality and new services, prompting the need for more information security specialists and competence in the energy sector. On the more technical side, R#1 and R#3 highlighted the importance of enhancing technical and organizational security measures, particularly in the area of intrusion detection to handle increased usage of data and added functionality with a sufficient level of security.

Changes in regulation were pointed to by some of the participants (R#1, 2 and 6, E#5) as a factor that could both enhance but also to some extent limit the future use of AMI. R#1 and 2 state how new regulation from the EU concerning cybersecurity regulations and energy markets may require establishment of mandatory SOCs and increased logging requirements. This can put additional strains on the actors and particularly the DSOs but may also harmonize the implementation across EU to some extent by standardizing the requirements. E#5 also believes such increased requirements and the harmonization is greatly beneficial to the overall performance of the grid, by improving operations, maintenance, error correction and reliability. In contrast, R#6 focuses on how imposed expansion of functionality and use of data can exceed the regulatory control efforts and make AMI and the energy sector more susceptible or attractive to manipulation and tampering. Such expansion could include increased real-time requirements (more data transferred and processed) and throttle functionality, providing more control to DSOs but also more responsibility and potential vulnerable vectors.

Overall, these factors suggest that the actors in AMI may need to adapt to changing regulations and technological advancements to ensure the security and reliability of energy and data.

Changes in the international security landscape is mentioned previously by most of the participants in conjunction with cyber SA and how the international security situation affects the information security focus. The current situation is perceived to have a significant impact on the participants focus, and several of the participants (DSO#1 and 10, E#1-2, R#2-3, PV#1) also mention how future changes will affect their risk perception. PV#1 mentions how the threat level is expected to rise when the current conflict in Ukraine settles down, similar to what was experienced after the Georgian conflict in 2008 and the different Chechen wars. Similarly, some of the participants (DSO#3 and 8, PV#1-2 and R#2) highlight how they had expected more attempts and attacks with the increased tension of today.

The digitalization of society with the proliferation of more devices and functionalities will create more attack vectors and potentially introduce more vulnerabilities. Some participants (DSO#9, E#3-4, R#1 and 4-5) point to this, but with both positive and negative considerations. They all acknowledge how digitalization increases the security challenges, where DSO#9 and E#3 are concerned that the created interdependencies may become increasingly attractive and easier to exploit. This is based on the use of more distributed digital devices in the infrastructure requiring specialized knowledge to address the challenges. This view is shared by the others, but R#1 also states that the overall benefits of AMI, such as cost savings and improved energy supply security, outweigh the pitfalls through the joint effort on securing the system. R#4 and 5 further highlight how this effort in securing the system is going to be increasingly important with the digitalization, increasing the demand for securing AMI and other energy sector infrastructures compared to other IT-systems due to their critical role.

Digitalization also brings along more data being transferred, processed and stored. In terms of AMI, requirements for higher frequency on measurements and more functionalities produce more data. Three of the participants (DSO#2, 5 and 9, E#5 and R#2) highlight this as a future challenge for AMI, where the increased volumes of data can entail new possibilities for privacy-related exploits. Increased proliferation of

devices handling and storing data with several interfaces increase the vectors for attacks, where more detailed data and measurements can be exploited for profiling and traffic analysis of individual end-users. To mitigate this threat, both DSO#2 and R#2 recommend stricter requirements on encryption and management of data, whilst R#2 expresses a positive view on the future in this regard as best practices are expected to emerge in the near future to guide the industry.

The increased digitalization with the increased volume of data will also entail the need for improved big data analytics, faster retrieval and better reporting to meet future requirements in terms of increased resilience, more efficient operation of the grid and a higher level of security. Some participants (DSO#3-7, PV#1 and R#4) point to these factors as changes to how data is fetched and processed, in addition to the importance of improved data quality and availability to the data processors. These expectations are based on the growing reliance on AMI for network maintenance and monitoring, increasing the demands on standards in terms of operational reliability, functionality and security. And as PV#1 highlights, without sufficient measures to handle the volume of data securely, the use of functionalities and features can be restricted.

Technological advancements are what several participants (14 from different actors and levels) pointed to as what would produce the most changes and challenges for AMI in the future. Several factors in technological advancements were highlighted. This includes the standardization and structure of data sharing, the potential for new HW and communication channels, such as 5G, the usage of cloud solutions, and the introduction of AI and ML. Overall the participants elaborating on technological advancements suggest that the incorporation of new services, greater flexibility and a more distributed infrastructure would necessitate more specialized competence and an increased focus in secure development and operation of these.

DSO#1-2, 6, 9 and 10 pointed to how new communication channels may emerge and how the functionalities of technologies like 5G may improve the security posture of the channels compared to today's use of PLC, RF and other cellular technologies. Further, DSO#2 elaborated on how more standardized and structured data sharing is an ongoing effort in the industry to meet the proliferation of actors and systems handling data, where security and the handling of authentication and authorization lie as a foundation.

The use of cloud solutions is pointed to by several of the participants (DSO#4-5 and 8-9, AV#1, O#1, PV#1 and E#5) as an expected trend in the near future. The requirements for more efficient and automated operations entail the use of more data, and with the incorporation of AI and ML, scalable systems provided in cloud environment are needed. Additionally, as stated by PV#1, the use of cloud solutions is where the technology is headed, and at the same time the actors do not necessarily have the competence or resources to provide similar services on their own. This implies the need to focus on more strict and detailed data processor agreements to sufficiently place the responsibility and authority between the actors providing and using cloud solutions.

Several of the actors (R#1, AV#1-2, PV#1) also pointed to how technological advancement will entail changes for both the defenders and adversaries. They describe how development of equipment and techniques will benefit both parties,

where the use of AI and ML can be a significant threat towards security, e.g., by being used to break encryption.

Within the operation centers in the energy sector, the technological advancements and the increasing IT-nature of systems will bring about an integration of IT and OT in the future. PV#1 underlines this development by highlighting how OT is increasingly dependent on IT for production of energy and smart maintenance in order to optimize the operation of the grid. This dependence can entail the use of AI and ML to enhance the optimization, entailing a closer connection between IT and OT necessary for the flow of data.

The development of the next generation of AMI and SMs was described by some of the participants. It was asked as a probing question developed in the later stage of the interviews, where only 7 participants (O#2, DSO#2-5, E#5 and R#2) were challenged to describe how the development of the next generation AMI would take place. Their responses provided some insights into how they perceive the challenges and opportunities with the next generation of SMs.

DSO#3 and 5 pointed to how the planning and preparation of the current AMI highlighted the need for an early roadmap for the next generation that considers potential future technological advancements and government policies. An early roadmap and clear guidelines may prevent a similar rushed-out experience as the current version was perceived as by DSO#3 and 5. This may result in a more detailed focus on information security in the development process, using standards for incorporating security mechanisms from the start.

DSO#2 mentioned how new HW could enable new communication channels and methods, with a wider range of possible carriers. Specifically, 5G and the introduction of more IoT devices in the grid were seen as enablers for a more secure and reliable operation of the grid. This view is supported by R#2, which also states that new components and features will entail more vectors and increased risk without significant work on requirements for the implementation and operation.

Both O#2 and DSO#5 state how the work with the next generation is important to start within the next few years, as the development process will take considerable time. The current implementation is assumed to have an expected technical and financial lifespan of 15 years and has a minimum of 5 years in operation to this date. Both R#2 and DSO#2 state in this regard that the work has already started, but without a clear timeline as of now. On the other end of the scale is DSO#4, which states that the current system has sufficient remaining lifespan to warrant any work on the next generation yet.

Securing the value chain in AMI and the energy sector is a concern pointed out by some of the participants (DSO#8, E#1-2 and 5, O#1) in a future scenario with increased numbers of devices and providers in the network. DSO#8 points to how the reliance and dependence on suppliers and services will be increasing with more digitalization and outsourcing of services and competence. This will entail a need for more focus on collaboration and clear data processing agreements between the actors. This view is supported by O#1, E#2 and 5, who also state how insufficient agreements can have significant severe effects especially in cloud-based solutions and their data chain. Further, E#1 also describes a potential shift in where and how services and HW are produced in order to have better control of the value chain. It is

expected that more of the production of components and services, such as cloud solutions, will happen closer to home, potentially avoiding or reducing the reliance of a single manufacturer or nation state, e.g., China.

FW and SW updateability is a functionality that will enable devices in the AMI-network to receive updates and patches designed to enhance their operation. In an information security perspective, updateability ensures the possibility for closing FW or SW vulnerabilities or mitigating consequences of faulty or erroneous codes. Only a few participants (E#2 and 4, O#2, R#2 and 3) make a point of the importance for facilitating and ensuring an update regime for the distributed devices in relation to their lifespan expectancy and the technological changes in AMI and SMs.

Once the SMs and the system are operational, considerable costs to replace equipment will be incurred if faults or vulnerabilities are discovered. In addition, the process of developing, deploying and operationalizing AMI-systems takes several years, where the technological development may render them obsolete in the meantime. An important feature and requirement for secure operation of AMI in the future is to ensure sufficient updateability of the distributed elements. O#2 emphasizes the need for a more focused approach to ensure that devices can be easily and efficiently updated, and thus remain secure and functional. This approach is suggested to be incorporated into regulations, putting more concrete and strict requirements on updateability.

- **Security controls and mitigative measures**

The study challenged the participants about different mitigative measures that could be implemented to enhance the security posture of the AMI. The main categories of mitigative measures were divided into two factors, being processual and technical security related measures for addressing cybersecurity vulnerabilities. They emphasized five elements of mitigative measures that have a processual focus. These five are: (1) persistent security focus, (2) security awareness and education, (3) non-repudiation and accountability, (4) compliance with regulations, and (5) collaboration. Further, 4 elements of mitigative measures that have a technical factor are emphasized, namely (6) zero-trust, (7) surveillance and logging, (8) security audits and (9) authentication and authorization.

(1) Persistent security focus was mentioned by several DSOs (DSO#1-2, 4, 7) and one end user (E#4). DSO#1 highlighted the need for a continuous security focus with mechanisms such as monitoring, logging and procedures for regular updates of security protocols. This is further elaborated on by DSO#2, who emphasized the importance of proactive measures, including vulnerability testing and proactive planning to ensure an acceptable level of security. This focus needs to be maintained over time, thus requiring a sufficiently staffed and resourced organization with the right competence. This is also stressed by E#4, DSO#4 and 7, which highlight the need for continuous education and training on security protocols, risk assessments, and the organization's different control measures for handling and mitigating information security risks in general.

(2) Security awareness and education were identified as essential mitigative measures by 6 participants. O#1, E#3, 5, DSO#3 and 4 highlighted the significance of promoting security awareness to reduce risks associated with the human factor. This includes educational efforts and employee training both internally and externally

covering topics such as password hygiene, social engineering tactics and threat awareness. Further, both R#2 and O#1 recognized the positive impact that increased competence through education and training have on awareness and the robustness of the organization.

O#1 also proposed that stricter requirements be placed on the competence, staffing, and training of operators to address the vulnerability on the operator's side in terms of awareness and competence. As a proposal, these requirements could be specified in the Power Contingency Act, which already includes requirements for safety domains in SCADA systems.

(3) Accountability and personnel control in the workplace were also highlighted as crucial components of mitigative measures by some participants. O#1, PV#1 and E#5 emphasized the importance of accountability of the employees by providing measures to ensure accountability in how critical operations and actions are conducted and by whom. In addition, PV#1 and E#5 highlighted how simple measures such as background checks and regular employee interviews will provide a more fine-grained control and overview of the individual's background and potential vulnerable spots. This can to some extent mitigate the threat from insiders.

(4) Compliance with regulations as a mitigative measure for protecting sensitive information and assets in the AMI system was emphasized by 8 participants. The constantly evolving nature of cybersecurity threats and the need for continuous work on regulations were highlighted by DSO#5, R#1 and 4. They emphasized the importance of continuous work on and updating of regulatory requirements to maintain the security of AMI systems. As an extension of this, both PV#1 and DSO#8 state how compliance with the Power Contingency Act is believed to ensure a sufficient security posture with today’s threat landscape. In contrast, R#4 and O#2 underline how compliance in effect is the minimum level of security expected by the regulatory authority and considered a red line in this regard. O#2 points to the benefits of also absorbing the meaning and suggestions within the guidelines as well as to be better prepared and have a better security posture. However, O#2 together with several others acknowledges that it is not necessarily information security that generates revenues for the actors, and how it is a constant cost-benefit struggle.

Further, R#1 points to how the regulations and requirements in terms of information security are spread across several legislations. At the same time, there is a mix of regulatory authorities responsible for supervising and enforcing the regulations. This creates to some extent confusion amongst the actors as to what and who they are accountable to. Collaboration and joint effort amongst the actors and the regulatory authorities are therefore crucial as a means to reduce the confusion and aid the actors in reaching compliance.

(5) Collaboration and dialogue were identified as essential components of mitigative measures. Six participants from different organizational levels placed significant emphasis on collaboration and dialogue as a crucial component of addressing cybersecurity vulnerabilities in the AMI as part of the joint effort.

In this regard, DSO#8 and 9 indicated the need for a closer dialogue and cooperation with suppliers to ensure a mutual agreement on the responsibilities and accountability for the parties involved. This includes the integration of security experts in projects and in forming SLAs. This view is also evident within responses from AV#1 and 2, where the importance of collaboration and information sharing to address cybersecurity risks is underlined. They also highlight the need for a deeper

understanding of the most significant risks and how greater utilization of industry collaboration fora could enhance this. Similarly, in terms of the regulatory authorities, R#2 also suggested that better communication and information sharing amongst all supervisory authorities could lead to clearer delineation of roles and responsibilities, and ultimately enhanced security focus and efficiency. These recommendations highlight the crucial role of collaboration in achieving greater efficiency and organization towards information security for the AMI ecosystem.

Furthermore, almost all participants point to how information security in AMI and the energy sector is a joint effort, which emphasizes the need for communication and collaboration between all the different actors. Similarly, they perceive that the system will never be 100% secure and how there is always room for improvement, also in the form of collaboration and communication.

(6) Zero Trust security adaptation was recommended by PV#1 as a potential future measure. Implementing Zero Trust principles within organizations in the energy sector involves assuming that the organizations have already been breached and thus improved cybersecurity measures are required. This approach holds considerable potential for enhancing the overall cybersecurity posture of the individual organization and the sector as a whole. PV#1 describes that the concept of Zero Trust is recognized in larger organizations within the energy sector but is perceived as a mere buzzword by smaller entities due to concerns about the associated costs of implementation. According to PV#1, Zero Trust has been implemented across both IT and OT environments in some larger organizations, whereas smaller organizations tend to focus more on IT. However, PV#1 notes that a significant gap still exists between IT and OT in most organizations and needs additional focus in the near future.

(7) Surveillance and logging were highlighted by DSO#9, E#5, R#2 and 3. They emphasized the significance of enhancing logging as a key component for surveillance of the information security posture of the system. E#5, DSO#9 and R#3 underlined the need for logging activities to maintain accountability and the possibility for surveillance of the system and its distributed elements. From a regulatory perspective, R#2 stated that the current requirements for logging and surveillance are perceived to be satisfactory and is now a question of compliance within the actors subject to the requirements. However, R#2 recommended that organizations accountable for AMI operations should improve logging and monitoring capabilities to bolster the overall security of the ecosystem on a general basis.

(8) Security audits were emphasized by several participants (5 DSOs and 3 from regulatory) in relation to building cyber SA. But most importantly, they are also perceived as measures for controlling the security posture of the organizations. By supervising the systems and the organization of the work within the actors, non-compliance, vulnerabilities or other shortfalls can be detected, and the actors can be held accountable to rectify the issues. As described by R#3, such incidents can serve as valuable learning opportunities for the actor itself and others if shared in a suitable format, further contributing to knowledge sharing and improved security practices across the industry.

(9) Authentication and authorization were described by some participants (DSO#9, PV#1, AV#2 and E#5) as important components of an organization's security policy. The participants underlined the importance of tightly controlling access to specific functions and resources and of having a clear separation of duties. This involves having only a limited set of superusers and authorizing read and write

access based on role or functionality within the organization. In this regard, PV#1 describes how consequences of attacks depend on the security measures and the specific implementation of the system, where effective authentication and authorization mechanisms can significantly limit an attacker's reach. Access can be limited to only a small number of devices over a certain period and limited to originating from a specific physical location using a specific port with a specific MAC-address with a specific user.

5 Discussion and recommendations

This chapter will provide the foundation for answering the problem statement by addressing and discussing the different research questions and put them in context. First, the most prevalent vulnerabilities, threats and risks identified from the body of literature analyzed in the SLR will be discussed in Section 5.1. The stakeholders' perception of the most prominent vulnerabilities, threats and risks to information security in AMI are then discussed in Section 5.2. These are divided into 3 main themes: Perceptions of risk (Section 5.2.1), influencing factors (Section 5.2.2), and information security focus (Section 5.2.3). In Section 5.3, a comparison between the SLR and SSI is made, and the divergences are identified and outlined, contributing to answering RQ3. The measures to address divergences are discussed in relation to technological and organizational factors in Section 5.4, contributing to answering RQ4.

5.1 The most prominent vulnerabilities, threats and risks identified in literature

Based on the chosen methodology in Section 3.2.1 and the analysis of the SLR in Section 4.1, the focus areas of the research and the most prominent vulnerabilities, threats and risks in AMI were identified. The findings are summarized at HW-level (Section 4.1.5), communication channels (Section 4.1.6) and system level (Section 4.1.7). The body of research described a wide variety of vulnerabilities, threats, consequences and risks. Assessment of risk and likelihood was to a limited degree described for threats and incidents in the different levels.

5.1.1 Vulnerabilities

The vulnerabilities identified at the different AMI-levels revolve around the accessibility to HW and communication medium; design flaws in HW and protocols; and the system platform itself.

HW level: The most prominent vulnerability described in literature is the physical access to the devices and their interfaces, which enables further vulnerability discovery by utilizing attacker tools or by physical tampering. This can provide access to the inside and functionality of the devices, such as the metrological element, the main control unit, the communication systems or the breaker. There exist different tampering and detection mechanisms, but these can be circumvented as explained in [103]. Further, the resource constrained environment in both SM and DC increases the vulnerability, as limited computational power and memory inhibits implementation of complex and resource-demanding security controls which may exhaust their resources or put considerable amount of overhead in computation or memory. Similarly, an attacker can more easily overwhelm or exploit HW with limited resources to withstand attacks, both in the cyber and the physical domain.

Communication channels: In terms of vulnerabilities, the most prominent are considered to be the publicly accessible and shared communication media, both wired and wireless in this regard, and the use of publicly available technology within the media. The distributed nature of the network and devices entails that data will follow communication paths traversing a diverse set of media and technology, with inherent and

design vulnerabilities, implemented in a similar diverse manner. The accessibility of wireless channels, combined with their shared nature, allows potential threats to exploit them. Additionally, the choice of technology, such as IEEE 802.16 WiMAX or 4G LTE, being based on open standards, makes them susceptible to vulnerability scanning and discovery. Further, the protocols and mechanisms used can have inherent vulnerabilities making them insecure by specification (such as ANSI C12.22) or by design (such as ModBus RS-485). These vulnerabilities are often based on insufficient secure authentication, encryption or communication mechanisms, as described in [104], [100] and [107]. A resource constrained network and its devices further adds to the list of vulnerabilities, as limited bandwidth and computational power to a certain extent limits the available defensive mechanisms and the type and implementation of the different protocols, as described in [111]. The high-level vulnerabilities described make the communication network one of the most prominent attack surfaces in AMI, a system that is already considered one of the most vulnerable attack surfaces in the SG [87]. To mitigate and reduce vulnerabilities and threats, most of the literature identifies controls and techniques to obtain an acceptable risk level, however there is always the risk of introducing new vulnerabilities with such controls or functionality. A concrete example is described in [115] with the introduction of ML techniques for attack detection, load forecasting and energy pricing. ML models can be vulnerable to AML techniques, attempting to influence the decisions or the training of the models to avoid detection of malicious activities or to impact the operational decisions of the SG and AMI.

System level: The most prominent and frequently observed vulnerabilities at system level, are the IT-nature of the networks, using IP-based communication, and the interconnections between networks. The business network and the distribution control center have connections in the corporate WAN to enable the flow of data and information between systems to enable automation of several functions as described in Section 2.1.4, such as EDS and CIS. These interconnections and the IT-nature at this level make them susceptible to both targeted and non-targeted threats originating from remote attacks via the internet. In addition, both [43] and [118] also describes the challenges in how security is implemented at the distribution control center and the managements systems. They particularly outline how a poorly implemented platform configuration in the form of insufficient security policies and poor cyber hygiene can give rise to excessive access rights, insufficient authentication, and weak password policies.

5.1.2 Threats

The described threats described concern all the different levels, where some are specifically tailored to the distributed elements and a proprietary environment, while others again are based on regular IP-based communication and platforms.

HW-level: The described vulnerabilities can be exploited by a wide array of threats, where the most frequent threats described in the reviewed literature are the extraction and modification of data/SW/FW, and injection of false data (FDI). These threats can affect the operation of the SM itself and the data and commands it stores, receives or sends, which can cause cascading effects to other elements in the system such as the DC or the HES/MDMS. However, there are few accounts in the reviewed literature which weigh the threats against each other in terms of likelihood or consequences. [103] mentions the threat of FDI attacks affecting the consumption data in the physical memory of SM as the most common type of attacks, whereas [43] mentions threats from buffer overflow as one of the most significant threats exploiting the resource constrained environment in SMs. As a result of a risk assessment, [42] assesses targeted

manipulation of breaker functionality in SMs and DCs causing mass disconnections of breakers at end-users as catastrophic in severity and the most likely of the assessed threat-scenarios.

Communication channels: The vulnerabilities tabulated in Table 4.5 and briefly described in Section 4.1.6 can be exploited by a significantly wider selection of threats compared to the HW. The most frequent threats described in the literature review are threats targeting the data, signaling and commands transferred or stored in the network. This includes the interception, modification or extraction of SW, FW, data or commands, and the injection of false and malicious code. These threats overarchingly aim to impact the operation of devices or AMI as a system, by maliciously controlling the routing, the content and the timing of messages. False data injection threats are specifically researched in [87] and [86], giving a broad overview of the different facets of FDI. Both interception, modification, extraction and injection of data, FW, SW, signaling or commands can be performed by different methods, but the most frequent method mentioned in the literature is the use of MitM, where an attacker places himself at some point in the communication channel, acting as a relay in the communication between parties of the network. This enables a wide range of other more specific threats to be realized, such as eavesdropping, spoofing, replay and traffic analysis. Further, due to the nature of the communication channels, different types of DoS threats are frequently described as a common threat, which can have low cost in terms of complexity and resources for an attacker. [88] focuses on this threat in specific, looking at how flooding and vulnerability attacks can create DoS conditions and how they can impact AMI. However, DoS and DDoS comes in many shapes and forms, such as puppet and buffer overflow, targeting the communication channels used or the operation of the device (congesting the channel or device to break system performance).

Despite the wide range of threats identified in the literature, the SLR encountered the same issue as with HW in terms of ranking of threats. The different threats are not necessarily weighed against each other in terms of likelihood or consequences, but [89], [104] and [112] describe what they perceive as the most common threats in communication: Variants of DoS, FDI, eavesdropping, MitM and traffic analysis. However, they do not present any statistical data for this assumption, which again can be due to the observation from [13]: the lack of historical data and statistical examples of threats and attacks targeting AMI.

System level: The vulnerabilities tabulated in Table 4.6 enables several threats (both cyber and physical) and their potential for damage. Most of the threats described in the SLR revolves around regular IT-threats originating from the internet and are not described in detail besides what is briefly detailed in [118]. However, the IT-nature and the IP-communication directly enables the use of open-source intelligence tools as described in [99] and [118], to map out the system under scrutiny and conduct further vulnerability scanning.

At an overarching level, the main threats regard the SW and data modification and extraction, and the injection of malicious code or malware in the servers. These threats can be divided based on the intentions of the attacker, as described in [118] as steal data, control or take down the management server, or affect the input data to the management system (as described in [86]). Server in this regard can also be specific services. Stealing data is to some extent explored further in [117], which describes privacy-related threats in regard to the increasing volume of data with different

granularity communicated and stored at system level. The paper highlights potential threats such as data disaggregation and de-pseudonymization, where attackers can exploit data sets reported at different intervals to re-identify individual customers and reveal their consumption patterns. These are threats common at both communication and system level, but with a potentially wider impact at the system level, where all data is collected. However, regardless of the type of threat that is realized, it is assumed that they are trying to either to obtain information about the system or to gain access to it for further exploitation in the forms of stealing data, taking control or bringing down the server, or affecting the data used as input to the system.

5.1.3 Consequences

Impact and consequences of successful attacks are described highlighting both impacts to the individual devices, AMI as a system, but also to other dependent systems and critical infrastructures to some extent. The affected security objectives affected are tabulated in Table 4.2, Table 4.5 and Table 4.6 for HW, communication channels and system level, respectively.

HW-level: The descriptions of impacts from threats successfully being employed in attacks are often general in nature and does not necessarily describe each threat and its direct impact to security objective or AMI. This can be due to the observation that most of the literature describes theoretical and simulated threats and attacks, where the impact at different levels can be challenging to simulate and predict due to the diversity of AMI systems and their implementation. However, the most frequently described impact described is theft of power and the following subsequent financial loss, which by in [105] is mentioned as the most considerable challenge due to the impact on DSOs. This implies that the threat is multiplied or automated over an extended set of devices, other than the individual meter itself, which on its own would provide minimal impact to the operation of the distribution grid itself. Such automation could also cause unreliable operation of the grid, as load forecasting and operational decisions could be based on wrong estimates for larger volumes of measurement data. Further, it could increase the severity of denial of power, which can be considered one of the most severe impacts in terms of physical consequence. [42] describes how exploiting the breaker functionality increases the severity to catastrophic when affecting a large number of end-users, an effect automation could produce.

Another significant impact that is mentioned, but not widely considered, is the bricking of the device. This implies the implementation of attacks that permanently disable or degrade the SM to the point where the meter will have to be replaced or sent in for maintenance. Conducted at a large scale as described by [1] will cause significant financial impact in terms of replacement and service costs, and potential blackouts if the breaker functionality is engaged as well. But as described by Tøndel et al. in [90], both consequences and likelihood are dependent on the individual system that is implemented and can be challenging to predict on a general basis.

Communication channels: Similar to HW, the description of impacts and consequences from threats are often generic and does not necessarily describe each threat and its direct and concrete impact to the security objectives or AMI. In terms of the tabulated results from the SLR, the most frequently described impact described is the unreliable operation of the communication network and the devices within. This implies that the routing, the timeliness of data and commands, and the general operation of communication do not work as intended, which further can cause unreliable operation of

the grid. Both [86] and [87] in this regard describe how FDI could cause instability and disruption in the SG, by providing erroneous basis for decisions on grid operation. Further, theft of power and theft of data is also frequently described as a considerable challenge, such as in [115] and [87], similar to what is described for HW, and is based on the financial impact it has on DSOs and grid operators. Theft of data follows theft of power in this regard, and can represent significant breaches of privacy, which due to current legislation (e.g., GDPR), also may cause significant fines and severely impact the level of trust within the system. In terms of level of severity, [105] describes specifically denial of power, which it considers to be inflicting the most severe impact to the SG. This is underscored by the general focus on the SG and grid operations, where the main operational goal is to ensure continuous availability of power.

However, as described in HW, both likelihood and consequences are dependent on the individual system, and as such can be challenging to evaluate with generic and simulated systems.

System level: The described consequences and impacts are often generic and overarching in nature. However, it is evident that by accessing the control center and servers at system level, an attacker has the potential to impact all security objectives and cause more widespread and severe effects in the SG and AMI. The overarching impacts to the SG and AMI are like those described for communication and HW; the theft of data and denial of power, based on the brief overview given by the articles describing challenges at system level.

Theft of data and the privacy-related impacts are described in [117], where disaggregation and de-pseudonymization attacks will impact the privacy of a significant number of individual customers, affecting their trust in the system and its security and enabling profiling of individuals. Further, it is assumed that with the current privacy legislation such as GDPR, a breach will entail significant fines to the DSOs, as SM-data is considered privacy information (i.e., in a Norwegian context).

Denial of power is previously described by [105] as one of the most severe impacts which can be realized by either attacking HW, communication or the system level, and is further considered by [100], [42], [43] and [118]. This effect can be obtained by a wide variety of threats, such as modifying commands and functionality described by [105], [42] and [43], and can at system level affect all distributed elements in the AMI chain.

A significant impact also described at this level is how threats can affect the reliability and secure operation of the grid and AMI, and in particular how state estimators can be affected by corrupted input data from SM. This can cause operational decisions based on the wrong basis and cause unreliable and unstable operations and service delivery in the grid.

However, as described for both HW and communication channel, both impacts and likelihood are dependent on the individual system and how it is configured and implemented.

5.1.4 Likelihood

Likelihood in terms of how it is defined in Section 2.1.2 is to a large extent not described or evaluated in the identified literature. This is both based on the scope on some of the literature, such as [100], [101] and [86], and the challenges in defining likelihood as briefly reviewed in [90] and [13]. As an exception, the work of [42] defines likelihood as

a combination of complexity of an attack and the severity of consequences (how many end-users is affected), where targeted attacks are by default set as likely, and used on both HW and system level incidents.

HW-level: Likelihood of successful attacks (based on the described threats described) is not evaluated or calculated by the identified literature with the exception of [42]. This can be explained by the same reasoning given by [90], as being dependent on the individual system and its implementation. At the same time there is a lack of historical data and statistics on conducted attacks conducted specifically targeting or impacting AMI-devices or the system as a whole. The few attacks mentioned in the literature, such as in [87] and [114], mainly concern ICS and SCADA systems, and took place in the era before AMI was implemented or did not impact AMI. The work in [42] defines likelihood of incidents concerning manipulation of HW, data and functionality are considered from unlikely to likely depending on affected end-users and the complexity of an attack.

Communication channels: As with HW, the identified literature in largely does not evaluate or describe likelihood. This can be explained by the same reasoning as for HW and done by [90], as being dependent on the individual system and its implementation, together with a lack of historical data and statistics on conducted attacks conducted specifically targeting or impacting AMI-devices or the system as a whole.

[114] is an exception in this regard, where the likelihood of the different threats and attacks described is defined based on the attack complexity and the exposure of the vulnerability or attack vector, e.g., how easy they are to reach or obtain intelligence on. Table 4.4 shows how the different threats are classified according to likelihood. What is considered as complex attacks in regards of resources and skills are deemed to have low likelihood of being performed, while attacks requiring little effort and the use of well-established tools are deemed to have high likelihood. How the different threats are weighed against each other is not explained in this regard but appears to be a subjective analysis.

However, several of the articles make observations and proposals on methods and techniques on how likelihood can be evaluated on a generic basis. [112] states that most conducted attacks are of wireless nature in general but does not provide any statistics in support of this claim. However, this induces that wireless attacks are more likely to be performed and can be seen as in line with the proposed evaluation of likelihood done in [114], where attacks of low complexity have a high likelihood. Further, the general observation from [13] and [90] still holds true, where it is challenging to evaluate the likelihood based on performed attacks, due to the lack of significant data on incidents, and how likelihood and consequences are highly dependent on the individual system under scrutiny.

System level: The likelihood of successful attacks based on the described threats described is not evaluated or assessed in the identified literature, with the exception of [42], where targeted attacks at system level are set as likely. However, the most frequently described threats are exploiting the interconnections and the IT-nature of the systems and are internet-based. Thus, it can be assumed that the probability of being attacked is higher compared to the proprietary systems and networks in the distributed elements of AMI. The HES and MDMS at system level are also considered targets with a potential higher pay-off if the attacker can obtain information on or gain access to them, thus being more attractive targets. However, this will most likely cause the security posture at system level to be higher, increasing the complexity, the required resources

and knowledge to be able to successfully breach security at this level. And by following the reasoning of [114], the likelihood should then be reduced.

5.1.5 Risk

Risk in terms of assessed risk as defined in Section 2.1.2 lacks a sufficient holistic approach by assessing both likelihood and consequences of threats in most of the identified literature. However, some attempts are made using methods such as STRIDE and DREAD ([90] and [112]), and modelling risk in as a combination of likelihood and severity in a risk matrix ([114] and [42]).

HW-level: The lack of evaluation of likelihood and consequences in the identified research makes it challenging to evaluate risk as a function of them both, and for HW it is only conducted by [42] in the SLR. In this study incidents at HW level (both SM and DC) are assessed, where modification of data and functionality affecting several end-users are considered high risk incidents.

Nonetheless, there are some articles that convey observations and reflections of how risk is affected and can be handled. [107] describes how the likelihood of HW tampering has increased due to a long and exposed supply chain, and the ubiquitous presence of devices in the field, thus increasing the risk in total. Similarly, [43] describes how the widespread use of AMI will increase the likelihood, and additionally how the increasing numbers of connected devices and a more diverse set of system vendors will increase the overall risk by increasing the complexity, the number of attack vectors and increasing the reach and impact of successful attacks. Additionally, 3 of the articles also identify certain techniques and systems useful in identifying and evaluating risk. [108] proposes trust systems in relation to risk assessments of systems, where trust models can be used to identify risks and to give assign weight to them, e.g., by using a trust management system to verify if the SM generate malicious measurements on energy consumption. However, trust models are typically based on reputation systems, which rely on previous experiences to rate the devices or systems under scrutiny. In terms of information security and risk assessment in AMI, there is lack of data on attacks, making it potentially challenging to rate their performance. However, as noted in [43] the system owners will need to conduct risk assessment on a regular basis for their system, in order to continually update and evaluate their information security posture. In this regard, [90] proposes the use of threat models (such as DFD, STRIDE, Attack Tree and DREAD) which can produce valuable input to the risk assessments. These models are versatile in nature, easy to use and applicable to AMI, producing clear and easy to understand presentations of the system and its threats.

Communication channels: Similar as in HW, the lack of evaluation of likelihood and consequences in the identified research makes it challenging to evaluate risk as a function of them both. However, both [114] and [112] evaluate the risk of incidents or specific threats and present them in matrices, where each threat is evaluated and weighted against each other, using different basis and techniques.

In [114], likelihood and severity are subjectively evaluated for each identified threat identified, using a scale of low, medium and high for both. The definition of likelihood is based on the attack's probability of being performed, which is dependent on the complexity of the attack (e.g., the resources and knowledge required to be able to successfully carry it through), while severity is based on which security objective that is breached by the attack. The priority order in the SG in terms of security objectives are

availability (considered the most important), with integrity, accountability and confidentiality following. Thus, threats breaching availability are deemed to have high severity, while breach of confidentiality will have low severity. This results in the matrix presented in Table 4.4 for the identified threats.

Similarly, in [112], a risk matrix is presented. This research is using similar models and follows to a certain extent the recommendations described in [90], but additionally uses DREAD for risk assessment. The model rates the five most common wireless threats into five categories: 1) Damage, which states the severity of the attack, 2) Reproducibility, which states how complicated it is to reproduce the attack, 3) Exploitability, which is a measure on how resource- and knowledge intensive an attack is to conduct, 4) Affected clients, which states the consequence of the attack in terms of affected devices or clients in the network, and 5) Discoverability, which is a measure on how challenging it is to disclose the attack. Table 4.3 visualizes the result and show the risk ranking from medium to high risk for the threats analyzed. This is very much a subjective analysis, where the score given within the categories for each threat lacks a statistical or a reasoned explanation in the article. As a subjective method, it is assumed that different people with different backgrounds could produce a wide range of scores for similar threats and categories. Further, the method does not directly consider the likelihood of each threat successfully exploiting a specific vulnerability, and thus does not evaluate risk as defined in Section 2.1.2.

In addition to the risk assessments conducted in [114] and [112], there are some articles in the identified body of research that makes observations and reflection of how risk is affected. Both [105] and [13] proposes the use of attack graphs to identify attack paths that are most likely to succeed, but in this regard they can also be used as a tool or basis for conducting risk assessments by representing vulnerabilities, threats and conditions for each attack combined in a model. [13] and [108] also look briefly at how PRA can be used in the SG for risk assessment, but as described in [13] the method relies on historical data and statistical examples which can be challenging to obtain due to lack of real-life examples of attacks impacting AMI. Regardless of the techniques used, the importance of conducting risk assessments is underlined in [43] and [85]. It should be conducted as a continuous process to determine if the security posture is adequate and with acceptable risk to keep the pace of ICT development and the ever-evolving threat landscape. As mentioned in HW, [90] also proposes different useful tools in this regard, which can provide valuable input in risk assessments, i.e., DFD, STRIDE and Attack Tree.

Further, as mentioned for HW, [43] emphasized how the increasing number of devices will increase the overall risk. This is also extended to the increasing number of connected networks in the infrastructure, which entails a more complex structure and an increased number of attack surfaces and entry points into the target network. An increased number of devices and interconnected networks also entails a higher volume of traffic passing through the networks, making them potentially more attractive as a target and more prone to disruptions and availability challenges. The development and availability of attacker tools as described in [104] further complicates and increases the risk for networks attacks, by exploiting the interconnected nature of the networks, the vast number of connected devices to these networks, and the obscurity that the complex infrastructure entails.

System level: As for HW and to a certain extent the communication channels, the lack of evaluations or calculations on likelihood and the overarchingly described impacts

makes it challenging to evaluate risk as a function of likelihood and consequences. Only [42] does a risk assessment for incidents at system level, where targeted modification of data, manipulation of functionality (breaker) and theft of data is considered a high risk. But as for HW and communication channels there are some articles related to system level that convey general observations and reflections on how risk is affected and can be handled in the SG and AMI ([105] and [43]). These considerations have been mentioned when discussing the communication channel and are valid for the system level as well.

5.1.6 Summary of SLR

The previous sections described the different levels in AMI, and the challenges identified by the body of research included in the SLR. The findings are tabulated in Table 5.1 and represent the most prominent elements relevant for comparison with the stakeholders' perception of vulnerabilities, threats, consequences, likelihood, and risk.

Deductive list				
Code	**Category**	**Name**	**Detail**	**Definitions**
DV1.1	Vulnerabilities	HW	Physical	The physical access to HW and interfaces makes them vulnerable for physical and logical tampering
DV1.2			HW design	Resource constrained HW with limited ability to handle security controls and/or handle attacks
DV2.1.1		Communication	Technology and protocol design	The technology used may have inherent vulnerabilities in its protocols or specifications
DV2.1.2				Limited bandwidth
DV2.2			Medium	The public access to the medium (wired or wireless) makes it susceptible to attacks
DV3.1		System level	SW/FW	SW/FW may have faults/vulnerabilities and needs to mature in design, testing and operation
DV3.2.1			Platform	The IT-nature of systems
DV3.2.2				Interconnections between systems from MDMS and to the corporate WAN
DV3.3			Technology	IP-based communication between networks
DV4.1		Organizational	Management	Policy, procedures, and training insufficient or lacking (weak security policy and poor cyber hygiene)
DV4.2			Complex supply chain	High vendor diversity and a long supply chain increases complexity and potential vectors
DT1.1	Threats	HW	Physical	Physical tampering and modification
DT1.2			HW design	Attack different layers in the protocol stack, often by physical access to device
DT1.3			Data and information	False data injects, interception and modification of data/SW/FW
DT1.4				Extraction of data and information
DT1.5				Delay or deny availability of data
DT1.6			SW/FW	Extraction of SW or FW
DT1.7				Manipulation and tampering in supply chain
DT1.8			Signalling and commands	Delay or deny signalling and/or commands
DT2.1		Communication	Technology	Technology-specific attack (Attack different layers in the protocol stack)
DT2.2			Medium	Medium-specific attack (wired or wireless)
DT2.3.1			Signalling and commands	Interception and modification of commands in transit
DT2.3.2				Delay or deny signalling and/or commands
DT2.4.1			Data and information	False data injects, interception and modification of data in transit
DT2.4.2				Disaggregation and de-pseudonymization of data
DT2.4.3				Extraction of data and information
DT2.4.4				Deny or delay availability of data
DT2.4.5			SW/FW	Extraction of SW or FW
DT3.1.1		System level	SW/FW	Malware or malicious code in servers
DT3.1.2				Extraction of SW or FW
DT3.2.1			Data and information	False data injects, interception and modification of data in servers
DT3.2.2				Disaggregation and de-pseudonymization of data
DT3.2.3				Extraction of data and information
DT3.3.1			Signalling and commands	Modification of commands
DT3.3.2				Delay or deny signalling and/or commands
DT3.4			Targeted	Targeted and compound threats derived specifically to affect AMI through HES
DT4.1		Threat actor	Local	Insider or use of open-source tools for social engineering
DI1.1	Impact and consequences	HW	Physical	Rendering HW inoperable (e.g., bricking of device)
DI1.2.1			Integrity	Theft of power
DI1.2.2				Denial of power

DI1.3			Data and information	Theft of data
DI1.4			Availability of service	Hindering or blocking commands (DoS) locally
DI2.1		Communication	Power	Theft of power
DI2.2			Data	Theft of data
DI2.3.1			Availability of service	Denial of power
DI2.3.2				Hindering or blocking commands (DoS)
DI2.4			Operation	Unreliable and insecure operation of the grid or devices
DI2.5			Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))
DI3.2		System level (AMI and SG)	Data	Theft of data
DI3.3			Availability of service	Denial of power
DI3.4			Operation	Unreliable and insecure operation of the grid or devices
DI3.5			Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))
DL1.1	Likelihood	HW	Accessibility	The access to the medium can increase attempts
DL1.2.1			Quantitative data	Lack of statistical and historical data
DL1.2.2				System and implementation dependent
DL2.1		Communication	Accessibility	The access to the medium can increase attempts
DL2.2.1			Quantitative data	Lack of statistical and historical data
DL2.2.2				System and implementation dependent
DL3.1		System level	IP-platform	IT-nature of systems and IP-based communication increases likelihood
DL3.2			Interconnections	The interconnections between systems and to internet at top-level increases likelihood
DL3.3.1			Utility	Higher pay-off for attacker increases likelihood for attempts
DL3.3.2				Higher utility entail higher security (reduces likelihood for successful attacks)
DL3.4.1			Quantitative data	Lack of statistical and historical data
DL3.4.2				System and implementation dependent
DL4.1		General	Complexity	Attack complexity in terms of knowledge and resources may affect likelihood
DR1.1.1	Risk	HW	Supply chain	Increased risk of HW tampering
DR1.1.2				Vendor diversity increases complexity and risk
DR1.2			Ubiquitous	Increased presence and widespread use will increase risk (will be scrutinized by both malicious and non-malicious actors)
DR2.1		Communication	Utility	Increased data and information can increase utility and overall risk for breach of CIA
DR2.2			Ubiquitous	Increased presence and widespread use will increase risk (will be scrutinized by both malicious and non-malicious actors)
DR3.1		System level	Utility	Aggregation of data and information increase utility and overall risk for breach of CIA
DR3.2			Consequence	Breach at system level will increase severity and reach of consequences

Table 5.1 Identified elements of risk in SLR

5.1.6.1 The concept of risk in the literature

The meaning of the term information security risk will have different substance depending on the chosen definition. This study has used the definition from ISO and NIST, and based on this, a risk assessment will include an evaluation of likelihood and consequence. As described in the previous sections, there are only a few studies that fully assess risk according to this definition, but the other articles provide nonetheless valuable input into defining the risk landscape for AMI as seen in the literature.

The level of detail in all descriptions of the elements of risk is in general overarching in nature and does not necessarily go into detail concerning operationalization of threats and vulnerabilities. The lack of detailed vulnerability, threat, attack, and impact descriptions in literature may be due to the sensitivity and the damage potential of such information. Thus, to avoid providing a recipe for malicious actors, in a Norwegian context, the energy sector and AMI is considered a critical infrastructure, and as such is subject to regulations concerning sharing and publication of information (i.e., by the Energy Act § 9-3 [46] and the Power Contingency Regulation § 6-2 [56] as described in Section 2.2.1.2). This prevents actors in the Norwegian energy sector and academia from providing detailed data and information of such categories through open sources and publicly accessible databases used in this SLR.

Research methodologies used within the body of research identified in the SLR covers both qualitative and quantitative methods, describing the elements of risk in theory or through simulation in lab and testbed environments. However, none of the studies have conducted tests in full-scale scenarios in a real-life setting, i.e, in an implementation of AMI. This entails that there may be a degree of uncertainties in the external validity of the results in terms of how applicable the studies are to real-world implementations of AMI with a complete value chain. Table 5.2 describes the different approaches used and shows the lack of practical and full-scale testing and verification of results.

References	Theoretical	Testbed	Simulation	Proof-of-concept	Survey - review
[1], Security analysis of an advanced metering infrastructure, 2017	X				
[13],Cyber-security on smart grid: Threats and potential solutions, 2020					X
[42], Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter I AMS, 2012	X				
[43], Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision, 2022					X
[60], Smart Meter Modbus RS-485 Spoofing Attack Detection by LSTM Deep Learning Approach, 2022		X		X	
[61], By-design vulnerabilities in the ANSI C12.22 protocol specification, 2015		X	X		
[85], Security of Power Line Communication systems: Issues, limitations and existing solutions, 2021	X		X		
[86], False data injection threats in active distribution systems: A comprehensive survey, 2022					X
[87], Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts, 2022					X
[88], Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure, 2015			X		
[89], Communication Security for Smart Grid Distribution Networks, 2013					X
[90], Threat Modelling of AMI, 2013	X			X	
[109], Smart grid security: Attacks and defence techniques, 2022					X
[99], Exploration of Smart Grid Device Cybersecurity Vulnerability Using Shodan, 2020	X				
[100], Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure, 2015	X				
[101], Review of Cyber-Physical Attacks and Counter Defence Mechanisms for Advanced Metering Infrastructure in Smart Grid, 2018					X
[102], Attacks, vulnerabilities and security requirements in smart metering networks, 2015					X
[103], A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure, 2015	X				
[104], Communications Systems in Smart Metering: A Concise Systematic Literature review, 2022					X
[105], Advanced metering infrastructures: security risks and mitigation, 2020					X
[106], A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid, 2015	X				
[107], Performance analysis of smart metering for smart grid: An overview, 2015	X				
[108], The role of communication systems in smart grids: Architectures, technical solutions and research challenges, 2013	X				
[114], Cyber-security in smart grid: Survey and challenges, 2018					X
[110], Data-centric threats and their impacts to real-time communications in smart grid, 2016	X		X		
[111], Authentication for Smart Grid AMI Systems: Threat Models, Solutions, and Challenges, 2019	X				
[112], Threat Modelling of Wireless Attacks on Advanced Metering Infrastructure, 2019	X				
[113], An information security model for an IoT-enabled Smart Grid in the Saudi energy sector, 2022.	X				X
[115], Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures), 2022	X				X
[116], 5G as an Enabler for Secure IoT in the Smart Grid: Invited Paper, 2019	X				
[117], Analysis of the impact of data granularity on privacy for the smart grid, 2013	X		X		
[118], Survey in smart grid and smart home security: Issues, challenges and countermeasures, 2014					X

Table 5.2 Research methodologies used in body of research

5.2 The stakeholders' perception of information security risks in AMI

Based on the chosen methodology in Section 3.2.2 and the analysis of the interviews in Section 4.2, three main themes emerged. These themes serve as the structure of the following chapter.

5.2.1 Perceptions of risk

5.2.1.1 Perceptions of the concept of risk

As described in Section 2.4, perception of risk concerns the ability to identify the different interdependencies and the links between cause and effect. The degree of complexity and uncertainty are provided as two of the most prominent factors distorting the ability to link cause and effect in this regard, further affecting how the perception of risk develops. As described by Endsley and Jones in [65], perception based on incomplete or inaccurate knowledge of causes and effects is the single most cause of errors in developing accurate SA, and in this case cyber SA.

In terms of defining concepts, the study only defined the concept of risk as a function of likelihood and consequence to the participant in the initial structured interview. However, the answers provided by the participants further in the semi-structured interview show some divergence in the use of concepts related to risk as described in Section 4.2.4.1, compared to the definitions in literature described in Section 2.1.2.

Cyber risk was considered both as attacks, impacts, vulnerabilities or threats, or as combinations of likelihood and consequence (5 participants). The divergence in how the term risk is used can indicate differences in their understanding of the concepts, which further impacts how their cyber SA is built. A misunderstood concept can lead to a participant failing to perceive information relevant to their SA, or misperception of information inputs, causing errors in developing accurate SA already at level 1 in Endsley's mental model (see Section 2.4).

The level of SA is not specifically measured in this study, but when challenged regarding what builds their individual cyber SA, most of the participants stated that their SA is based on information received within their own organization. They are relying on others for providing tailored cyber and information security updates, but the different perceptions of the concepts of risk, threats and vulnerabilities can nonetheless create individually divergent cyber SA. An erroneous perception of what the different elements or risk contain can further distort how they individually comprehend the situation and state of information security, and further affects how they are able to predict how an incident will affect them and the organization. This indication of a potential lack of a uniform understanding of risk concepts can cause different or erroneous perceptions of risk and risk levels, which in turn affects their cyber SA.

5.2.1.2 Perceptions of the most prominent vulnerabilities

The different participants highlight several aspects of AMI that are perceived as vulnerable to attacks with the intent of affecting information and the information systems in AMI. Vulnerabilities are discussed in relation to dependencies, the complexity of systems, and knowledge and training based on the findings in Section 4.2.4.6.

- **Dependencies**

Critical societal functions such as the supply of energy have become increasingly dependent on ICT and both digital and analogue value chains in this regard (see Section 2.3). An increased span and complexity in this chain makes it challenging to have a complete overview of all assets and uncertainties as to where vulnerabilities are and what vectors are exposed.

Six of the participants pointed out concerns regarding how exposed the value chain is for HW and data in a Norwegian context. This is based on three factors: the number of potential vendors, the length of the supply chain, and the use of open tender competitions for public procurement in Norway.

The length of the supply chain, where each vendor may have several sub-vendors, distorts the participants' view of the involved party, forcing them to rely on trust and stringent security requirements to vendors regarding supply chain security. A considerable concern is that highly motivated and resourceful malicious actors (i.e., nation state actors) will target the weakest link in this chain to manipulate HW or SW/FW, as experienced in other areas (see Section 4.2.4.6). A complete overview of the supply chain with all its levels is deemed unfeasible, but persistent communication and active control through security requirements and audits are seen as important steps in achieving improved transparency in the supply chain.

The dependence on a limited number of vendors and service providers for AMI in Norway further makes targeting their supply chain more attractive. A single compromised vendor or provider will potentially impact a significant number of end-users, using the same HW with malicious components or being updated with similar FW or SW containing malicious code.

The DSOs and AMI operators also have considerable dependence on the limited number of vendors and providers in terms of outsourcing of AMI- services, either partially or through a complete operation of AMI. Several of the participants raise concerns about the level of outsourcing and how it both creates a knowledge gap within the DSOs or AMI operators, but also contributes to complacency in terms of information security. This gap of knowledge can contribute to failure to perceive information relevant for building improved cyber SA as (see Section 2.4.1), thus affecting their perception and comprehension of risk. They may be to a larger extent forced to trust the information and assessment conducted by third parties, further consolidating their dependence on these parties. This dependence and trust on others for overall security in AMI may further influence the perception of risk and reduce it if the actors believe that the risks are known by their providers, similar to what is found in [68].

- **Complexity of systems**

In level 1 of Endsley's model for building cyber SA, perception is heavily influenced by the complexity of the environment and the systems and the abundance of data and information (see Section 2.4.1). The complexity will challenge the individual's ability to perceive information relevant for their SA, which is substantiated by most of the participants. 15 of them deem the complexity of the system as a significant vulnerability, challenging a holistic overview of risks within the system. This can indicate that trust is a significant factor as described in Section 2.4.3, due to the

overall perception of a low risk level in terms of cyber risks in AMI and how several of the participants also mention how security within in AMI is considered a joint effort.

The complexity of the system is further increased with challenges in the updateability and the technical lifespan of the distributed elements such as SMs and DCs. These challenges can introduce new vulnerabilities in terms of HW and FW being outdated and/or missing security patches. The lifespan of devices is considerably longer compared to regular IT- systems and as such requires considerable efforts in predicting future technological developments regarding security and functionality. However, the system will need to be able to handle both legacy and new systems due to long, but different lifespans of devices, adding to the complexity.

- **Knowledge and training**

The interviews show that some of the participants perceive an insufficient level of specialized knowledge and training in information security amongst the actors. This also coincides with the statements from most of the participants perceiving the security of AMI as a joint effort, where most of the actors are mutually dependent on each other for competence and knowledge.

As stated in the research by Skotnes in [67] and further cited by Larsen et. al. in [68], the level of knowledge about the risks being exposed to can affect the level of risk perception, i.e., an insufficient level of knowledge and training will increase the level of perceived risks. However, as described earlier, the general perceived level of information security risk to AMI is low by most of the actors, changing the outcome. This can be based on the availability heuristic and optimistic bias, as there is a lack of known incidents and a perceived low utility for attackers.

5.2.1.3 Perceptions of the most prominent threats

The threats include both physical and cyber-threats, where the former can be used as a precursor and enabler to the latter.

Manipulation and tampering with data, SW and FW is perceived as one of the most prominent threats, as the integrity objective is considered one of the most important features. The most adverse threat in this regard is the data, commands, and signaling related to the breaker functionality at system level, producing the most severe and widespread impact by potentially cutting power to end-users. The overall risk to breaker functionality is however considered low by the participants, based on how unlikely they perceive such a scenario to be and the protective measures already in place. As the breaker functionality and the risk it poses are considered to be well-known in the sector (knowledge to science/experts) and the risk is perceived as controllable (controllability), these psychometric dimensions may seem to explain why the risk is still considered low.

Reconnaissance is considered by several of the participants as a considerable threat, by mapping out the infrastructure and potential vulnerabilities. The consequence of this threat is not direct, but through the use of this information to operationalize other types of threats. Further, reconnaissance is perceived to already be happening by using passive methodologies such as OSINT and is indicated as common knowledge amongst the actors. Using the psychometric paradigm, the immediacy of risk consequences can be low, as the consequences of this threat are not necessarily immediate and direct from this threat. Further, the common knowledge of cyber-reconnaissance as a threat implies knowledge to the exposed and knowledge to science/experts. This would then indicate

that the risk from reconnaissance should be considered low by the participants, but some of the participants still perceive the threat from reconnaissance as significant. Several of the participants highlight how reconnaissance to some extent is made easier by how information is spread on public sources and the lack of complete system-overview, indicating a lack of controllability of the threat, potentially overshadowing the other dimensions.

Traffic analysis and profiling is highlighted by some participants as a specific threat towards sensitive end-users, such as other critical infrastructures. Traffic can be intercepted and analyzed, but most of the participants also state how the security measures are perceived to account for this threat by encryption of traffic. This indicates that the threat is controllable as of now (controllability dimension), but 2 participants pointed to how advances in technology could make current encryption mechanisms obsolete.

Targeted attacks are indicated both in the structured and in the semi-structured interviews as one of the most severe threats, posed by nation state actors or insiders. At the same time, significant uncertainties regarding the actual capabilities and potential in targeted attacks in AMI are perceived, due to the general lack of knowledge of incidents and no experiences with the capabilities of nation state actors. Some of the participants refer to statements from governmental threat assessments which indicate that nation state actors will gain access if the expected utility is high enough. This uncertainty and uncontrollability may then increase the perception of severity and risk for targeted attacks, as in the controllability dimension of the psychometric paradigm.

5.2.1.4 Perceptions of the most prominent consequences

The perception of consequences can be related to both physical and digital impacts but can be affected by the uncertainties in threat capabilities and the efficiency of implemented security mechanisms, implemented as stated by some of the participants.

- **Distributed HW and communication channel**

  The distributed HW (SM and DC) and the communication channels are perceived as secure with limited possibilities to cause severe consequences. The participants also state that the current security measures currently in place will handle what they describe as threats to the system. In this regard, Larsen et al. [68] describes a notion that demands for risk mitigation are often tied to consequences and not probabilities. Further, the study describes research on how difficulties in seeing or understanding cyber risks as severe incidents with disastrous potential can cause individuals to overlook the probability of cyber incidents happening. Based on the lack of incidents with consequences reaching AMI and the perception of a secure system reducing the potential severe consequences, a notion of low likelihood can be the result. However, the interviews show a mixed perception of likelihood in this regard, ranging from possible to unlikely (see Section 4.2.4.3).

  Looking at the psychometric paradigm, the notion of a low severity in consequences can produce a low perceived risk. Similar, as the system is perceived secure by the industry and the actors themselves with the implied thorough work on security during design and implementation, the knowledge to science/experts, controllability and knowledge of exposed dimensions may further reduce the perceived consequences and risk.

- **System level**

The more severe consequences a cyber risk is perceived to have, the higher the risk will be perceived to be according to the psychometric paradigm. Attacks on the system level are considered by the participants as what would produce the most severe consequences in AMI and is considered by the participants as the most attractive layer with the highest risk. Inversely, the likelihood is perceived as low by the participants. Compared to the distributed HW and communication channels, the system level is considered at a higher risk, but all are generally summarized as low risk in terms of cyber incidents. This perception is in line with the severity of the consequences dimension as described in the psychometric paradigm, where risks which are perceived to have higher consequences are perceived to be higher. The overall general perception of low risk at system level can be explained by the knowledge to science/experts and controllability dimensions: The consequences at this level are indicated to be well-known amongst the actors, and to be sufficiently mitigated and protected within the corporate network.

- **Physical consequences – Denial of power**

Denial of power is considered the most severe impact to end-users, due to the dependency of power that has been built up in modern society. It manifests itself as a physical consequence by cutting the power supply through the breaker functionality. Similar to attacks on system level, this is considered one of the highest risk factors in AMI but is perceived with a low likelihood and risk. This can be explained by the same indications as for system level, using the severity of consequences, controllability and knowledge to the science/experts dimension, and is not further elaborated on.

- **Loss of confidentiality, integrity and availability of data**

Traditionally speaking, the energy sector prioritizes availability, then integrity and lastly confidentiality as described by several participants. However, in AMI both integrity and confidentiality may need to be elevated, whereas availability of data and devices in the network is not necessarily crucial for the delivery of power to the end-users. A bricked device or lack of data from the device do not affect the power delivery as long as the breaker functionality is not triggered but will incur additional costs to the operator in terms of replacing devices or resorting to manual collection of measurement data. In a future scenario with more frequent measurements and increased usage of AMI data, the grid optimization and tertiary systems built around the increased availability of data may be more dependent on the availability of data.

Loss of confidentiality, integrity and availability is considered by several participants from different levels and organizations as potential consequences of breaches, with varying severity. However, as for system level and distributed HW and communication levels, the perceived security of the system and the thoroughness in the design and implementation is indicated to reduce the potential consequences and risks, as in the controllability and knowledge to the science/experts dimension.

- **Societal trust**

Societal trust is described by some of the participants as a potential consequence of a breach and is a more intangible consequence. As the security and cyber SA in AMI is considered a joint effort, it indicates a certain level of trust between the actors. The actors have varying degrees of competence and insights into information and

information systems in AMI and the energy sector and are dependent on each other for overall system security through the joint effort. Larsen et. al. [68] point to how the perception of cyber risks can be reduced if the risks are known by science/experts taking part in this joint effort, placing trust in their ability to control it. Thus, a loss of trust in the wake of a cyber incident can severely affect the joint effort and increase the perceived risk in AMI and the energy sector. At the same time, the objective risk can increase as well, if actors actively avoid using patches/updates from affected suppliers/vendors and choosing to live with potential vulnerabilities.

5.2.1.5 Perceptions of risks in AMI

- **Breaker functionality at system level**

The element with the highest risk is perceived to be the breaker functionality at system level. The level of consequence is high, but the majority of the participants perceive the likelihood as low due to the security implemented at this level, and thus perceive the overall risk to be low. This coincides with some of the dimensions in the psychometric paradigm: The ability to control the risk in terms of security measures and mitigative efforts put in place increases the controllability dimension. How the risk is known amongst the actors and within expert-communities such as CERTs further increases the knowledge of science/experts and knowledge of exposed dimensions. The severity of consequence dimension may be that which increases the perceived risk compared to other risk factors in AMI, however it is still perceived to be low.

- **Breach of data confidentiality, integrity and availability at system level**

Breach of integrity and confidentiality are considered as the most significant risks following the breaker functionality at system level. Breach of integrity can lead to financial loss and erroneous grid operation, while confidentiality breaches at this level may cause significant privacy challenges due to the amount of potential PII stored at this level. Compared to breaker functionality, the participants perceive the risk as lower, as in less severe consequence than cutting the power. An incident at system level is still considered to be unlikely, thus contributing to an overall low risk perception in this regard. The factors affecting risk perception can be similar to those describe for breaker functionality, as both resides within a protected corporate WAN with heightened security due to its perceived increased attractiveness, impact-potential and utility for attackers.

- **Distance to information security risks in AMI**

Most actors see the elements of AMI as secure and perceive the system as being too proprietary and not being attractive or providing low utility for attackers. Such a notion can be based on an unrealistic optimism regarding security and how exposed the distributed elements are to cyber risks or related to no experiences of severe cyber incidents and attacks affecting AMI. This can indicate a notion of distance to consequences and the effects of information security risks in AMI.

Unrealistic optimism concerns how the participants perceive the overall information security risks as low towards AMI. This is based on beliefs that AMI is not an attractive target in itself and not directly connected to other publicly available systems such as the internet. Several of the participants said it is difficult to see what motives attackers would have for targeting AMI due to the resources and effort

necessary to succeed, and the expected utility of targeting AMI compared to other energy systems.

The cyber incidents briefly described by participants were related to malicious attacks on IT systems at the corporate network, resulting in no known consequences or effects towards AMI. The most severe consequence in AMI is perceived to be incidents related to breaker functionality but are considered unlikely and of low risk. This is also the general trend that makes the participants to see the overall risk for successful cyber incidents in AMI as low.

Unrealistic optimism or biased optimism are described in both [68] and [67], where individuals may display a biased optimism when facing cyber risks. Together with the perception of distance to cyber risks that is indicated by the participants can give the notion of divergence between the actors' perception of risk and the likelihood for cyber incidents in AMI. This distance to risk can be further enhanced by the level of dependence on others (Section 4.2.4.6) and the trust that the actors places within and between themselves in the joint effort of securing AMI (Section 4.2.4.4).

- **An observation on how participants' perception of risk in AMI can be formed:**

An example of how perception can be formed can be given by looking at how the DSOs describe their risk perceptions of the distributed layer and further how they perceive and build their own cyber SA.

In general, the distributed layer with HW (SMs and DCs) and the communication channels are perceived as secure from attacks due to the implemented security and control measures such as encryption, Intrusion Detection Systems (IDS) and logging. Thus, the overall risk is perceived as low by the participants, which can be linked to the controllability and knowledge and to the science/experts dimensions in the psychometric paradigm. When the distributed elements of AMI are perceived secure and reliable, and the actors can operate and understand the system in a safe manner, it can enhance the feeling of controllability can be enhanced. This can be substantiated by the participant's perception that the most frequent types of cyber incidents in the energy sector are occurring towards in the IT- systems at DSO control centers and corporate networks, where most of it is stopped and with no known incidents affecting AMI.

In terms of cyber SA, it can be built and formed by both the responsibilities put on DSOs from regulations and the inherent complexity of AMI and the energy sector. The mandatory regulations as described in Section 2.2.1 are assumed to provide a basic but sufficient level of protection when adhered to, providing functional and security requirements for information and information systems. Further, the regulations are not technology-dependent, but system-dependent and provide intentions rather than specific technical details, to be able to maintain relevance. This places considerable responsibility on the DSO for choosing and implementing sufficiently secure systems and organizational measures to ensure compliance. Knowledge and training in information security and system knowledge is then crucial to understand a complex system such as AMI. However, the majority of the participants highlighted how security in AMI is a joint effort, where no single actor has the complete picture of the system and its ramifications. They rely on others, such as their internal IT-departments, CISOs or external industry organizations (CERTS) and vendors to

provide updated threat and vulnerability assessments. Their own knowledge and understanding are not necessarily detailed considering technological vulnerabilities and threats in AMI. Coupled with a lack of experienced attacks, the participants at large may fall into the category of unexperienced to a certain extent, indicating that they do not necessarily have a sufficient mental model (as described in Section 2.4.1 and 2.4.2) to be able to both sufficiently perceive and comprehend information and inputs regarding the state of information security. This challenge can create biased perception of risk, as described by Skotnes in [67]. However, this is not measured in this study, and is as such it is just an observation on how the individual's perception of risk can be flawed or biased due to the lack of knowledge and understanding, and the dependence on others or third parties for cyber SA.

- **The outliers in risk perception of AMI**

The end-users are generally perceiving the risk in terms of likelihood and consequence as higher compared to the other actors, considering the overall risk to information security in AMI in the range of high and extreme. At the same time the end-users indicate a lack of detailed knowledge of AMI -technology and its implementation, both in the structured interviews - in the range of low to intermediate in terms of information security proficiency in AMI - and the semi-structured interviews. This coincides with the findings in [68] and [67], where the knowledge of the systems and of the cyber risks they are exposed to, influences the perceived level of risk. Limited knowledge thus increases the perceived level of risk and can serve to indicate as to why the end-users become outliers in terms of perceived level of risk.

5.2.2 Influencing factors

The study additionally explored the participants' notion of influencing factors of cyber SA and further on their perception of risk in this regard.

- **Cyber SA – Dependence on others**

Cyber SA and perception are closely related as described in Section 2.4, where level 1 SA concerns the individual's ability to perceive the states and attributes of elements in the environment. A complete and accurate SA in level 3 is dependent on sufficient knowledge and the value of the elements to obtain a more accurate perception in level 1, e.g., meaning that the individuals are capable to obtain relevant information concerning cyber security in AMI, concerning their own and the organizations tasks. This perception is used to give meaning and significance of the perceived information in level 2, and produce comprehension of the situation, risk or incident, meaning that the individuals are able to define the significance of the information to the state of cyber security according to the goals and objectives.

Most of the participants stated how they are dependent on others for information and updates on the state of information security in general and AMI in specific (see Section 4.2.4.4). The indicated complexity of the systems and the scarcity of detailed technical knowledge of all the different elements in the system entail a dependence on others for a more complete cyber SA, both for information and knowledge sharing regarding the state of security. To some extent can the complexity, the knowledge scarcity, and the dependency on others for information and knowledge indicate that they may have finite ability to themselves perceive what information is relevant (level 1 cyber SA) and further to define the significance of the information (level 2 cyber

SA). Thus, they may be dependent on others to be able to communicate cyber risk information in an appropriate manner for them to sufficiently perceive and comprehend the information to build relevant and correct cyber SA. This communication and information sharing also need to consider how perception of risk can influence the recipients' motivation to receive risk information and communication. As described by Larsen et al. [68] referencing the work of [119] and [120], individuals may be less motivated for mitigation of risk or attentive to communication of risk if they do not perceive themselves or their systems at risk.

- **Cyber SA – Lack of incidents in AMI**

None of the participants were aware of any malicious cyber incidents affecting AMI in Norway, and only a few incidents abroad were briefly recalled. The lack of incidents can be linked to the availability heuristic (see Section 2.4.3) and creates biased perception of the risk (subjective risk) compared to the objective risk (the actual number of incidents). However, in this case there is currently no statistical evidence of such a discrepancy.

In biased optimism another significant factor is the controllability of the threat and the feeling of being able to protect the systems [69]. In AMI, the majority of the participants perceive the system as secure with low risk of successful malicious cyber incidents, indicating that they are able to handle and control the threats both at distributed and system level. They believe that most of the attacks in the energy sector happen at the corporate network and towards IT networks due to their connectivity and attractiveness. Thus, creating the notion that IT systems are more inclined to experience cyber incidents and is where the attackers will most likely put their resources at play. Despite this, successful attacks at the distributed level may have severe consequences at the distributed level as well, both in terms of physical effects (cutting power) and financial impacts (loss of integrity of data for settlements and loss of confidentiality PII) for the individual end-users. For example, attackers may target end-users such as other critical infrastructures (e.g., telecom or defense) or high-profile individuals at critical times to obtain a strategic effect in terms of affecting national security.

5.2.3 Information security focus

The developed cyber SA may influence the information security focus that the actors have and the effort they put into further enhancing the security.

The participants describe how several factors influence their area of focus in information security:

- **The international security situation and the technological development**

The evolving international security situation and the rapid development in technology are stated as affecting the perception of threats, threat actors and their potential. It is indicated that the development is sharpening their focus on the potential effects and contributing to raising their guard in terms of cyber security vigilance. The complexity of the situation and the rapid changes as of today entail uncertainties in the capabilities and motives of attackers and challenges the knowledge and competence of the actors, implying the need to keep a persistent focus. This further indicates that the feeling of controllability is lowered as the nation state actors are seen as a considerable threat actor (see Section 4.2.4.5). Further, this may influence

and increase the participants' focus due to a higher risk perception as described in the psychometric paradigm (see Section 2.4.3).

- **The collaboration in the industry and with the regulatory authorities**

The collaboration and information exchange between actors and the effort by the regulatory authorities further affects the focus by increasing the actors' knowledge and enhancing their cyber SA. In terms of cyber risk communication this depends on the ability to provide relevant information, which aids the perception and comprehension of the information to improve SA, meaning information that can affect different perception dimensions, such as controllability and newness (e.g., new and unprotected vulnerabilities or zero-days have been discovered), and severity of consequences (e.g., an attacker can traverse from SMs to HES using zero-days). The regulatory authorities in this regard are both viewed as facilitators for collaboration and information exchange, but also to a certain extent as an enforcer of a focus by compliance requirements and audits.

- **The traditional focus of the energy sector**

The energy sector has traditionally had a focus on their main task of energy delivery and the associated functionality, as pointed out by several participants. Information security is then considered an additional task, not directly aiding in their main objective but entailing additional cost without directly generating revenue. The enforced focus through regulations and audits can then be seen as a necessary evil, where compliance can be seen as good enough. This coincides with the notion of a distance from cyber risks based on optimistic bias and lack of experience with cyber incidents as explained in Section 5.2.1.5. However, this is only the case for 2 participants (DSO#4 and 10), and all DSO participants see the regime of audits and controls as both useful and appropriate, contributing to an imposed persistent focus.

- **Personal interests and company resources**

Personal interests combined with allocated resources are considered as some of the key factors for information security focus amongst the actors. The notion of a joint effort in securing the AMI and the knowledge of other actors pursuing a persistent focus with allocated resources can be linked to the knowledge to science/experts and the controllability dimensions of actors lacking these factors. As there is a perception that knowledge and updates will trickle down to smaller actors, together with how the larger DSOs have increased capabilities to handle the challenges, a reduced perception of risk can further lead to relaxed and reduced focus for the other actors. This is indicated by some of the actors (O#2, DSO#3 and PV#1-2), while most of the remaining actors believe that the focus is there for all actors, both due to personal interests and regulations, but that the decisive factors are resources and competence to turn the focus into tangible action.

5.2.4 Summary of perceived risk factors from interviews

The previous sections described how the perception of risk amongst the participants of the study can be formed and affected. The analysis in Section 4.2 and its findings are tabulated in Table 5.3 and represents the most prominent vulnerabilities, threats, consequences, and risks described as compiled inductive codes. These will be compared to the findings in the SLR in Section 5.3. The remaining categories will be used as input and basis for discussions related to the comparative analysis.

The indications highlighted by the participants in the SSI are to a certain degree similar to some of the findings in the report on the state of digital vulnerabilities in the Norwegian society [59]. The digital value chain, the integration of IT/OT, dependence on others due to outsourcing and limited market are elements highlighted for both the general value chain in the energy sector, and the operational control centers and smart nets (or AMI) in the report, which are also elements highlighted by the participants (Section 4.2.4.6). In terms of AMI in specific, the tampering with functionality such as the breaker functionality at system level is highlighted by the participants as a considerable threat, introducing significant risk to the system and a potential factor of strategic importance to malicious actors (Section 4.2.4.5). Similarly, the report highlights the strategic vulnerability that such a functionality entails. Further, the report also considers the threat of manipulation and tampering of HW, data and functionality, both at the SMs, communication channels and at system level, where the interconnectedness increases the number of vectors. This is also highlighted by the participants, but where the risk at the distributed and communication level is considered to be lower compared to system level. Lastly, the report points to how there can be privacy challenges related to measurement data and how the power consumption is considered PII, potentially vulnerable to profiling threats. Few of the participants view loss of confidentiality as a considerable impact, and do not necessarily view the data as PII. The threat from profiling and traffic analysis is primarily highlighted by some of the end-users due to the criticality or sensitivity of their operations.

The similarity in identified factors from [59] and the findings in this study as described in the section above shows that these may be consistent challenges, warranting a persistent and future focus.

Inductive list related to risk factors				
Code	**Category**	**Name**	**Detail**	**Definitions**
IV1.1	Vulnerabilities	HW	Physical	The physical access to HW and interfaces makes them vulnerable for physical tampering and access to interfaces
IV1.2.1			HW design	Resource constrained HW with limited ability to handle security controls and updates (updateability)
IV1.2.2				Technical lifespan can be outpaced by ICT development
IV2.1.1		Communication	Technology	Limited bandwidth for data and updates
IV2.1.2				Technical lifespan can be outpaced by ICT development
IV3.1		System level	SW/FW	SW/FW may have faults/vulnerabilities and needs to mature in design, testing and operation
IV3.2			Platform	Interconnections between systems from MDMS and to the corporate WAN
IV3.3			Technology	IP-based communication between networks
IV4.1.1		Organizational	Complexity	Technological and cognitive complexity challenges the ability for a comprehensive overview of vulnerabilities, threats and consequences
IV4.1.2			Management	Inadequate knowledge and training in information security creates lack of experienced personnel
IV4.2			Service providers	Dependence on third parties (outsourcing of competence and data value chain)
IV4.3			Supply chain and market	Small market with few vendors entails low redundancy of service providers and HW (supply chain)
IT1.1	Threats	HW	Physical	Physical tampering and modification in operation and supply chain
IT1.2.1			Data and information	False data injects, interception and modification of stored data
IT1.2.2				Disaggregation and de-pseudonymization of data
IT1.2.3				Extraction of data and information
IT1.2.4				Deny or delay availability of data (DoS)
IT1.3.1			SW/FW	Extraction of SW or FW
IT1.3.2				Manipulation and tampering in supply chain
IT2.1.1		Communication	Signalling and commands	Interception and modification of commands in transit
IT2.1.2				Delay or deny signalling and/or commands
IT2.2.2			Data and information	False data injects, interception and modification of data in transit
IT2.2.3				Traffic analysis and profiling by disaggregation and de-pseudonymization of data
IT2.2.4				Extraction of data and information for traffic analysis and profiling
IT2.2.5				Deny or delay availability of data (DoS)
IT2.3			SW/FW	Extraction of SW or FW
IT3.1.1		System level	Signalling and commands	Modification of commands
IT3.1.2				Delay or deny signalling and/or commands
IT3.2.1			Data and information	False data injects, interception and modification of data in servers
IT3.2.2				Profiling by disaggregation and de-pseudonymization of data
IT3.2.3				Reconnaissance: Extraction of data and information on infrastructure
IT3.3.1			SW/FW	Manipulation and tampering in supply chain
IT3.3.2				Extraction of SW or FW
IT3.4			Targeted	Tailored attacks to enable traversal into HES and MDMS
IT4.1		Threat actor	Local	Insider or use of open-source tools for social engineering
IT4.2			Nation state actor	Competence and resources to target AMI by cyber, insider or open-source tools
II1.1	Impact and consequences	HW	Physical	Rendering HW inoperable (e.g., bricking of device)
II1.2.1			Integrity	Local theft of power (false consumption data)
II1.2.2				Local denial of power by manipulating commands locally
II1.3			Confidentiality	Local theft of data for profiling and extraction of PII

II1.4			Availability of service	Hindering or blocking communications (DoS)
II2.1.1		Communication	Integrity	Theft of power (false consumption data)
II2.1.2				Denial of power by manipulating commands in transit
II2.2			Confidentiality	Local theft of data for profiling and extraction of PII
II2.3			Availability of service	Hindering or blocking communications (DoS)
II3.1		System level	Availability of service	Breaker-functionality (denial of power)
II3.2			Confidentiality	Theft of data for profiling and extraction of PII
II3.3			Operation	Unreliable and insecure operation of the grid or devices
II3.4			Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))
II4.1		Societal	Trust	Loss of societal trust and trust in vendors and operators due to breach
IL1.1	Likelihood	HW	Accessibility	The accessibility to the HW can increase attempts
IL1.2			Quantitative data	Lack of statistical and historical data
IL2.1		Communication	Accessibility	The access to the medium can increase attempts
IL2.2			Quantitative data	Lack of statistical and historical data
IL3.1		System level	IP-platform	IT-nature of systems and IP-based communication increases likelihood
IL3.2			Interconnections	The interconnections between systems and to internet at top-level increases likelihood
IL3.3.1			Utility	Higher pay-off for attacker may increase likelihood for attempts
IL3.3.2				Higher utility entail higher security (reduces likelihood for successful attacks)
IL3.4			Quantitative data	Lack of statistical and historical data
IL4.1.1		General	Complexity	Attack complexity in terms of knowledge and resources may affect likelihood for attempts
IL4.1.2				The complexity of the system and uncertainties in capabilities of threat actors make predictions on likelihood challenging
IL4.1.3			Utility	Low likelihood perception at all levels
IR1.1	Risk	HW	Utility	Low risk perception (low likelihood and consequence)
IR1.2.1			Supply chain	Low vendor diversity
IR1.2.2				Long and complex supply chain increases attack vectors and risk
IR1.3			Ubiquitous	Increased presence and widespread use will increase risk for attempts (will be scrutinized by both malicious and non-malicious actors)
IR1.4			Ease of access to HW	Lack of safe disposal
IR2.1		Communication	Utility	Low risk perception (low likelihood and consequence)
IR2.2			Ubiquitous	Increased presence and widespread use will increase risk for attempts (will be scrutinized by both malicious and non-malicious actors)
IR3.1.1		System level	Utility	Aggregated data and information can increase utility and overall risk for breach of integrity and confidentiality
IR3.1.2				Low risk perception (high consequence but low likelihood)
IR3.2			Confidentiality	Profiling and big data analytics from aggregated data
IR3.3			Integrity of data	Erroneous operation of grid and settlements
IR3.4			Availability	Lack of access to data may disturb market operations and settlements
IR3.5			Consequence	Breach at system level will increase severity and reach of consequences
IR3.6			Breaker functionality	Breach of integrity and further functionality increase severity in terms of physical impacts to end-users
IR4.1		Organizational	Risk assessments	Challenging to share and disseminate confidential and time-critical information

Table 5.3 Identified elements of risk in interviews

5.3 Comparison SLR and SSI – Where is the focus?

The chapter is organized according to the framework and categories developed during the SLR (see Section 5.1 and Table 5.1). The compiled inductive codes are categorized and tabulated in the framework, enabling a comparison between the SLR and the SSI.

5.3.1 Comparative analysis

The analysis was conducted by aligning the compiled inductive codes developed in the SSI (Table 5.3) with the deductive codes (Table 5.1) developed during the SLR. The complete overview of overlaps and mismatches is tabulated in Appendix E. The following subsections will describe the findings in terms of divergence between SLR and SSI. The code *"Not present"* with the color black is used where the code is only categorized within one of the methods. The color grey is used on codes containing similar factors, but with different viewpoints or with weak indications.

5.3.1.1 Vulnerabilities

Table 5.4 shows the divergence in described vulnerabilities, where the SLR and SSI have different areas of identified and perceived vulnerabilities.

- **HW and communication channels**

  In IV1.2.2 and IV2.1.2 some of the participants describe how the pace of ICT development is changing the preconditions. The lifecycle of development, roll-out and operation of HW may cause HW to be outdated at a faster pace than expected regarding information security. This requires the ability to maintain a persistent focus at HW security posture through the lifespan of HW, with surveillance and logging within the system (Section 4.2.4.8) to be able to capture sudden changes in security posture. Additionally, as a measure to substantiate such a persistent focus, FW and SW updateability need to be in place and ensured for the entire distributed chain (Section 4.2.4.8). The SLR does not describe the technical lifespan of HW and communication channels as a specific vulnerability but describes how risk assessments should be conducted on a regular basis to keep up with the pace in ICT development.

- **Communication channels**

  DV2.1.1 concerns technology and protocol designs that may have inherent vulnerabilities, where the use and maturing of the system over time can bring flaws in technology, code, and protocols into light. The SLR, with several articles such as [60] and [61], highlight these vulnerabilities, which are not considered by the participants as a significant element. The participants' perception of an initial thorough preparatory work with extensive testing prior to the implementation, as well as the implemented and overall security in the Norwegian system, means that they assume that the system will be able to mitigate and handle the abovementioned factors (Section 4.2.4.8). However, none of the participants states this with specific references.

  In DV2.2 the SLR further describes the ease of access to communication media (wireless and wired) as a potential vulnerability. The wireless medium is in this regard exposed, as RF- signals can easily be surveyed and mapped, even by commercially available tools. The participants however consider an attacker's utility by exploiting

vulnerabilities in the communication channels as low, due to perceived proprietary and complex technical solutions, requiring specific knowledge, equipment, and effort (Section 4.2.4.7). Further, they state how the requirements in the design and operation of the system will limit the potential for attacker- traversal between devices and communication channels (Section 4.2.4.7). This indicates that with compliance with regulations, vulnerabilities in one part of the system will not affect the operation and functioning of other parts, limiting the consequences of exploitation of vulnerabilities in the communication channels.

- **Organizational**

In IV4.1.1 the participants point to the complexity of the system and the challenge to obtain a holistic overview of the risk picture for AMI. The multitude of technologies, stakeholders and the interconnectedness challenge their cyber SA, requiring a joint effort to be able to secure the system sufficiently (Section 4.2.4.4). However, no one will sit with the complete picture of all the different vulnerabilities and attack vectors a threat actor could exploit. The literature identified in SLR does not focus on management and organizational challenges related to information security in specific but focuses on technology and individual elements in the system.

IV4.2 in SSI describes the perceived dependency the participants and the different actors have on third parties when operation, knowledge and competence are outsourced (Section 4.2.4.6). They rely on others to provide security, which will require stringent control measures such as a thorough SLA and data processor agreements to ensure compliance and an adequate level of security. In this regard, the in-house competence, knowledge, and information security focus is to some extent affected by the level of outsourcing of service- and operational tasks. It may reduce the retained ability to handle information security challenges on their own and create a certain distance to the challenges. Similar to IV4.1.1, this challenge is not highlighted in the SLR due to their focus on general implementations and the technical solutions, where the Norwegian implementation and its management is not considered specifically.

Both the SLR (Section 4.1.5) in DV4.2 and the SSI (Section 4.2.4.4) in IV4.3 have identified vulnerabilities within the complex and long supply chain of AMI technology, vendors and operators. However, their focus differs. The SLR highlights in DV4.2 the vast diversity and number of AMI vendors and technological solutions, and the resulting challenges in maintaining adequate cyber SA and technological understanding, as a complex vulnerability. It is described to be difficult to keep track of all the different technologies, subsystems and components, their security features, and potential vulnerabilities.

In a Norwegian context, the SSI in IV4.3 addresses the complex supply chain vulnerabilities unique to the Norwegian implementation. The participants state how the Norwegian market is limited in volume compared to other implementations and serviced by a limited number of AMI vendors and operators. Despite this, these vendors are perceived to have implemented highly secure AMI solutions with enhanced security features and controls that meet the demands stipulated by regulations during the procurement phase of the system. The main vulnerability in this regard is the reduced redundancy, where a small market with few vendors entails the potential to impact the sustainability of AMI. For example, by maliciously

targeting one vendor or service provider, a significant number of the total metering points and end-users in Norway can be affected.

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Vulnerabilities	HW	**Not present**			**IV1.2.2**	HW design	Technical lifespan can be outpaced by ICT development
	Communication	**DV2.1.1**	Technology and protocol design	The technology used may have inherent vulnerabilities in its protocols or specifications	**Not present**		
		Not present			**IV2.1.2**	Technology	Technical lifespan can be outpaced by ICT development
		DV2.2	Medium	The public access to the medium (wired or wireless) makes it susceptible to attacks	**Not present**		
	Organizational	**Not present**			**IV4.1.1**	Complexity	Technological and cognitive complexity challenges the ability for a comprehensive overview of vulnerabilities, threats and consequences
		Not present			**IV4.2**	Service providers	Dependence on third parties (outsourcing of competence and data value chain)
		DV4.2	Complex supply chain	High vendor diversity and a long supply chain increases complexity and potential vectors	**IV4.3**	Supply chain and market	Small market with few vendors entails low redundancy of service providers and HW (supply chain)

Table 5.4 Comparison vulnerabilities

5.3.1.2 Threats

Table 5.5 shows the divergence in described threats, where the SLR and SSI have different areas of identified and perceived threats.

- **HW**

DT1.2 describes threats to HW design and how threats may target different layers in the protocol stack, e.g., by targeting layers from the physical to the application layer to achieve the intended purpose. The participants do not specifically mention such threats, which can indicate that the perception of a relatively well-tested and secure system, based on the initial groundwork, has accounted for such threats (Section 4.2.4.8). Further, as stated by the participants, AMI and its technology constitutes a complicated system, where detailed knowledge of the risk factors of different specific elements can be challenging to get an overview over (Section 4.2.4.4). How risk perception is formed and the indicated distance to information security risks can further result in a missing focus on such threats, as they are not considered a risk.

IT1.2.2 concerns threats targeting data and information in HW, by disaggregation and de-pseudonymization attacks on data at SM. However, the utility is perceived as low, with limited PII available at the SM. Further, security audits, authentication and authorization regimes, a joint effort in building cyber SA for the system and general compliance with regulation is perceived to handle and mitigate this (Section 4.2.4.4 and 4.2.4.8). Both consequence and likelihood are perceived as low by the participants. The SLR does not specifically consider the threat from disaggregation and de-pseudonymization at HW-level, however, it is considered at communication and system level, where increased volume of data increases the utility.

DT1.8 considers how different attacks such as local DOS attacks on signaling and commands at HW-level can be performed to render the HW incapable of receiving or transmitting signals or commands. Attacks at this level can include the use of DT1.1 and DT1.2. This is not brought up as a specific threat by the participants. As described earlier, most of them perceive the utility as low at this level, with a low risk level due to minimal consequences.

- **Communication channels**

DT2.1 and DT2.2 describe technology and medium-specific threats to the communication channels, including threats to communication protocols such as ANSI C12.22 with routing table poisoning, and eavesdropping and different DoS attacks on wireless channels. Similarly, as to HW and DT1.8 and DT1.2, this is not mentioned as a significant threat by the participants. This can be based on similar reasoning as given for DT1.8, where a perceived low utility, lack of detailed knowledge and a supposedly secure system create a distance from such threats.

- **Threat actor**

IT4.2 concerns the threat actors originating from or supported by nation state actors. They are perceived to have both the competence and resources to pose as the most powerful threat actor, but with significant uncertainties regarding their capabilities and reach, but also the motives for targeting AMI in specific. It is generally believed that there is limited utility in AMI alone, but it can be targeted as part of larger efforts to affect the national security situation and to obtain strategic effects (Section

4.2.4.5) as the energy sector has become a strategic target for nation state actors (Section 1.2). The SLR largely does not focus on the potential threat actors and as such it provides limited descriptions.

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Threats	HW	**DT1.2**	HW design	Attack different layers in the protocol stack, often by physical access to device	**Not present**		
		Not present			**IT1.2.2**	Data and information	Disaggregation and de-pseudonymization of data
		DT1.8	Signaling and commands	Delay or deny signaling and/or commands	**Not present**		
	Communication	**DT2.1**	Technology	Technology-specific attack (Attack different layers in the protocol stack)	**Not present**		
		DT2.2	Medium	Medium-specific attack (wired or wireless)	**Not present**		
	Threat actor	**Not present**			**IT4.2**	Nation state actor	Competence and resources to target AMI by cyber, insider or open-source tools

Table 5.5 Comparison threats

5.3.1.3 Impacts and consequences

Table 5.6 shows the divergence in described consequences, where the SLR and SSI have different areas of identified and perceived consequences.

- **Communication channel**

  DI2.4 concerns how unreliable operation of devices and the distribution grid itself can be caused by several threats targeting assets such as state estimation (manipulating or injecting erroneous consumption data through FDI). This is not specifically considered by the participants, except for 2 participants highlighting how FDI can lead to erroneous decisions on the operation of the grid, potentially overload or cause a fine-tuned grid to not be operated optimally. However, several of the participants also point out how the distribution grid and the delivery of power is not solely dependent on AMI, with significant controls and mechanisms to conduct state estimation and to correct or adjust potentially erroneous data. This indicates that the Norwegian implementation and the requirements set for its operation in conjunction with AMI do not rely as substantially on AMI-data, in contrast to some of the literature identified and their assumptions and preconditions for the research (such as [88] and [86]).

  DI2.5 in the SLR outlines how financial loss can have a considerable impact due to breaches in the communication channels. This can be in the form of loss of revenue due to theft of power, loss of reputation affecting the market value, or by fines based on the level of privacy breach (GDPR-legislation). This is not a prominent concern within the participants, where the financial loss both in HW and communication level is assumed to be limited in scope (Section 4.2.4.7). Both the configuration and the required security mechanisms in AMI concerning both confidentiality and integrity (Section 2.2.1) is perceived to limit such consequences (Section 4.2.4.8).

5.3.1.4 Likelihood

Table 5.7 shows the divergence in described likelihood in terms of threats and attacks, where the SLR and SSI have different methods and descriptions of likelihood.

- **HW, communication channels and system level**

DL1.2.2, DL2.2.2 and DL3.4.2 concerns how the identified body of literature to a very limited extent describe or evaluate likelihood. They tend to describe general or theoretical systems, and do not deal with specific implementations of AMI. [90] states how both likelihood and consequence will depend significantly on the specific system implemented, which may indicate why there is a lack of such descriptions in the remaining literature. However, a few articles proposes different methods for calculating likelihood and risk, such as [13] and [105] describing attack graphs, but without implementing them on a specific system. In the SSI, the participants are challenged to assess the likelihood in relation to the Norwegian implementation, where they used subjective judgement, as described in Section 4.2.4.3 and defined in Section 2.1.2 and 4.1.4.

- **General**

IL4.1.2 in the SSI describes how some of the participants perceive the determination of likelihood as challenging, due to perceived uncertainties related to specifically to the capabilities of nation state threat actors' capabilities, potential and motives for attacking

AMI (Section 4.2.4.3). This is substantiated by the perceived complexity of the system affecting cyber SA (Section 4.2.4.4 and 4.2.4.8) distorting the overview of information security challenges, such as potential vulnerabilities and attack vectors. In the SLR, the complexity of specific system implementations and uncertainties regarding capabilities and motives are not analyzed. This is assumed due to the scope of the literature, that does not focus on threat actors and specific system implementations.

IL4.1.3 points to how participants perceive the level of likelihood for successful attacks in AMI, where both the distributed elements with HW and communication channel and the system level have a low likelihood assessment (Section 4.2.4.3). Their perception of likelihood can be formed by the lack of incidents and the perceived low utility of AMI compared to other elements in the energy sector. In this regard, the availability bias and unrealistic optimism (Section 2.4.3) can be influenced by a certain feeling of control of threats (the system is perceived to be secure, Section 5.2.1.5), and further substantiated by an indicated discrepancy between their overall risk perception of the system, and the actual increased targeting of the energy sector in general (Section 1.1 and 2.3). The literature in the SLR at large does not assess likelihood, and as such does not assess the level. Two articles ([42] and [114]) produce a likelihood description. [42] describes the likelihood of targeted attacks as being based on a combination of the severity of consequences (the number of affected end-users and DSOs) and the complexity of an attack (how easily it can be carried out). This is based on a generic Norwegian implementation. Targeted attacks are here given a default value of likely, where attacks with the capability to affect several users and DSO increases the likelihood. In a similar manner [114] describes likelihood as a combination of attack complexity and exposure of the target, providing general and not system-specific assessments.

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Impact and consequences	Communication	**DI2.4**	Operation	Unreliable and insecure operation of the grid or devices	**Not present**		
		DI2.5	Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))	**Not present**		

Table 5.6 Comparison impacts and consequences

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Likelihood	HW	**DL1.2.2**	Quantitative data	System and implementation dependent	**Not present**		
	Communication	**DL2.2.2**	Quantitative data	System and implementation dependent	**Not present**		
	System level	**DL3.4.2**	Quantitative data	System and implementation dependent	**Not present**		
	General	**Not present**			**IL4.1.2**	Complexity	The complexity of the system and uncertainties in capabilities of threat actors make predictions on likelihood challenging
		Limited descriptions			**IL4.1.3**	Utility	Low likelihood perception at all levels

Table 5.7 Comparison likelihood

5.3.1.5 Assessment of risk

Table 5.8 shows the divergence in described risk, where the SLR and SSI have different areas of identified and perceived risk.

- **HW**

DR1.1.2 and IR1.2.1 describe how the supply chain for AMI creates risk because of its extension and diversity. However, their focus or starting point is different. DR1.1.2 focuses on how the increased numbers of vendors and devices in the grid increase the complexity by different HW with different capabilities and connections, while an increased share of providers and vendors may undoubtedly contain rogue actors with questionable management and implementation of information security. This is described as a factor increasing the risk, by a complex market with a multitude of vectors and vendors. IR1.2.1 describes the perception of the Norwegian market, where a low number of vendors and providers reduces the redundancy in the market based on the few vendors available, limited variety in HW (SMs) and the dependency the actors have on third parties and external knowledge (Section 4.2.4.6 and 4.2.4.8). This is believed to increase the potential consequences, as targeting a single or a few of the vendors can affect a considerable number of end-users and metering points. However, the Norwegian market and energy sector is perceived to be functionally regulated with sensible and adapted regulations and organization (Section 4.2.4.8), where the participants in general consider the Norwegian implementation as one of the most secure. This further place considerable requirements on the vendors, potentially removing the rogue actors as described in DR1.1.2 and increases their focus on information security in their products and services.

IR1.4 concerns a perception stated by 2 participants, where a potential lack of a safe disposal requirement can increase the availability of HW for malicious actors, thus easing their efforts and possibilities for exploring and dissecting the HW for vulnerability discovery and operationalization of threats (Section 4.2.4.2), increasing the risk to HW. The literature in the SLR does not consider this;, however, it may be dependent on individual government regulations and requirements provided by the vendor.

IR1.1, IR2.1 and IR3.1.2 concern how the participants perceive the overall risk in the distributed elements of HW and communication channels and at system level as overall low. This is based on a stated low level of consequence and likelihood for successful attacks for IR1.1 and IR2.1, while at system level in IR3.1.2 the consequence is considered as high, but still perceived as unlikely and with low risk. This perception is indicated as based on how the Norwegian system is implemented and regulated (Section 2.2.1 and 4.2.4.8), providing a secure and state-of-the-art system. The risk level is only assessed in the identified literature in SLR in [42], and the lack of such assessment can be, as stated in [90], that such assessment is dependent on the specific implementation. In [42] at HW level, manipulation of data and functionality (breaker) is deemed a high risk if the incident affects a larger number of end-users. This implies the use of automation in attacks to be able to affect several SMs or DCs (Section 5.1.3).

- **Communication channel**

IR2.1 is described together with IR1.1 and IR3.1.2 in HW. In terms of the SLR, there are is limited work conducted on assessing risk at this level, with the exception of the work of [114] and [112]. They conduct assessments for specific threats within the communication channels producing matrices as tabulated in Table 4.4 and Table 4.3.

However, they do not provide an overall assessment of the communication channel as an asset.

DR2.1 in the SLR describes how increased utilization and more functionality in AMI will lead to increased volumes of data in transit within the communication channel, thus increasing the potential utility for malicious actors and increasing the overall risk for threats targeting the communication channel. Availability can be targeted, when more services become reliant on the data, and confidentiality can be targeted, as more data potentially means more PII and system information with increased value for e.g., big data analytics. This is not mentioned by the participants as a significant risk factor, as the Norwegian implementation and the communication infrastructure has limited the number of SM per DC and communication channel, thus reducing the number of end-users generating data. This indicates that a malicious actor will have to compromise communication between SMs and HES at several different channels in order to obtain a significant volume, thus potentially increasing the required effort and use of resources.

- **System level**

IR3.1.2 is described together with IR1.1 and IR2.1 under HW layer in this section. In terms of SLR and as described for HW, the risk level is only assessed in [42]. The article describes the targeted manipulation of data, manipulation of functionality (breaker) and theft of data as high-risk incidents, based on the potential to affect a larger number of end-users and DSOs.

IR3.6 and the risk for incidents to breaker functionality is perceived by the participants as the highest risk factor in AMI, when compared to incidents in HW and communication channels. However, the level of risk is nonetheless considered to be low as explained for IR1.1. Within the SLR, only [42] assesses the risk specifically for manipulation with functionality at system level and, as described above, is considered a high risk.

IR3.3 concerns how the need to maintain integrity of data at system level is considered a risk factor, where breaches can impact functionality such as the operation of the grid and billing functionality for settlements. The consequence of loss of integrity is represented as mainly financial cost to end-users and/or DSOs, and the loss of trust from other actors. As described in IR3.1.2, the overall risk is assessed as low based on a perceived low likelihood due to the implementation and present measures. This is not assessed specifically in the literature in terms of risk, but DR3.1 and DR3.2 point to how aggregation of data increases the risk by increasing the consequences. In order to affect the operation of the grid and billing functionality at a considerable scale, it is assumed that there is a need for aggregated data, thus falling into the same category but with different level of focus.

IR3.4 concerns how the risk of loss of availability of data may further cause financial impact to the actors, by potentially disturbing functionality related to areas such as market operations reliant on AMI data from MDMS, and the ability to conduct end-user settlements for their customer groups. The likelihood and consequence are perceived as for IR3.1.2, with a low likelihood and high consequence. The identified research does not assess the risk of loss of availability at system level but describes how the availability objective can be affected by threats such as injection of malware (e.g, ransomware) and insiders.

- **Organizational**

IR4.1 highlights how some participants indicate challenges in disseminating information and knowledge within the energy sector and notably in operational security for the AMI system (Section 4.2.4.8). This is not described in the literature in the SLR, as it is out of scope, based on how the SLR was conducted.

The challenges in dissemination can be substantiated by how the same participants perceive the organization of communication and notification channels as to a certain degree suboptimal, where actors to some extent must subscribe to incident notifications. This is further worsened by the complexity of AMI with a multitude of stakeholders and organizations. Additionally, some actors may face dilemmas in what information to disclose, potentially not disclosing security incidents, fearing negative effects on market trust and potential exploitation by malicious actors. Moreover, not all actors can receive classified information or updates, which can delay critical information from reaching them, affecting the basis for building relevant cyber SA and making risk-informed predictions and decisions. It is identified by some participants that more effective fora and channels for sharing knowledge and experiences are necessary to enhance the overall security of AMI and the energy sector, ensuring that necessary and time critical information will reach all the pertinent actors.

The need for increased cooperation and knowledge sharing is essential to improve information security and building cyber SA in a joint effort (Section 4.2.4.4). Lack of knowledge and expertise can be seen as a factor inhibiting the development of AMI cyber SA and is a challenging factor for the stakeholders. Several participants point out that there is a shortage of educated information security professionals within the energy sector, including the regulatory authority. It is an important factor that needs to be addressed in order to better secure and provide a reliable grid in the future with the potential implementation of new functionality and increased usage of data in AMI.

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Risk	HW	**DR1.1.2**	Supply chain	Vendor diversity increases complexity and risk	**IR1.2.1**	Supply chain	Low vendor diversity increases risk
		Not present			**IR1.4**	Ease of access to HW	Lack of safe disposal
		Limited descriptions			**IR1.1**	Utility	Low risk perception (low likelihood and consequence)
	Communication	**Limited descriptions**			**IR2.1**	Utility	Low risk perception (low likelihood and consequence)
		DR2.1	Utility	Increased data and information can increase utility and overall risk for breach of availability and confidentiality	**Not present**		
	System level	**Limited descriptions**			**IR3.1.2**	Utility	Low risk perception (high consequence but low likelihood)
					IR3.6	Breaker functionality	Breach of integrity and further functionality increase severity in terms of physical impacts to end-users
		Not present			**IR3.3**	Integrity of data	Erroneous operation of grid and settlements
		Not present			**IR3.4**	Availability	Lack of access to data may disturb market operations and settlements
	Organizational	**Not present**			**IR4.1**	Risk assessments	Challenging to share and disseminate confidential and time-critical information

Table 5.8 Comparison risk

5.3.2 Is there a need to address the divergence?

The comparison revealed several divergent elements between the literature in the SLR and the participants in the SSI. The following sections will discuss if there is a need to address these divergences based on the differences in perception and the research on information security challenges in the different layers of AMI.

5.3.2.1 The system is secure – Low risk perception in the Norwegian implementation

The divergence described in Section 5.3.1 revolves around all elements of risk. But the common factor indicated by the comparison is the perception by the participants that AMI with HW, communication and system level is secure. This is based on several factors, such as a thorough initial groundwork and requirements in regulations (Section 2.2.1 and 4.2.4.2), resulting in a perceived low level of risk for all levels as described in IR1.1, IR2.1 and IR3.1.2. There are only three articles in the SLR that assess the risk for AMI in relation to threats and incidents (Section 5.1.5). In [42], data manipulation, data theft and manipulation of functionality in HW and at system level are assessed as threats with high risk.

Observations SLR: The SLR highlights a technological perspective that outlines various potential threats, vulnerabilities, and risk factors against AMI technology. The current risk assessments that are published by the national security agencies (Chapter 1) emphasize that the energy sector is a primary target for nation-state threat actors, and as with all systems and implementations there exist both inherent and induced vulnerabilities. These publications provide clear indications for and reinforce the technological threats, vulnerabilities and risks outlined in the SLR. While the risk is perceived to be real, it is not assessed in the SLR. This can be due to the sensitivity and confidentiality of such information, as it can be argued that disclosure of information of this kind could provide a step-by-step guide for malicious actors on how to exploit the AMI system.

Complexity is also identified as a significant challenge in the SLR (Section 5.1.1). It is stated that it can be challenging to obtain an overview of the different technological components in the AMI value chain, as identified within IT, OT, and SCADA/CPS technologies. The study's SSI also identifies this complexity as a potential vulnerability and risk in the implementation of the Norwegian AMI (Section 4.2.4.2 and 4.2.4.6). Based on this, the study indicates that there is an absence of a complete and comprehensive overview over risk factors in AMI, implying a need for mitigating measures to build a more comprehensive and detailed cyber SA of the overall risk to the system.

Observations SSI: The participants in the SSI do not provide concrete technological justifications as to why they perceive the level of risk as low to the system overall and the different levels within. Instead, the actors refer to the regulatory requirements, the organization in Norway, the initial work with the system and the trust in the other actors as a joint effort in securing the system (Section 4.2.4.2 and 4.2.4.4). As a complex system, the actors are dependent on each other for both competence and security, which is further substantiated by increased outsourcing of competence and services in the operation of the AMI implementation.

However, as described in Section 4.2.4.8, the participants are divided in their view of how the regulations are designed and the organization of roles and responsibilities. Several of the participants view the regulations as partly inconclusive, while others again deem them as sufficiently concrete and open enough to not be technologically dependent. Furthermore, several participants perceive the organization of the different roles and responsibilities as complicated due to the vast number of different stakeholders and regulatory requirements. The stakeholders may have different perspectives, roles and authorities towards managing and regulating AMI and its actors and are perceived to introduce additional complexity. At the same time, there are other participants that view this organization as sufficient with relevant distribution of roles and responsibilities, building on the already established government agencies prior to the introduction of AMI.

In Section 4.2.4.4 and 5.2.1.4 several of the participants indicate how the main focus in the energy sector traditionally has been on the availability and integrity objectives of data and the obligation to deliver energy to the end-users. This is substantiated by the finding in the SLR (Section 5.1.3), prioritizing availability, integrity and –lastly- confidentiality. The main objective is to make the system work, providing a safe and reliable supply of energy. However, as described in Section 4.2.4.4, this focus is changing, both due to external factors but also by the need to stay compliant. This entails placing a considerable responsibility on the individual actor in establishing and managing systems and procedures for information security to reduce the risk to an acceptable level. Such responsibilities mean that the level of knowledge and competence must be raised within actors that do not necessarily have the resources or the prerequisites to meet them. The interest in information security and the CIA triad is there, but as described, the level of resources, outsourcing and personal interest are considered considerable factors affecting the ability to focus. These are factors that can vary based on the organizational size and can further enhance the vulnerabilities in knowledge and training, complex systems and dependence on others (Section 4.2.4.6). This is substantiated by the research in [67] described in Section 2.5.2, which indicates that both the size of companies (differences in security management, resources and outsourcing), the level of knowledge and the complexity can affect the perception of risk. A perceived divergent focus is described within the different actors in Section 4.2.4.4 and can raise concern about their understanding of the technical risks associated with AMI and information security. This emboldens the study to question whether the different actors have sufficient knowledge about the information security challenges across the entire value chain of AMI in specific and the energy sector in general.

Additionally, an increased risk (and potentially a systemic risk[49]) for incidents in the energy sector, as described in the national threat assessments (Chapter 1), may challenge their perception of a secure system with today's implemented technological and organizational security measures. The level of risk is perceived as low, with low consequence and likelihood in the distributed elements, and with high consequence and low likelihood at system level. As the energy sector is a prominent target, it is reasonable to believe that the risk to AMI, with a complex implementation and to some extent shared and accessible communication channels and distributed elements, is increasing.

This may indicate a need for a more comprehensive approach to AMI security considering both technological and organizational factors, potentially through an authority with the

[49] Systemic risk can be seen as the result of *"….risks spreading across interdependent systems."* [121, p.1606]

coordinating responsibility for information security in the energy sector. By consolidating the responsibility for information security on a single authority, some of the challenges described above may be mitigated or reduced. Such an approach would require a deeper understanding of the technical risks involved and a clearer delineation of roles and responsibilities amongst the various actors involved in managing AMI security. Ultimately, addressing these challenges may be crucial to maintain and ensure the security and resilience of AMI against evolving risks.

5.3.2.2 Cyber security conformity – Cognitive bias?

As described in Section 5.3.2.1 a significant number of the participants perceive the level of risk of cyber incidents in AMI as low. They in large don't see any immediate threats or vulnerabilities within AMI, and perceive it as secure as of today. As indicated in Section 4.2.4.4, security and awareness are joint efforts, where a significant level of trust is placed between amongst and within the actors to provide this effort.

Trust is highlighted in both [67] and [68] as a crucial factor in risk perception and in understanding how it is formed. This trust had in the research of [67] developed into a certain level of gullibility within power network companies in Norway in relation to their providers and ICT security challenges (Section 2.5.2). The notion that security is handled by others (when services and/or security are outsourced) was seen as a potential factor influencing the focus on information security and thus further influencing the perception of risk.

Within the SSI the participants have highlighted both dependence on others due to outsourcing of services and/or competence (Section 4.2.4.6), and the trust in others for cyber SA (Section 4.2.4.4), which indicate a distance to cyber risks (Section 5.2.1.5). Further, the perception of a joint effort and the level of trust within a small market such as the Norwegian, with a limited number of organizations and individuals with information security competence and knowledge (Section 4.2.4.6 and 4.2.4.8), can make them susceptible to cognitive bias as described in Section 2.4, by being influenced by a selected few actors in which they depend on and trust.

5.3.2.3 Observations on cyber security information sharing – Regulatory challenges?

As described in Section 2.2.1.2, the Power Contingency Regulation § 6.2 refers to legal requirements regulating the handling of sensitive energy sector information, essentially defining its type and the associated duty of confidentiality. This is a significant threat to the study's validity as described in Section 3.2.2.3, but also to the validity in the claims made in Section 5.3.2.1 and 5.3.2.2, as it is currently not authorized to access power sensitive information that may challenge or substantiate these claims.

However, § 6.2 may also produce challenges concerning the general research effort in the energy sector and the sharing of information with academia in this regard. In [122], ENISA points to how possible legal constraints hinder the sharing of cyber security information, based on the fear of non-compliance risks. This study focuses specifically on information sharing and interaction between Computer Security and Incident Response Teams (CSIRT) and Information Sharing and Analysis Centers (ISAC) between EU countries, but it also considers national level challenges in this regard. It is assumed that such challenges will also be transferrable to external and academic research efforts. Further, it elaborates on how complexity and fragmentation of the legal and policy framework in an EU context in addition entail challenges in information sharing. As

described in Section 4.2.4.8, the legal and regulatory frameworks in Norway are perceived differently by the participants. They are both seen as functional, with responsibilities reasonably placed, based on the current organization of the energy sector. At the same time, several of the participants also perceive it as fragmented and complex, challenging the ability to gain an overview for the participants in terms of requirements and which regulatory stakeholder to deal with. Such indications are to a certain extent substantiated by the findings in [122], which causes the study to imply this as a potential challenge, contributing to some of the indicated differences between the SLR and the SSI.

The fragmentation and complexity can also in a Norwegian context lead to fear of non-compliance in information sharing. However, this is not specifically indicated by the participants beyond dilemmas in information sharing (Section 4.2.4.8) considering trust between actors. Nonetheless, the study indicates that information and knowledge sharing are not necessarily optimal within the current implementation (Section 4.2.4.8) where some participants also highlight how some actors are not necessarily eligible to receive information that is classified based on the National Security Act. Thus, facing a similar challenge regarding fear of non-compliance risks and how to compliantly share information.

The challenge in sharing information that stems from legal requirements may to a certain degree limit the research efforts within the energy sector and AMI. The perceived lack of incidents, coupled with limited knowledge of research or testing conducted on the subject of information security in AMI can further lead to a cognitive bias, as described in Section 2.4 and 5.3.2.2. The participants may perceive that they are adequately addressing the information security risks, but without being challenged by research or by incidents. This notion is based on the study's investigation into the academic literature available on publicly available academic databases, and as such is limited in its scope (see Section 5.5 for limitations).

In order to remove this challenge, a potential solution could be to establish agreements with a broader research environment to challenge or confirm the actors' perception. For example, to test the perceived challenges, such as uncertainties in consequences and cascading effects, and how systemic risk can affect AMI. And notably, to explore the possibility to conduct tests in full-scale scenarios in a real-life setting. This implies providing methods for sharing information and authorizing research efforts on an extensive scale with academia and creating incentives for research within the subject, while still adhering to § 6.2.

5.3.2.4 Summary

The comparison conducted in Section 5.3.1 and further the evaluation of the divergence in this chapter have identified a difference in perception of level of risk and the absence of holistic risk assessments in the SLR. Further, it shows the difference in areas of focus for information security. While the SLR has a technological focus, with the main body of research conducted on the distributed elements, the participants in the SSI focus on the system level. However, both highlight the complexity and potential technological vulnerabilities and threats associated within all levels of AMI. In this regard, the participants perceive the system overall as a secure implementation capable of handling most of the identified challenges. But the SSI and the chosen methodology do not provide the study with concrete justification for the participants' claim of AMI security and how it handles the vulnerabilities, threats and consequences like those described in

the SLR. The ability to test such perceptions can be through research on the implementation, but the SLR was not able to identify significant efforts which were publicly available. This can be both due to the methodology chosen for the SLR, but also due to the sensitivity and regulatory requirements to protect information and knowledge, so as to not provide a cookbook for malicious actors.

The regulatory requirements are indicated by the study as a potential challenge regarding sharing knowledge and information. This may threaten the validity of this study but can also be potentially limiting to research efforts and thus can create a certain cognitive bias within the participants, where their perception is not adequately challenged. This cognitive bias can be further affected by the level of dependence on others and the trust in a limited set of actors in a small market such as the Norwegian implementation.

The divergent focus in a complex system such as AMI, an indicated cognitive bias and potentially finite research efforts due to limitations imposed by regulations and information sharing may imply the need for a comprehensive approach, addressing both technological and organizational factors.

The justification for addressing the divergences can be summed up in the following potential areas for improvement:

1) The need to level the knowledge and cyber SA of information security challenges.
    - The need for more holistic risk assessments of the AMI system.
    - The need to challenge a potential cognitive bias in risk perception and increase knowledge and competence.
    - The ability to challenge, verify and enhance technical and organizational solutions in a full-scale/real-life environment.
2) The need for a comprehensive approach to address the complexity in AMI and energy sector considering information security.
    - Regulation may limit research efforts.
    - Fragmentation of roles and authority.
    - Significant responsibility for information security placed on the individual actor creates uncertainties and the need for more competence and knowledge.

5.4 Alignment of focus – Addressing the divergence?

This chapter discusses recommendations on addressing the divergence identified in Section 5.3.1 based on the justifications and areas for improvement discussed in Section 5.3.2.

5.4.1 Levelling the knowledge and cyber SA

The study indicates a shortfall in knowledge and competence regarding information security, affecting cyber SA and potentially contributing to a cognitive bias. Without addressing these factors, the weak indications of a divergence in risk perception may evolve into a significant distance to cyber risks and development of incorrect cyber SA. To address the challenges identified in Section 5.3.2, it is recommended to address the level of knowledge and competence within AMI and its actors in regard to information security.

To enhance the level of competence and knowledge concerning information security in AMI, there are several factors that need to be considered, as summarized in Section

5.3.2.4. The need for more comprehensive risk assessments and the ability to challenge and verify the technical and organizational solutions in a full-scale/real-life environment can be conducted both by internal and external auditing and research. Conducting research and audits as external participants may provide an outsider perspective and reduce the organizational conflict of interests and influences in the research.

To enhance research efforts in international and national academia concerning the Norwegian implementation of AMI, establishing a research program which seeks to bring about a comprehensive approach to information security risks may be a potential solution. The main objective of the program would be to address the assumed need to strengthen research efforts and by this contribute to level the knowledge and competence by conducting research and sharing findings between the Norwegian AMI stakeholders and academia. By organizing such efforts under the regulatory authority or other adequate entities, the §6.2 may still be enforced, and information and findings can be distributed in accordance with the paragraph. The study's participants indicated that there are ongoing research efforts in Norwegian academia and by Norwegian organizations based on the sector's input and orders, however there were little evidence of this in the SLR. In [59] there are mentioned several research and development efforts for the energy sector, which could take into account and handle some of the efforts that the proposed program should instigate. Such efforts are further prioritized in [123] (the National Strategy for Digital Security Competence for Norway) where resources and focus are directed towards increasing research and educational efforts within digital security. However, as described in [124], the investments in digital security competence have not necessarily been as targeted as intended. This may indicate a need for a more sector wise approach to incentivise external and international research on the subject.

The establishment of this program will help challenge and verify the technical and organizational solutions, thus challenge or verify the perception of the state of security. It may further identify potential knowledge divergence that exist between Norwegian and international academia and describe identified vulnerabilities, threats and risks introduced with the evolving technology and interconnectedness in the AMI and the energy sector. However, this may depend on the ability to share, receive, and utilize classified or sensitive information with external actors, or on providing sanitized data and information for international research efforts. An improved ability to share information and data can embolden such a research program and enhance the program's precision and validity. This is to include sources such as NSM's threat assessments and perspectives from resources with AMI technical knowledge and insights and to research both technical and organizational challenges. Such efforts may further contribute to gaining a better overview of the system's challenges and strengths, looking at concrete vulnerabilities and threats, enabling more precise and comprehensive assessments of risk.

In addition to the described program, further encouraging knowledge and information sharing amongst industry stakeholders is another measure that can be taken to level the knowledge between the actors. This can be done through enhanced workshops, conferences, and training programs that bring together academia, regulators, and operators, hosted with the same intent as the described program above. By further promoting collaboration and knowledge sharing, these efforts can enhance the understanding of the Norwegian AMI and its unique challenges in terms of information security. This approach will ultimately contribute to multiply knowledge and competence amongst the actors, and potentially increase the scope of possibilities for academia to contribute. The participants in the study detailed several arenas and channels for information sharing, but recurring themes were that these were not excessively used, some required to actively subscribe to them, and that the actors were not necessarily

represented by the right people or competence (Section 4.2.4.8). This may entail the need to have fixed channels where all actors have default subscriptions, and a required participation on such arenas, potentially organized through the regulatory authorities. Another or supplemental approach may be the establishment of an incentive system, either in terms of economic incentives or proof of professional status, e.g., in the form of certifications of organizations or individuals. Examples of this are certifications provided by ISO (organizational, such as 27000-series), SANS Global Information Assurance Certification (GIAC) or industry specific certificates from vendors such as G3-PLC Alliance.

Furthermore, it is essential to recognize the potential impact of the scarcity of information security professionals as described in Sections 4.2.4.4 and 4.2.4.6. Strained access to competence and the presence of only a few SMEs with considerable influence can also create an unbalanced and biased view of the risks associated with AMI. This may result in an unchallenged perception of the security in AMI and the associated risk factors, and incorrect or insufficient cyber SA of the security posture and the threat environment. To counter this effect, an increased effort in the educational sector may be necessary to be able to handle the digitalization of society in general and the energy sector in specific. Efforts appear to be underway, as described earlier in [123]. However, the effect of this strategy has been questioned by the Office of the Auditor General of Norway as described earlier, where it appears that the measures in educational and research areas of digital security have not been fulfilled as intended [124]. The educational effort may mean that the different actors of AMI and the energy sector must enter into partnerships with educational institutions to a greater extent. With such partnerships established, they would also need to provide incentives and support for personnel pursuing a career in information security, and for research efforts within subjects aiming at challenging or developing security solutions. Areas of focus could be HW, communication, the integration of IT/OT, and how to best organize and manage information security work in AMI and the energy sector.

A persistent focus on all levels of the AMI ecosystem is needed, including through educational and research efforts. Increased education and research within information security in the energy sector will affect the knowledge and understanding of the distribution of risk in AMI. It is also important to persistently share information on the technical and organizational solutions and shortfalls for the Norwegian AMI implementation through various means, such as the proposed program.

5.4.2 A comprehensive approach and governance

The challenges related to the information security governance and regulation of the AMI systems based on the indications highlighted in this study have several aspects. Firstly, the complexity of the system makes it challenging to get a comprehensive overview in terms of information security challenges and potential vectors. This complexity can further be reinforced by how the distribution of roles and authority is perceived as fragmented, and how the responsibility for information security is placed within actors that do not necessarily have the prerequisites in terms of resources and competence for handling the information security work and solutions. Handling and mitigating the complexity in a comprehensive manner will potentially be more important in a future scenario. Here, the expected increased functionality and data within AMI and the continued integration of IT and OT can further increase the number of vectors and the expected utility of AMI for malicious actors.

By looking at how other sectors within the Norwegian society have organized their information security work and governance, there are several available models. These can be used for inspiration to address these challenges and provide a more comprehensive

approach. On an overall level, it is this study's opinion that combining the roles and responsibilities of information security within the energy sector would provide a less fragmented organization and distribution of roles and responsibilities. This could be done by establishing a central entity which can have the role of approval and supervision authority for implementations and their operation. This implies the development of frameworks and descriptions of architectural security solutions on a technical level. The suggested entity can then more appropriately verify and audit the solutions before they are put into operation. This would further contribute to reducing the uncertainty within the individual organization on how to implement, operate and maintain their AMI information security solutions.

In terms of the current work of the regulatory authority and information security, [59] describes a recommendation to organize and prepare the system to accommodate for future use and functionality, where increased complexity is expected. Further, it is recommended to strengthen the supervision and guidance by the regulatory authority (NVE), due to limited capacity to follow up on supervision in information security. However, as described in [10] there are still significant ICT challenges to address, and few supervisions are conducted focusing on digital security [124] despite the strategies described in [25]. Thus, an increased focus on increasing the supervision and guidance is needed, and this may to a certain extent be mitigated by using the proposed approval and supervision entity focusing on information security in the energy sector.

The proposed entity would be responsible for approving and supervising the technical solutions which are implemented concerning the information security posture. This includes documentation on technical implementation, operation and maintenance, and the organization of the security work. The Norwegian Armed Forces Security Department (FSA)[50] may serve as a model for this entity. FSA is responsible for approving and supervising regulated secure ICT systems handling classified or sensitive data and information, together with their associated value chains in the defense sector.

Establishing an approval entity within regulating authorities could handle several of the challenges mentioned initially. The fragmentation of responsibilities and roles related to information security can be mitigated by using a single authority. The strain and uncertainties on the individual actor due to varying competence and knowledge in ICT and information security can be reduced, as systems and the management organization would require preapproval before the system is put into operation. This may also reduce the risk of operationalizing systems with inadequate information security posture, as can be the case with today's implementations. To function as an approval authority, it would also require the entity to collect and analyze information concerning information security risks and vulnerabilities to produce recommendations and requirements in terms of security. This will aid them in developing a more comprehensive and detailed overview of information security challenges in the energy sector and AMI. This implies persistent and close collaboration with all actors in the energy sector to see holistically and broadly the complex field of information security in the energy sector, with both IT and OT and their integration as challenges. Secondly, it would also require close collaboration and access to information from internal and cross-sectorial agencies handling ICT security, such as KraftCERT and NSM NorCERT. An additional option is to incorporate a sector-specific CERT within the entity, provided as a mandatory service to all its subjects. This could entail a more unified approach to surveillance, detection, and response in terms of information security incidents. Further, it could contribute to elevating the security posture in the whole value chain concerning the operation and sustainability of AMI and

[50]Forsvarets Sikkerhetsavdeling - FSA (NO), [125]

energy sector and create a baseline for all entities. Additionally, such an approach could enhance the overall cyber SA, with all relevant actors reporting to one entity.

This study also believes that such an entity would provide several other benefits. Firstly, it is assumed that it would enable a more efficient regulation of pre-approved architecture and security solutions. As a system is already approved, the implementation is already known to the entity and the supervision could then revolve around confirming if it is operated as approved, and further updated as required. Secondly, as an entity with a more comprehensive and wider overview of the information security challenges in the energy sector, it could facilitate and provide better input to the planning and organization of the next generation of AMI and its requirements in terms of security. This will also enable the development of more holistic and detailed risk assessments, where competence and knowledge are gathered within the sector and in a unifying entity.

The implications of such a model are not investigated by this study and as such would need additional research to investigate its feasibility both organizationally, technically and financially.

5.5 Limitations

This section examines the research study's limitations and shortfalls, by reviewing the research undertaken and evaluating its validity and reliability in an overall manner.

5.5.1 Scope

This study conducted research to identify prominent risk factors to information security in AMI amongst stakeholders and in academic literature. The study further compared the factors to identify overlaps and divergence and, as an extension, made proposals on how to reduce the divergence. The study was conducted between December 2022 and May 2023, including SLR and SSI. The sample for SSIs consisted of individuals from all identified stakeholders in AMI, from different organizational levels, managing, operating, servicing or using AMI and AMI data. Stratified purposeful sampling was used to collect participants and is deemed to be appropriate as the study sought to recruit participants from all stakeholders and different levels within the stakeholders. However, the study was not able to recruit participants from all levels within all actors, and as such it did not have a sufficient sample size to be able to compare the different organizational levels within each actor. A total of 27 participants took part in the study, where all participants were based in Norway. The interviewed stakeholder DSO and AMI operators represented 1/3 of the metering points in Norway, while the stakeholder regulatory authority is responsible for auditing all KBO units.

5.5.2 SLR

The conducted structured literature review, and the method chosen may have excluded or missed relevant academic studies. These can be in the form of unpublished information and knowledge not intended for publication, but to be retained within organizations. As an example, the area of research in the study revolves around sensitive information with a certain damage potential if the level of technical detail is too high, thus prohibiting publication by organizational policy or by regulations (Section 5.1.6.1).

Some of the knowledge obtained in the SLR may be outdated due to the selected time frame for research papers in the academic databases. The study chose a 10-year timeframe based on the decision on implementation of AMI in 2011 and may include outdated knowledge and information. However, AMI in Norway predates 2012 and with a

significant lifespan of the technology, these older sources may still be relevant in certain implementations.

The method used in the SLR is described and conducted with the intention of providing objective results. However, the review process will to some extent be affected by the researchers' bias, knowledge, and experience in the area of research.

The generalization of the findings in the SLR may have weaknesses, as the intention was to present a comprehensive overview of the area of research with studies conducted on different implementations of AMI. This resulted in inclusion of studies from different countries such as the US [1], Saudi Arabia [113] and Norway [42].

5.5.3 SSI

The sample size was to some extent determined by the resources and time to complete the study and the availability of subjects. Due to a low sample size (N=27), the interview findings may have low generalizability, where the results may only be applied to a narrow population. However, considering sample composition, the subjects represent 1/3 of the end-users using two out the three most common SMs in use in Norway. Thus, their perception of and focus on information security challenges will represent those of a considerable part of the AMI actors in Norway. Additionally, considering that information security can be seen as a common phenomenon with the ubiquity of interconnected technology, the participants' perceptions may apply to a broader population in the energy sector.

Interviews in general will unavoidably lead to different forms of biases, such as researcher and response bias [74]. The interviews were digitally recorded and transcribed to ensure that the interview itself was in center and ensured the ability to review the interviews and capture the content with more accuracy, if necessary.

The structured part and the section concerning ranking of risk, consequence, and likelihood in terms of incidents yielded acceptable, good and excellent internal consistency respectively. Excellent consistency implies high reliability but could also be an indication of redundant questions. By conducting further analysis to identify such questions, e.g., by performing Principal Component Analysis (PCA) on the collected data, redundant questions can be identified and excluded.

The analysis technique used may have been another potential weakness of the SSI. The analysis and interpretation of the interviews was conducted using inductive meaning coding and compilation into categories. This aided in systemizing longer statements and grouping them into categories for comparison with the SLR. This entailed coding statements as they appeared during the analysis, compiling them, and further condensing the statements before categorizing them. The method of condensing the statements aids in capturing their essence and identifying consistencies and inconsistencies amongst the participants. However, this may also have led to the loss of subtle distinctions along the way. Similarly, by conducting most of the interviews and coding in Norwegian (26 out of 27), it may have led to further loss of distinction in the translation to English, which was necessary to be able to present the results in this study.

The level of detail in all descriptions of the elements of risk are for both the SLR and SSI generally overarching in nature and do not necessarily go into technical details concerning operationalization of threats and vulnerabilities. As mentioned in Section

5.1.6.1, the lack of detailed vulnerability, threat, attack, and impact descriptions in literature may be due to the sensitivity and the damage potential in such information. The energy sector (including AMI) in the Norwegian context is considered a critical infrastructure, and as such is subject to regulations concerning sharing and publication of information (i.e., by the Energy Act § 9-3 [46] and the Power Contingency Regulation § 6-2 [56] as described in Section 2.2.1.2). This prevents actors in the Norwegian energy sector and academia from providing detailed data and information on such categories through open sources and publicly accessible databases used in this SLR. Based on this, the study also refrained from probing into technical details regarding the risk elements in the SSI to avoid participants revealing sensitive and classified information. This has to a certain extent led to blurred and general descriptions of risk elements in SLR and SSI. There may also be incidents where the participants have withheld specific technical knowledge or other information without notifying the researchers.

6 Conclusion

This study aimed to identify the differences and mismatches in information security risk factors between academic literature and the perception of stakeholders in the Norwegian AMI. The evidence-based knowledge of differences is produced based on two primary methods: A SLR and SSI combining structured and semi-structured elements. The SLR and SSI yielded primarily qualitative data, where the structured part of the SSI yielded quantitative data intended to enrich or substantiate the qualitative data. The data collected by the different methods were analyzed Chapter 4 and further discussed in Chapter 5, enabling the study to conclude on the stated problem and RQs in the following sections.

6.1 The most prevalent risk factors in literature

The findings in the SLR indicated a wide range of vulnerabilities, threats and consequences at all the different levels of AMI, with a technological focus on the distributed level. The lack of likelihood and assessment of risk can be due to lack of system-specific evaluations and the focus on theoretical and simulated environments in the identified body of literature. Further, the descriptions of the factors are of a functional nature and lack specific details on how the factors can be put into operations or how they can be exploited to cause impacts to AMI. This may be due to the sensitivity of the information as described in Section 5.1.6.1. However, the nature of the factors still makes them valid, as the functional descriptions have the potential to affect any implementation. The functional descriptions of the factors are summarized in Section 5.1 and tabulated in the framework for comparison in Table 5.1, answering RQ1.

6.2 The perception of risks according to stakeholders

The findings in the SSI indicated a more condensed view of factors with a more system level focus. The participants provided assessment of risk when able to do so, where unwanted malicious cyber incidents affecting AMI as a whole were considered a low risk. When the HW, communication and system level were compared, the level of risk was considered highest at system level, followed by the communication level and lastly the HW level with the lowest perceived risk level. This is based on the level of severity of consequences, as incidents and breaches at system level will have the potential to affect larger volumes of aggregated data and the functionality for a considerable number of end-users. The implementation of AMI with the organization and the regulatory requirements are perceived to be secure by the majority of the participants with the current controls and mitigative measures. They highlight several vulnerabilities and threats at all levels but believe the system will be able to handle them, and as such describe the likelihood as low. The outliers in this regard are some of the end-users, who perceive the likelihood to be ranging from high to extreme at system level. This can be based on their lack of detailed system knowledge, their perception and experiences with general ICT-related threats and how they see the system level as a more or less IT-based with different interconnections.

The shared perception of factors is summarized in Table 5.3, where the participants share functional descriptions of the factors, answering RQ2. The lack of detailed and

profound descriptions as provided by the participants may be grounded in the restrictions given by national regulations concerning power sensitive information, as described in Section 5.3.2.3. The conduct of the interview and the self-imposed limitations on the researchers also contributed to limiting the level of detail to avoid non-compliance with national regulations. However, the provided functional descriptions enabled a high-level comparison of divergent factors in terms of risk factors and assessments.

6.3 Identifying the mismatches in risk factors

The findings in the research indicated how differences exist between the focus of literature and the perception of stakeholders of AMI in terms of information security risks (tabulated in Table 5.4 to Table 5.8. The complete comparison containing both overlaps and mismatches is tabulated in Appendix E), answering RQ3.

The comparison and evaluation conducted in Section 5.3.1 have identified differences in perception of risk factors and the absence of comprehensive risk assessments, showing varying areas of focus in information security. The SLR emphasizes and focuses on the technological aspects, particularly the distributed elements, while the participants in the SSI concentrate on the system level. Both recognize the complexity and potential vulnerabilities and threats across all levels of AMI. However, the SSI and the chosen methodology do not provide concrete justifications for the participants' claims of AMI security and its handling of vulnerabilities, threats, and consequences outlined in the SLR towards the distributed elements. Research efforts to test such perceptions were not significantly identified in the body of research identified in the SLR, potentially due to the chosen methodology and regulatory requirements on power sensitive information. However, the identified divergence in focus and perception concerning the distributed level versus the system level, coupled with a potential lack of recent research may warrant a need to challenge and verify the technical and organizational solutions in a real-life environment, thus potentially leveling and adding to the knowledge and cyber SA of information security challenges in the Norwegian implementation.

The study indicates that regulatory requirements may be a potential obstacle to the sharing of knowledge and information. This obstacle has the potential to impose constraints on research efforts. Consequently, it may contribute to a cognitive bias amongst participants, wherein their perspectives are inadequately challenged. Furthermore, this cognitive bias can be further reinforced by a high level of reliance on a limited set of actors within a small market, such as in the Norwegian AMI implementation, affecting the individual actor’s level of knowledge and competence. Given the complex nature of the AMI system, indications of a possible cognitive bias and potential limitations imposed by regulations on information sharing, a comprehensive approach is warranted. Such an approach should encompass both technological and organizational factors to effectively address the challenges at hand.

The indications of a need to level the knowledge and cyber SA implies a need to address the level of knowledge and competence within information security amongst the actors and challenge the system and the organization. Further, the complexity in AMI and the energy sector both in technical and organizational aspects, implies the need for a comprehensive approach to information security to alleviate the complexity and uncertainties.

6.4 Proposed solutions to minimize the divergence

The current and future investments in information security in AMI and the energy sector should be grounded on a clear perception and awareness of risks. This study has indicated a divergence between the research efforts in academic literature and the focus and perception of risks amongst the stakeholders of AMI. Further, it has indicated how a complex system and its organization challenges the ability to obtain a comprehensive view of the risk factors in the system, and thus makes it challenging to get a clear perception and awareness of information security risks.

To aid in developing a more clear and updated knowledge and insight of risks in AMI, this study proposes two overarching approaches based on the findings.

1) **Incentivizing more research - Enhancing and adding to the level of knowledge and cyber SA.**
   In order to enhance research efforts in both international and national academia pertaining to the Norwegian implementation of AMI, the establishment of a research program that adopts a comprehensive approach to address information security risks could be a potential solution. The primary objective of this program would be to address the indicated need for strengthening research efforts and contribute to the enhancement of knowledge and competence. By conducting research and facilitating the exchange of findings between the stakeholders involved in the Norwegian AMI implementation and the academic community, knowledge and insights are added, affecting perception and SA of information security challenges.
2) **Centralized and enhanced information security governance – Reducing complexity.**
   Establishing an approval entity similar to what has been done in the Defense sector can potentially reduce the complexity in organizing and enforcing the work around information security in the energy sector and AMI. By additionally incorporating CERT-functionality within, it could aid in building a more comprehensive cyber SA, with a mandatory membership for all actors. Placed within the regulatory authorities, the fragmentation is reduced in terms of roles and responsibilities, empowering one entity with the overall responsibility for supervision and pre-approval of technical and organizational solutions. This could provide a more persistent focus and overview of the overall information security posture and status in AMI and the energy sector.

6.5 Future work and research

This study produced indications on how information security risks are perceived amongst stakeholders in AMI, on the focus areas of literature on information security risks in AMI, and in which areas these differ from each other. Further, solutions to reduce the differences were proposed. Based on the information collected from literature and the participants, several aspects could be the subject for further research.

Primarily, the scope of the study's SSI has been limited to a small number of participants from different organizational levels within each stakeholder in AMI. To survey the perception of risk of a broader or narrower audience could provide interesting and new findings. A broader audience implies a larger sample size in terms of number of actors and number of participants from different organizational levels. A narrower audience could imply surveying participants in the academic sector researching information security within IT/OT.

There are several variables that could affect the perception of information security risks amongst the stakeholders. The participants highlight how incidents, technological development, knowledge exchanges and changes in the international security situation affect their cyber SA and perception of risks in information security. Research could give more insights into what factors influence perception the most, and thus provide a foundation for improving risk communication.

Further on perception of risk and influencing factors, it could be interesting to conduct a study measuring cyber security knowledge and information security risk perception. This could be done by revising the study's structured interview guide to incorporate questions measuring cyber security knowledge more precisely for comparison towards risk perception. This could provide interesting findings and measure competence towards perception of risk.

In terms of risk assessments, both literature and the participants highlighted how risk assessments is a requirement for new services and functionality. Risk informed decisions are critical to avoid and mitigate unwanted incidents and potentially cascading effects due to the identified interconnections within AMI and the energy sector. However, there will always be residual risk which must be accepted, transferred, or mitigated. Research could give more insight into how a malicious actor with resources and capabilities (i.e., nation state actor) can exploit the residual risk to potentially cause severe consequences not accounted for in the initial risk assessments.

In relation to confidentiality and privacy challenges, the current and future handling and aggregation of data should be given more attention from a research point of view. New data elements generated from the current AMI system can be analyzed and aggregated to reveal PII data. With an increase in both the frequency of data measurements and the types of data being measured and reported, there is a potential increase in the amount of PII that can be extracted from such data. Research could provide a better basis for decisions concerning measures to protect such data, potentially improving already implemented measures such as encryption and authentication or provide additional measures.

Based on the discussion in the study, the information security posture of AMI as a system seems to be complex and challenging to get a comprehensive overview of. The interconnections and variations in technology together with uncertainties of consequences and cascading effects could warrant more research into how these aspects could be exploited. By researching and challenging a complete implementation of the system in a real-life setting, a realistic overview of the posture and the potential for cascading effects from/to AMI and other dependent or interconnected systems could be obtained.

Further on technological areas for research, the next generation of AMI systems and their requirements are becoming more and more relevant as the current implementation is moving towards end-of-life. The implementation of new HW and functionality and the assumed potential to generate more data elements could produce new ways to use such data and provide new services to end-users. At the same time, it may introduce new vectors and vulnerabilities as the system is introduced and matured. Research into how updateability in the distributed HW could be optimized to account for rapid and continuous updates to keep up with the pace in technological developments could provide an enhancement in technological lifespan for the next generation.

Considering the proposed recommendation of a centralized approval authority for information systems in the energy sector and AMI, further research could investigate the viability and feasibility of such a solution. This could be conducted with different areas of focus, both organizational, technical and regulatory/legal: First and foremost, the proposed organizational model needs to be researched considering its applicability to the energy sector. Research concerning how to organize and unify the regulation of information security in such an entity could be conducted, considering the model from the Defense sector. Further, research concerning how the technical evaluation of implementations should be conducted during the pre-approval process would be beneficial to development of structures and routines in relation to organizing such work.

Bibliography

[1] A. Hansen, J. Staggs, and S. Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection,* vol. 18, pp. 3-19, 2017. DOI: 10.1016/j.ijcip.2017.03.004.

[2] H. Sæle, K. Ingebrigtsen, and M. Istad, "Fremtidens avanserte måle og styringssystem (AMS): Forventet utvikling 2-5 år frem i tid," SINTEF Energi AS, Oslo, 978-82-410-1921-0, 2019. [Online]. Available: https://publikasjoner.nve.no/rapport/2019/rapport2019_34.pdf. DOI: N/A.

[3] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A Methodology for Security Classification applied to Smart Grid Infrastructures," *International journal of critical infrastructure protection,* vol. 28, 2020, Art no. 100342. DOI: 10.1016/j.ijcip.2020.100342.

[4] Nasjonal sikkerhetsmyndighet (NSM). (2021). *Risiko 2021*. [Online]. Available: https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler, (Accessed on 2021-09-20).

[5] Nasjonal sikkerhetsmyndighet (NSM). (2020). *Risiko 2020*. [Online]. Available: https://nsm.no/aktuelt/risiko-2020, (Accessed on 2021-09-20).

[6] Politiets sikkerhetstjeneste (PST). (2021). *Nasjonal trusselvurdering 2021*. [Online]. Available: https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf, (Accessed on 2022-09-11).

[7] Politiets sikkerhetstjeneste (PST). (2020). *Nasjonal trusselvurdering 2020*. [Online]. Available: https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020, (Accessed on 2022-09-10).

[8] Lockheed Martin, "Cyber Kill Chain®." Lockheedmartin.com, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, (Accessed on 2022-10-10), 2022.

[9] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vienna, Austria, 2020, vol. 1, IEEE, pp. 1537-1543. DOI: 10.1109/ETFA46521.2020.9212128.

[10] Riksrevisjonen. (2021). *Undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*. [Online]. Available: https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen/, (Accessed on 2022-09-05).

[11] M. Simonov, F. Bertone, K. Goga, and O. Terzo, "Cyber Kill Chain Defender for Smart Meters," in *Advances in Intelligent Systems and Computing*, *vol. 772*, *Complex, Intelligent, and Software Intensive Systems (CISIS 2018)*, L. Barolli, N. Javaid, M. Ikeda, and M. Takizawa, Eds.: Springer, Cham, 2019, pp. 386-397. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-93659-8_34, (Accessed on 2023-02-01).

[12] J. Kim and Y. Kim, "Benefits of cloud computing adoption for smart grid security from security perspective," *The Journal of Supercomputing,* OriginalPaper vol. 72, no. 9, pp. 3522-3534, 2015. DOI: 10.1007/s11227-015-1547-0.

[13] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, 2020, Art no. 107094. DOI: 10.1016/j.comnet.2019.107094.

[14] K. P. Frogner, E. Lien, and K. M. G. Bergh, "Smart energy metering and its infrastructure – A survey on vulnerabilities and information security challenges,"

Department of Information Security and Communication Technology, Term paper, 2021.
[15] J. Mendel, "Smart Grid Cyber Security Challenges: Overview and Classification," (in English), *E-Mentor,* vol. 2017, no. 1(68), pp. 55-66, 2017. DOI: 10.15219/em68.1282.
[16] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," (in English), *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018. DOI: 10.1016/j.ijepes.2017.12.020.
[17] M. Asplund and S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services," (in English), *IEEE Access,* vol. 4, pp. 2130-2138, 2016. DOI: 10.1109/ACCESS.2016.2560919.
[18] Nasjonal sikkerhetsmyndighet (NSM). (2022). *Risiko 2022*. [Online]. Available: https://nsm.no/getfile.php/1312007-1664785983/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf, (Accessed on 2023-04-02).
[19] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical smart grid infrastructures," in *ISGT 2014*, Washington, DC, USA, 2014, IEEE, pp. 1-5. DOI: 10.1109/ISGT.2014.6816504.
[20] M. E. Whitman and H. J. Mattord, *Management of information security*, 5th ed. Cengage Learning, 2017.
[21] B. von Solms and R. von Solms, "Cybersecurity and information security – what goes where?," *Information and Computer Security,* vol. 26, no. 1, pp. 2-9, 2018. DOI: 10.1108/ICS-04-2017-0025.
[22] H. Taherdoost, "Cybersecurity vs. Information Security," *Procedia Computer Science,* vol. 215, pp. 483-487, 2022. DOI: 10.1016/j.procs.2022.12.050.
[23] *Information technology - Security techniques - Information security management systems - Overview and vocabulary*, ISO/IEC 27000:2018(E), International Organization for Standardization (ISO), Geneva, Switzerland, 2018.
[24] *Information technology — Security techniques — Guidelines for cybersecurity*, ISO/IEC 27032:2012(E), International Organization for Standardization (ISO), Geneva, Switzerland, 2012.
[25] Justis- og beredskapsdepartementet og Forsvarsdepartementet. (2019). *Nasjonal strategi for digital sikkerhet*. [Online]. Available: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf, (Accessed on 2023-03-10).
[26] *FIPS Pub 200 Minimum Security Requirements for Federal Information and Information Systems*, FIPS Pub 200, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, U.S., 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.
[27] Joint Task Force Transformation Initiative (JTFTI), "Guide for Conducting Risk Assessments," NIST, Gaithersburg, Maryland, U.S., Special Publication 800‐30 Rev 1, 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. DOI: 10.6028/NIST.SP.800-30r1.
[28] Cyber Physical Systems Public Working Group, "Framework for Cyber-Physical Systems Release 1.0," National Institute of Standards and Technology, Gaithersburg, Maryland, U.S., 2016. [Online]. Available: https://pages.nist.gov/cpspwg/library/. DOI: N/A.
[29] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security -- A Survey," 2017. DOI: 10.1109/JIOT.2017.2703172.
[30] *Risk management — Vocabulary*, ISO Guide 73:2009, International Organization for Standardization (ISO), Geneva, Switzerland, 2009.
[31] *Systems and software engineering — System life cycle processes*, ISO/IEC/IEEE 15288:2015(E), International Organization for Standardization (ISO), Geneva, Switzerland, 2015.
[32] S. O. Hansson, "Risk: objective or subjective, facts or values," *Journal of Risk Research,* vol. 13, no. 2, pp. 231-238, 2010. DOI: 10.1080/13669870903126226.

[33] S. Oltedal, B.-E. Moen, H. Klempe, and T. Rundmo, *Explaining risk perception : An evaluation of cultural theory*. Trondheim: Rotunde, 2004.

[34] A. Shahzad *et al.*, "A secure, intelligent, and smart-sensing approach for industrial system automation and transmission over unsecured wireless networks," *Sensors (Basel),* vol. 16, no. 3, pp. 322-322, 2016. DOI: 10.3390/s16030322.

[35] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. Mcquaid, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," Washington D.C., 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf. DOI: 10.6028/NIST.SP.800-160v2r1.

[36] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," in *The Proceedings of 15th Australian Information Security Management Conference*, Edith Cowan University, Perth, Western Australia, C. Valli, Ed., 2017, ECU, pp. 149-155. DOI: 10.4225/75/5a84f7b595b4e.

[37] J. Klaess, "IT/OT Convergence – Tips For Gaining Visibility In Your Connected Factory." Tulip.co, https://tulip.co/blog/it-ot-convergence-tips-for-gaining-visibility-in-your-connected-factory/, (Accessed on 2022-12-03), 2021.

[38] R. Bago and M. Campos, "Smart meters for improved energy demand management: The Nordic experience," *Eco-Friendly Innovation in Electricity Transmission and Distribution Networks*, J.-L. Bessède, Ed., Oxford: Woodhead Publishing, 2015, pp. 339-361. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9781782420101000161, (Accessed on 2022-12-05).

[39] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable & sustainable energy reviews,* vol. 57, pp. 302-318, 2016. DOI: 10.1016/j.rser.2015.12.114.

[40] A. Venjum, "Smarte målere (AMS): Status og planer for installasjon per 1. halvår 2016," NVE, Oslo, 978-82-410-1532-8, 2016. [Online]. Available: https://publikasjoner.nve.no/rapport/2016/rapport2016_79.pdf. DOI: N/A.

[41] C. Frøystad, M. G. Jaatun, K. Bernsmed, and M. Moe, "Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA," NVE, Oslo, 978-82-410-1789-6, 2018. Accessed: 2022-10-12. [Online]. Available: https://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf. DOI: N/A.

[42] M. B. Line, G. I. Johansen, and H. Sæle, "Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS," SINTEF, Trondheim, 8214052807, 2012. [Online]. Available: https://sintef.brage.unit.no/sintef-xmlui/handle/11250/2380394. DOI: N/A.

[43] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Generation Computer Systems,* vol. 136, pp. 358-377, 2022. DOI: 10.1016/j.future.2022.06.013.

[44] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering Infrastructure," *International Journal of Electrical Power & Energy Systems,* vol. 63, pp. 473-484, 2014. DOI: 10.1016/j.ijepes.2014.06.025.

[45] C. Greer *et al.*, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," NIST, Gaithersburg, Maryland, Special Publication (SP) 1108r3, 2014. Accessed: 2022-10-30. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916755. DOI: 10.6028/NIST.SP.1108r3.

[46] Energiloven – enl. (1990). Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) (LOV-1990-06-29-50). Lovdata. [Online]. https://lovdata.no/lov/1990-06-29-50.

[47] Olje- og Energidepartementet, "Kraftmarkedet - Energifakta Norge." Energifakatnorge.no, https://energifaktanorge.no/norsk-energiforsyning/kraftmarkedet/, (Accessed on 2023-02-01), 2023.

[48] Elhub, "Hva gjør vi? - Elhub." Elhub.no, https://elhub.no/om-elhub/hva-gjor-vi/, (Accessed on 2023-01-28), 2023.
[49] Statnett, "Elhub." Statnett.no, https://www.statnett.no/for-aktorer-i-kraftbransjen/systemansvaret/kraftmarkedet/avregningsansvaret/elhub/, (Accessed on 2023-01-25), 2023.
[50] Norges vassdrags- og energidirektorat (NVE), "Regelverk og skjema - NVE." Nve.no, https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/regelverk-og-skjema/, (Accessed on 2023-01-24), 2023.
[51] Norges vassdrags- og energidirektorat (NVE), "Kraftforsyningens beredskapsorganisasjon (KBO) - NVE." Nve.no, https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/organisering-av-kraftforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/, (Accessed on 2023-02-01), 2023.
[52] Forskrift om kraftomsetning og nettjenester. (1999). Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv (FOR-1999-03-11-301). Lovdata. [Online]. https://lovdata.no/forskrift/1999-03-11-301.
[53] H. Sæle, M. Istad, and M. G. Jaatun, "Omarbeidelse av veileder til sikkerhet for «Avanserte måle- og styringssystemer» (AMS) i avregningsforskriften," SINTEF, Oslo, 978-82-410-2219-7, 2022. [Online]. Available: https://publikasjoner.nve.no/rme_eksternrapport/2022/rme_eksternrapport2022_06.pdf. DOI: N/A.
[54] Personopplysningsloven. (2018). Lov om behandling av personopplysninger (personopplysningsloven) (LOV-2018-06-15-38). Lovdata. [Online]. https://lovdata.no/lov/2018-06-15-38.
[55] Forskrift om krav til elektrisitetsmålere. (2007). Forskrift om krav til elektrisitetsmålere (FOR-2007-12-28-1753). Lovdata. [Online]. https://lovdata.no/forskrift/2007-12-28-1753.
[56] Kraftberedskapsforskriften. (2012). Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften) (FOR-2012-12-07-1157). Lovdata. [Online]. https://lovdata.no/forskrift/2012-12-07-1157.
[57] Datatilsynet, "Automatisk strømmåling." Datatilsynet.no, https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/strommaling/, (Accessed on 2022-10-12), 2018.
[58] Datatilsynet, "Datatilsynets oppgaver." Datatilsynet.no, https://www.datatilsynet.no/om-datatilsynet/oppgaver/, (Accessed on 2023-01-23), 2023.
[59] NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. [Online]. Available: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf, (Accessed on 2022-12-11).
[60] M. D. Hossain, H. Ochiai, T. Arisawa, and Y. Kadobayashi, "Smart Meter Modbus RS-485 Spoofing Attack Detection by LSTM Deep Learning Approach," in *2022 9th Swiss Conference on Data Science (SDS)*, Lucerne, Switzerland, 2022, IEEE, pp. 47-52. DOI: 10.1109/SDS54800.2022.00015.
[61] J. L. Rrushi, H. Farhangi, R. Nikolic, C. Howey, K. Carmichael, and A. Palizban, "By-design vulnerabilities in the ANSI C12.22 protocol specification," in *Proceedings of the 30th Annual ACM Symposium on Applied Computing (SAC '15)*, Salamanca, Spain, 2015, ACM, pp. 2231–2236. DOI: 10.1145/2695664.2695835.
[62] P. Salmon, M. , N. Stanton, A. , and D. Jenkins, P., *Distributed Situation Awareness : Theory, Measurement and Application to Teamwork*, Farnham, England: CRC Press, 2009. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=298556&site=ehost-live&scope=site, (Accessed on 2022-11-28).
[63] M. R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors,* vol. 37, no. 1, pp. 32-64, 1995. DOI: 10.1518/001872095779049543.

[64] M. R. Endsley, "Situation awareness global assessment technique (SAGAT)," in *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, Dayton, OH, USA, 1988, IEEE, pp. 789-795 vol.3. DOI: 10.1109/NAECON.1988.195097.

[65] D. G. Jones and M. R. Endsley, "Sources of situation awareness errors in aviation," *Aviation, space, and environmental medicine,* vol. 67, pp. 507-512, 1996.

[66] M. Husák, T. Jirsík, and S. Yang, "SoK: contemporary issues and challenges to enable cyber situational awareness for network security," *ACM International Conference Proceeding Series,* pp. 1-10, 2020. DOI: 10.1145/3407023.3407062.

[67] R. Ø. Skotnes, "Risk perception regarding the safety and security of ICT systems in electric power supply network companies," *Safety Science Monitor,* vol. 19, no. 1, 2015.

[68] M. H. Larsen, M. S. Lund, and F. B. Bjørneseth, "A model of factors influencing deck officers' cyber risk perception in offshore operations," *Maritime Transport Research,* vol. 3, p. 100065, 2022. DOI: 10.1016/j.martra.2022.100065.

[69] M. H. Larsen and M. S. Lund, "Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review," *IEEE Access,* vol. 9, pp. 144895-144905, 2021. DOI: 10.1109/ACCESS.2021.3122433.

[70] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sciences,* vol. 9, no. 2, pp. 127-152, 1978. DOI: 10.1007/BF00143739.

[71] A. Tversky and D. Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science,* vol. 185, no. 4157, pp. 1124-1131, 1974. DOI: jstor.org/stable/1738360.

[72] S. Roeser, R. Hillerbrand, P. Sandin, and M. Peterson, "Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk," 2012. DOI: 10.1007/978-94-007-1433-5.

[73] N. D. Weinstein and W. M. Klein, "Unrealistic optimism: Present and future," *Journal of social and clinical psychology,* vol. 15, no. 1, pp. 1-8, 1996. DOI: 10.1521/jscp.1996.15.1.1.

[74] P. D. Leedy, *Practical research: Planning and design*, 11th ed. Boston: Pearson, 2015.

[75] C. M. Barnum, *Usability testing essentials: Ready, set...test!*, Amsterdam: Morgan Kaufmann Publishers, 2010. [Online]. Available: https://web.s.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzM0NDk4OF9fQU41?sid=74f0d4b4-c6b3-4413-b581-d2c3cd6ab9c4@redis&vid=0&format=EB&rid=1, (Accessed on 2022-12-10).

[76] A. Zibak, C. Sauerwein, and A. C. Simpson, "Threat Intelligence Quality Dimensions for Research and Practice," *Digital Threats,* vol. 3, no. 4, p. Article 44, 2022. DOI: 10.1145/3484202.

[77] J. Jesson, L. Matheson, and F. M. Lacey, *Doing your literature review: Traditional and systematic techniques*. London: Sage, 2011, p. 179.

[78] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," (in English), *The Journal of Systems and Software,* vol. 80, no. 4, p. 571, 2007. DOI: 10.1016/j.jss.2006.07.009.

[79] S. Brinkmann and S. Kvale, *Doing Interviews*, Second ed. 55 City Road, London: SAGE Publications Ltd, 2018. [Online]. Available: https://methods.sagepub.com/book/doing-interviews-2e, (Accessed on 2023-01-29).

[80] W. C. Adams, "Conducting Semi-Structured Interviews," *Handbook of Practical Program Evaluation*, K. E. Newcomer, H. P. Hatry, and J. S. Wholey, Eds., Online: Wiley Online Books, 2015, pp. 492-505. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119171386.ch19, (Accessed on 2023-02-10).

[81] H. Kallio, A.-M. Pietilä, M. Johnson, and M. Kangasniemi, "Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide," *Journal of Advanced Nursing,* vol. 72, no. 12, pp. 2954-2965, 2016. DOI: 10.1111/jan.13031.

[82] D. S. Cruzes and T. Dyba, "Recommended Steps for Thematic Synthesis in Software Engineering," in *2011 International Symposium on Empirical Software Engineering and Measurement*, Banff, AB, Canada, 2011, IEEE, pp. 275-284. DOI: 10.1109/ESEM.2011.36.

[83] L. S. Nowell, J. M. Norris, D. E. White, and N. J. Moules, "Thematic Analysis: Striving to Meet the Trustworthiness Criteria," *International Journal of Qualitative Methods,* vol. 16, no. 1, 2017. DOI: 10.1177/1609406917733847.

[84] D. George and P. Mallery, *IBM SPSS Statistics 26 Step by Step: A simple guide and reference*, 16th ed. New York: Taylor & Francis, 2019.

[85] J. P. A. Yaacoub, J. H. Fernandez, H. N. Noura, and A. Chehab, "Security of Power Line Communication systems: Issues, limitations and existing solutions," *Computer Science Review,* vol. 39, p. 100331, 2021. DOI: 10.1016/j.cosrev.2020.100331.

[86] M. A. Husnoo, A. Anwar, N. Hosseinzadeh, S. N. Islam, A. N. Mahmood, and R. Doss, "False data injection threats in active distribution systems: A comprehensive survey," *Future Generation Computer Systems,* vol. 140, pp. 344-364, 2023. DOI: 10.1016/j.future.2022.10.021.

[87] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts," *Renewable and Sustainable Energy Reviews,* vol. 163, p. 112423, 2022. DOI: 10.1016/j.rser.2022.112423.

[88] S. Asri and B. Pranggono, "Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure," *Wireless Personal Communications,* vol. 83, no. 3, pp. 2211-2223, 2015. DOI: 10.1007/s11277-015-2510-3.

[89] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.,* vol. 51, no. 1, pp. 42-49, 2013. DOI: 10.1109/MCOM.2013.6400437.

[90] I. A. Tøndel, M. G. Jaatun, and M. B. Line, "Threat Modeling of AMI," in *Lecture Notes in Computer Science*, *vol. 7722*, *Critical Information Infrastructures Security*, B. M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, Eds., Berlin, Heidelberg: Springer Berlin, Heidelberg, 2013, pp. 264-275. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-41485-5_23, (Accessed on 2023-01-25).

[91] *Information technology — Security techniques — Network security — Part 1: Overview and concepts*, ISO/IEC 27033-1:2015(en), International Organization for Standardization (ISO), Geneva, Switzerland, 2015.

[92] *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*, ISO/IEC 27039:2015(en), International Organization for Standardization (ISO), Geneva, Switzerland, 2015.

[93] *Information technology — Vocabulary*, ISO/IEC 2382:2015(en), International Organization for Standardization (ISO), Geneva, Switzerland, 2015.

[94] M. Ahmed and A.-S. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling,* vol. 8, no. 1, p. 4, 2020. DOI: 10.1186/s40294-020-00070-w.

[95] *Information technology — Security techniques — Entity authentication assurance framework*, ISO/IEC 29115:2013(en), International Organization for Standardization (ISO), Geneva, Switzerland, 2013.

[96] *Information technology — Security techniques — Entity authentication — Part 1: General*, ISO/IEC 9798-1:2010(en), International Organization for Standardization (ISO), Geneva, Switzerland, 2010.

[97] L. Lesavre, P. Varin, and D. Yaga, "NISTIR 8301 Blockchain Networks: Token Design and Management Overview," in "NISTIR," National Institute of Standards

and Technology, Gaithersburg, Maryland, U.S., 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8301.pdf. DOI: 10.6028/NIST.IR.8301.

[98] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital Identity Guidelines," NIST, Gaithersburg, Maryland, U.S., Special Publication 800-63-3, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. DOI: 10.6028/NIST.SP.800-63-3.

[99] D. Ackley and H. Yang, "Exploration of Smart Grid Device Cybersecurity Vulnerability Using Shodan," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, Montreal, QC, Canada, 2020, IEEE, pp. 1-5. DOI: 10.1109/PESGM41954.2020.9281544.

[100] C. Foreman, J. and D. Gurugubelli, "Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure," *The Electricity Journal,* vol. 28, no. 1, pp. 94-103, 2015. DOI: 10.1016/j.tej.2014.12.007.

[101] L. Wei, L. P. Rondon, A. Moghadasi, and A. I. Sarwat, "Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Denver, CO, USA, 2018, IEEE, pp. 1-9. DOI: 10.1109/TDC.2018.8440552.

[102] M. D. H. Abdullah, Z. M. Hanapi, Z. A. Zukarnain, and A. M. Mohamad, "Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks," *KSII Trans. Internet Inf. Syst.,* vol. 9, no. 4, pp. 1493-1515, 2015. DOI: 10.3837/tiis.2015.04.013.

[103] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure," *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2435-2443, 2015. DOI: 10.1109/TSG.2015.2418280.

[104] K. Al-Sammak, S. A.-. Gburi, and I. Marghescu, "Communications Systems in Smart Metering: A Concise Systematic Literature review," in *2022 14th International Conference on Communications (COMM)*, Bucharest, Romania, 2022, IEEE, pp. 1-9. DOI: 10.1109/COMM54429.2022.9817154.

[105] G. Bendiab, K.-P. Grammatikakis, I. Koufos, N. Kolokotronis, and S. Shiaeles, "Advanced metering infrastructures: security risks and mitigation," in *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20)*, Virtual Event, Ireland, 2020, ACM, pp. 1-8, Article 113. DOI: 10.1145/3407023.3409312.

[106] E. Sohl *et al.*, "A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC '15)*, Denver, Colorado, USA, 2015, ACM, in CPS-SPC '15, pp. 113-122. DOI: 10.1145/2808705.2808716.

[107] K. Sharma and L. Mohan Saini, "Performance analysis of smart metering for smart grid: An overview," *Renewable and Sustainable Energy Reviews,* vol. 49, pp. 720-735, 2015. DOI: 10.1016/j.rser.2015.04.170.

[108] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Computer Communications,* vol. 36, no. 17, pp. 1665-1697, 2013. DOI: 10.1016/j.comcom.2013.09.004.

[109] Y. Kim, S. Hakak, and A. Ghorbani, "Smart grid security: Attacks and defence techniques," *IET Smart Grid,* vol. 6, no. 2, pp. 103-123, 2022. DOI: 10.1049/stg2.12090.

[110] M. Wei and W. Wang, "Data-centric threats and their impacts to real-time communications in smart grid," *Computer Networks,* vol. 104, pp. 174-188, 2016. DOI: 10.1016/j.comnet.2016.05.003.

[111] M. Benmalek, Y. Challal, and A. Derhab, "Authentication for Smart Grid AMI Systems: Threat Models, Solutions, and Challenges," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for*

Collaborative Enterprises (WETICE), Napoli, Italy, 2019, IEEE, pp. 208-213. DOI: 10.1109/WETICE.2019.00052.

[112] M. H. Haider, S. B. Saleem, J. Rafaqat, and N. Sabahat, "Threat Modeling of Wireless Attacks on Advanced Metering Infrastructure," in *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Karachi, Pakistan, 2019, IEEE, pp. 1-6. DOI: 10.1109/MACS48846.2019.9024779.

[113] A. Akkad, G. Wills, and A. Rezazadeh, "An information security model for an IoT-enabled Smart Grid in the Saudi energy sector," *Computers and Electrical Engineering,* vol. 105, p. 108491, 2023. DOI: 10.1016/j.compeleceng.2022.108491.

[114] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering,* vol. 67, pp. 469-482, 2018. DOI: 10.1016/j.compeleceng.2018.01.015.

[115] P. H. Mirzaee, M. Shojafar, H. Cruickshank, and R. Tafazolli, "Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)," *IEEE Access,* vol. 10, pp. 52922-52954, 2022. DOI: 10.1109/ACCESS.2022.3174259.

[116] R. Borgaonkar and M. G. Jaatun, "5G as an Enabler for Secure IoT in the Smart Grid : Invited Paper," in *2019 First International Conference on Societal Automation (SA)*, Krakow, Poland, 2019, IEEE, pp. 1-7. DOI: 10.1109/SA47457.2019.8938064.

[117] V. Tudor, M. Almgren, and M. Papatriantafilou, "Analysis of the Impact of Data Granularity on Privacy for the Smart Grid," in *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society (WPES '13)*, Berlin, Germany, 2013, ACM, pp. 61-70. DOI: 10.1145/2517840.2517844.

[118] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys & Tutorials,* vol. 16, no. 4, pp. 1933-1954, 2014. DOI: 10.1109/COMST.2014.2320093.

[119] M. Siegrist and J. Árvai, "Risk Perception: Reflections on 40 Years of Research," *Risk Analysis,* vol. 40, no. S1, pp. 2191-2206, 2020. DOI: 10.1111/risa.13599.

[120] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, "Unrealistic optimism on information security management," *Computers & Security,* vol. 31, no. 2, pp. 221-232, 2012. DOI: 10.1016/j.cose.2011.12.001.

[121] J. W. Welburn and A. M. Strong, "Systemic Cyber Risk and Aggregate Impacts," *Risk Analysis,* vol. 42, no. 8, pp. 1606-1622, 2022. DOI: 10.1111/risa.13715.

[122] ENISA. (2017). *Report on Cyber Security Information Sharing in the Energy Sector*. [Online]. Available: https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector, (Accessed on 2023-03-01).

[123] Justis- og beredskapsdepartementet og Kunnskapsdepartementet. (2019). *Nasjonal strategi for digital sikkerhetskompetanse*. [Online]. Available: https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf, (Accessed on 2023-03-10).

[124] Riksrevisjonen. (2023). *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor*. [Online]. Available: https://www.riksrevisjonen.no/rapporter-mappe/no-2022-2023/undersokelse-av-myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor/, (Accessed on 2023-04-06).

[125] J. Børresen. *Forsvarets sikkerhetsavdeling* in Store Norske Leksikon, [Online] Available: https://snl.no/Forsvarets_sikkerhetsavdeling.

Appendix

Appendix A1 - Interview Guide English

Themes	Comments and questions	Probes
Introduction	*Thank you for participating *MSc thesis general info *Interview objective and structure based on invitation *Start audio recording (with consent) *Consent agreement *Scope of the study with reference model	AMS reference model visualized
Background information	**0.1** What is your formal role in the organization and at what level do you work on? (Strategic, tactical, or operational level) **0.2** How would you assess your knowledge of AMI and information security? (On a scale from 0 (no knowledge) to 10 (expert))	
Part 1: Structured interview issued as questionnaire		
Experience with AMI (Q1-3)	**1** Below are five assumed added values from AMI. How would you rate the described added values, from highest (1) to lowest (5)? - New services (e.g., smart charging of electric vehicles - Improvement of existing services (e.g., precise and timely consumption measurements) - Reduced costs of operation and maintenance of the distribution network - Increased security of energy supply to the society - Better utilization of existing resources (e.g easier integration of distributed energy resources such as solar and wind) **2** Below are five claims that can positively impact the security of the AMI system. How would you rank the claims described, from greatest (1) to lowest (5) impact? *"Information security in AMI will improve and AMI will be integrated more securely into a smart grid if..."* - Standardized technical solutions are established. - Guidelines for implementation and integration of solutions are adopted (best practice). - More precise guidelines and regulations are developed and implemented. - Increased cooperation and knowledge sharing amongst the stakeholders in AMI. - Benefit schemes and better cost allocation for investments are implemented for the stakeholders in AMI. **3** How would you rank the following challenges in information security which may impede further integration and development of AMI? From most negative (1) impact to least (5) negative impact - Costs - Immature technology - Lack of knowledge and expertise within AMI stakeholders - Insufficient regulations and guidelines (in terms of quality and specificity) - The current distribution of roles, responsibilities and governance within the AMI and the energy sector of Norway	The questions will be distributed in an online questionnaire prior to the semi-structured interview.
Ranking of risk elements (Q4-7)	**4** Several potential incidents which can affect information security are described below. How would you describe the risk of the following incidents occurring in AMI? (Very low, low, medium, high, extreme, unknown) *"Risk is a function of the likelihood of an incident happening and the consequences of the incident".* - Unauthorized manipulation of data and equipment through the communication channels.	

	- Unauthorized access and modification of hardware and its locally stored data (equipment and components, firmware, and software). - Inadequate/non-existing availability of data within AMI (e.g., consumption measurements, control signals, commands to units, events, and alarms, etc.). - Unauthorized access to data and information produced in the AMI (violation of data confidentiality). - Unauthorized modification of data and information produced in the AMI (violation of data integrity). - Targeted cyberattacks. - Untargeted cyberattacks. **5** How would you rank the abovementioned incidents in terms of negative impacts on AMI? (Very low, low, medium, high, extreme, unknown) **6** How would you describe the likelihood of the abovementioned incidents occurring in AMI? (Very unlikely, unlikely, possible, likely, very likely, unknown) **7** How would you prioritize the following risk-reducing measures that may handle the above-mentioned incidents? (Choose the 3 most significant) - Management of suppliers (securing the supply chain) - Secure life cycle process for devices and operating procedures - Personnel security (stakeholders and not end-users), security awareness and training - Systems for incident management - Knowledge sharing amongst stakeholders in AMI. - Auditing and accountability (roles, responsibility, and authority) - Physical security - Technical controls for information security	
Part 2: Semi-structured interview with a focus on information security threats and risks		
Infosec risks and threats **Experience with incidents** **Information security risks and threats in operation** **Organization and governance** **Future changes in AMI**	**2.1** What do you think when I say cyber risks in AMI? **2.2** What risks in information security in AMI in Norway are most prominent at your level? **2.3** Are you aware of any information security incidents in AMI or towards the stakeholders operating AMI (in Norway and abroad)? **2.4** How is your level of cyber situational awareness in terms of threats and vulnerabilities in AMI? **2.5** How do you perceive the risk of a cyber incident affecting HW, data and/or the communication channels in AMI occurring in the next 2 years, given the situation in the world today? (In Norway and abroad) **2.6** Do you have any thoughts about what may affect your perception of cyber risks in AMI? **2.7** How do you perceive the distribution of roles, responsibilities, and governance of information security in AMI and the Norwegian energy sector? **2.8** What do you think will be the most significant changes in AMI regarding information security in the next 10 years? (In Norway and abroad) **2.9** How do you perceive the interest in information security in AMI amongst the stakeholders in Norway?	2.2.1 Why these? 2.2.2 What is the most significant risk or threat for the whole system (the greater picture)? 2.2.3 What measure/actions must be implemented to handle the potential obstacles/risks you have identified? 2.2.4 Can you highlight some of the mentioned measures (if several are described)? 2.3.1 Was the vulnerability known? 2.3.2 Can you elaborated on the attack and consequences? 2.3.3 How could the incident have been mitigated? 2.4.1 Do you feel that you have sufficient cyber situational awareness today? 2.5.1 Do you assess the risk as higher or lower for the next 2 years compared to the following 2 years? 2.5.2 Do you perceive that mitigating measures handling the risk have been taken?

		2.6.1 What can improve your awareness for cyber risks? 2.7.1 What measures will potentially streamline and improve the information security work in the Norwegian energy sector? (On an overall level) 2.9.1 Who are the driving players? 2.9.2 Do you view the future of information security in AMI positively?
Additional comments	- Additional comments? - End audio recording - Information about the transcription process - Thank you for participating. We are available for questions and comments	Any comments regarding the interview? Anything we should know related to the MSc thesis topic?

Appendix A2 – Intervjuguide Norsk

Tema	Spørsmål og kommentarer	Oppfølgingsspørsmål
Introduksjon	*Takk for at du har mulighet til å bidra *Generell informasjon masteroppgaven *Kort gjennomgang av hensikt og struktur på intervjuet basert på invitasjon *Start av digitalt opptak (med godkjenning) *Innhente samtykke ihht. Invitasjonen *Avgrensninger i oppgaven og presentasjon av referansemodell	Visualisering av AMS-modellen
Bakgrunns-informasjon	**0.1** Hva er din formelle rolle i organisasjonen og hvilket nivå jobber du på? (strategisk, taktisk, operasjonelt eller teknisk nivå) **0.2** Hvordan vil du beskrive din kjennskap til AMS og informasjonssikkerhet? (På en skala fra 0 (ingen kjennskap) til 10 (ekspert))	
Del 1: Strukturert intervju		
Erfaringer med AMS (Q1-3)	**1** Under er fem antatte merverdier som AMS tilfører samfunnet og operatørene, i form av nye tjenester og leveranser. Hvordan vil du rangere de beskrevne merverdiene, fra størst (1) til lavest (5). - Nye tjenester (e.g., smartlading av elbiler) - Forbedring av eksisterende tjenester (f.eks. nøyaktig avregning av kunder) - Reduserte kostnader til drift og feilsøking av distribusjonsnettet - Økt forsyningssikkerhet av energi til samfunnet - Økt utnyttelse av eksisterende ressurser (f.eks. bedre utnyttelse av eksisterende kraftproduksjon og innlemmelse av distribuert kraftproduksjon (plusskunder)) **2** Under er fem påstander som kan påvirke informasjonssikkerheten i AMS positivt. Hvordan vil du rangere de beskrevne påstandene, fra størst (1) til lavest (5) påvirkning? *"Informasjonssikkerhet i AMS vil forbedres og AMS vil bli integrert på en sikrere måte i en smart grid dersom ..."* - Man etablerer standardiserte tekniske løsninger - Man tilpasser retningslinjer for utplassering og integrasjon (best practice) - Man utvikler og håndhever mer presise reguleringer/påbud - Man får til økt samarbeid og kunnskapsutveksling blant aktørene i AMS - Det innføres stønadsordninger og bedre kostnadsfordeling ved investeringer for aktørene i AMS **3** Hvordan vil du rangere følgende informasjonssikkerhetsmessige utfordringer som kan hindre videre integrering eller utvikling av AMS? Fra mest (1) negativ påvirkning til minst (5) negativ påvirkning. - Kostnader - Umoden teknologi - Manglende kunnskap og ekspertise blant AMS-aktørene - Mangel på eller utilstrekkelige reguleringer og veiledere - Den nåværende fordelingen av roller, ansvar og myndighet innen AMS og energisektoren i Norge	Strukturert intervju vil bli gjennomført med spørreskjema som blir distribuert før semi-strukturert intervju gjennomføres
Rangering av risiko-elementer (Q4-7)	**4** Under er en rekke potensielle hendelser som kan påvirke informasjonssikkerheten beskrevet. Hvor alvorlig vil du beskrive risikoen for at følgende hendelser inntreffer i AMS? (Veldig lav, lav, medium, høy, ekstrem, usikker) *"Risiko er en funksjon av sannsynlighet for at en hendelse inntreffer og konsekvenser av hendelsen"*	

	- Uautorisert påvirkning av data og utstyr i kommunikasjonskanalene - Uautorisert tilgang på og modifikasjon av hardware og dets lokalt lagrede data (utstyr og komponenter, firmware og software) - Mangelfull/ ikke-eksisterende tilgjengelighet på data innad i AMS (f.eks. forbruksmåling, styringssignaler, kommandoer til enheter, hendelser og alarmer etc.) - Uautorisert tilgang til data og informasjon produsert i AMS (brudd på data-konfidensialitet) - Uautorisert endring av data og informasjon produsert i AMS (brudd på data–integritet) - Målrettede cyberangrep - Tilfeldige cyberangrep **5** Over er en rekke potensielle hendelser som kan påvirke informasjonssikkerheten beskrevet. Hvordan vil du beskrive de potensielle hendelsene i form av negativ påvirkning på AMS? (Veldig lav, lav, medium, høy, ekstrem, usikker) **6** Over er en rekke potensielle hendelser som kan påvirke informasjonssikkerheten beskrevet. Hvordan vil du beskrive sannsynligheten for at de potensielle hendelsene inntreffer i AMS? (Veldig usannsynlig, usannsynlig, mulig, sannsynlig, veldig sannsynlig, usikker) **7** Hvordan vil du prioritere følgende risiko-reduserende tiltak som kan håndterer de overnevnte hendelsene? (Velg ut de 3 viktigste) - Administrasjon og kontroll av tredjeparts-leverandører - Sikker livssyklusprosess for komponenter og driftsprosedyrer - Personellsikkerhet, sikkerhetsbevissthet og trening - Beredskap for hendelseshåndtering - Kunnskapsdeling blant AMS-aktører - Revisjon og ansvarliggjøring (roller, ansvar og myndighet) - Fysisk sikkerhet - Tekniske kontroll-mekanismer for informasjonssikkerhet	
Del 2: Semi-strukturert intervju med fokus på infosec risiko og trusler		
Infosec risiko og trusler **Erfaringer med hendelser** **Infosec risiko og trusler i normal drift** **Organisering og styring**	**2.1** Hva tenker du på når jeg nevner cyber risiko i AMS? **2.2** Hvilke risikoer rundt informasjonssikkerheten i AMS i Norge anser du som mest fremtredende fra din posisjon i AMS? **2.3** Kjenner du til noen cyberhendelser i AMS eller mot aktørene som opererer eller leverer tjenester til AMS? (I Norge og utlandet) **2.4** Hvordan er din situasjonsforståelse for cyber-trusler og sårbarheter i AMS? **2.5** Hvordan opplever du risikoen for at en cyberhendelse som påvirker hardware, data og/eller kommunikasjonskanalene i AMS inntreffer de neste 2 årene, gitt dagens situasjon? (I Norge og utlandet) **2.6** Har du noen tanker rundt hva som kan påvirke din oppfattelse av cyber risiko i AMS? **2.7** Hvordan oppfatter du organiseringen og styringen av roller, ansvar og myndighet innenfor informasjonssikkerhet i AMS og kraftsektoren i Norge? **2.8** Hva tror du vil være de største endringene for informasjonssikkerhet i AMS de neste 10 årene?	2.2.1 Hvorfor disse? 2.2.2 Hva er den største risikoen/trusselen for hele systemet (det store bildet)? 2.2.3 Hvilke typer tiltak/handlinger må iverksettes for å håndtere de potensielle hindringene/risikoene du har identifisert? 2.2.4 Vil du fremheve noen av de nevnte tiltakene? (Hvis flere blir nevnt) 2.3.1 Var sårbarheten kjent på forhånd? 2.3.2 Har du mulighet til å utdype om angrepet og konsekvensen av hendelsen(e)? 2.3.3 Hvordan kunne denne hendelsen blitt begrenset/stoppet? 2.4.1 Føler du at du har god nok situasjonsforståelse informasjonssikkerhetsmessig i dag?

Fremtidige endringer i AMS	**2.9** Hvordan oppfatter du at interessen er for informasjonssikkerhet i AMS blant aktørene i Norge?	2.5.1 Vurderer du risikoen som høyere eller lavere de neste 2 årene sammenlignet med de 2 foregående årene? 2.5.2 Kjenner du til noen tiltak som er tiltenkt å håndtere og redusere risikoen? 2.6.1 Hva kan tilrettelegges for å øke oppfattelse/forståelse av cyber-risiko? 2.7 Hvilke tiltak ville kunne effektivisere og forbedre arbeidet med informasjonssikkerhet i kraftsektoren? (På et overordnet nivå) 2.9.1 Hvem er de drivende aktørene? 2.9.2 Ser du positivt på informasjonssikkerhetsfremtiden til AMS?
Kommentarer	- Ytterlige kommentarer? - Avslutte digitalt opptak - Informasjon om transkriberingsprosessen - Takk for din deltakelse. Vi er tilgjengelig for spørsmål og kommentarer	Kommentarer angående intervjuet? Er det noe vi bør vite relatert til oppgavens emne?

Appendix B1 - Invitation to Interview with Informed Consent

Master thesis: ***"****Attitudes and perception of AMI information security risk in the Energy sector of Norway" by Eirik Lien and Karl Magnus Grønning Bergh*

Dear participant,

Our names are Eirik and Karl Magnus, and we are inviting you to participate in a survey interview about the perception of information security within the Advanced Metering Infrastructure in Norway. The target audience includes decision makers and technical specialists at all organizational levels. We also encourage individuals in other positions to participate, e.g., researchers and analysts.

The survey is part of our master's thesis in Information Security at the Norwegian University of Science and Technology (NTNU), which is supervised by Sokratis Katsikas, Professor at the Department of Information Security and Communication Technology. Its findings will contribute to increased situational awareness at governance and industry-level of the state of risk perception within AMI in the energy sector of Norway.

Background and purpose of the study

The implementation of the Advanced Metering Infrastructure (AMI) has enabled smart distribution of energy to endpoints/end-users, facilitated by 2-way communication in near real-time, measuring and collecting the energy flow and usage data. To ensure the confidentiality, integrity and availability of data in AMI, controls and management systems have been established to protect against unwanted intended incidents (e.g., cyberattacks), set to handle the risks emerging in AMI.

In this study, the researchers want to explore the perception of information security risks amongst stakeholders in AMI and compare the perceived risks to risks identified by scientific literature, and further explore potential gaps between the two. If gaps are found, the study will attempt to identify causes for this gap, with a focus on knowledge, and organizational and regulatory challenges. It will also attempt to identify how these gaps can be addressed and bridged.

The participants are stakeholders in AMI of Norway, such as energy distributors, AMI operators, customers, and regulatory authorities.

Participation:

- The study will be conducted by interviewing participants, analyzing the results and comparing the findings against a structured literature study on prevalent threats and vulnerabilities in AMI.
- An initial internet questionnaire will be presented to each participant during the interview to optimize the data collection and give more time to the oral interview.
- The interview takes approximately 60 minutes to complete and will be done individually.
- The interviews will be digitally recorded for transcription, where the transcription will be forwarded to the participants for approval. The participant can at any time redact information from the interview if it is deemed sensitive.
- The participation is voluntary, and the participant can withdraw from the study at any given time. Subsequently, all recorded data will be deleted and excluded from the study.

Confidentiality and handling of data:

- Responses, data, results, and the final report will be anonymized, both in terms of personal and company identifiable information.
- The study is approved by Norsk Senter for Forskningsdata (NSD) and their privacy protection-department.
- Collected data will be retained in accordance with NSD regulations and guidelines. As such, all personal and company identifiable information will be treated as confidential and sensitive information and kept separate from the interview data collected. Only the researchers themselves will have access to this information.
- All personal and company identifiable information will be deleted when the report is approved after submission (expected Sept/Oct 2023).

If you want to participate or have questions concerning the study, please contact us by mail or phone: <*NTNU e-mail address*> or <*NTNU e-mail address*>. Please forward this invitation to anyone you think should participate in the study. Thank you in advance for your time! Sincerely, Eirik Lien and Karl Magnus Grønning Bergh

Consent to participate in the study:

I have received and understood the above information about the research study "*Attitudes and Perception of AMI information security in the energy sector of Norway"*. I hereby give consent that the information given may be used to support the research as described above.

_____ ,

Date Sign.

Appendix B2 - Invitasjon til intervju med samtykkeerklæring

Masteroppgave: *"Holdninger til og persepsjon av AMS informasjonssikkerhetsrisiko i energisektoren i Norge" av Eirik Lien og Karl Magnus Grønning Bergh*

Kjære deltaker,

Vi heter Eirik og Karl Magnus, og vi ønsker å invitere deg til deltakelse i en intervjuundersøkelse som tar for seg persepsjon av risiko knyttet til informasjonssikkerhet i Avansert Måle- og Styringssystemer (AMS) i Norge. Målgruppen inkluderer beslutningstakere og teknisk personell på alle nivåer i organisasjonene. Vi oppfordrer også individer i andre posisjoner til å delta, f.eks. forskere og analytikere.

Denne undersøkelsen er en del av vår masteroppgave i informasjonssikkerhet ved Norges Teknisk-Naturvitenskapelige Universitet (NTNU), som er veiledet av Sokratis Katsikas, professor ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi. Funnene i denne oppgaven kan bidra til å øke situasjonsforståelsen hos regulerende myndigheter og industrien for tilstanden til risikoforståelse innen AMS i energisektoren i Norge.

Bakgrunn og hensikt med studien

Implementasjonen av AMS har muliggjort smart distribusjon av energi til sluttbrukere, ved hjelp av 2-veis kommunikasjon i tilnærmet sanntid, ved måling og innsamling av energistrømmer og brukerdata. For å sikre konfidensialiteten, integriteten og tilgjengeligheten til data i AMS, har kontroller og styringssystemer blitt etablert for å beskytte mot uønskede, villede handlinger og hendelser (f.eks. cyber-angrep). Disse tiltakene skal håndtere risikoen som innføringen og driften av AMS medfører.

I denne studien vil forskerne undersøke persepsjon av risiko for brudd i informasjonssikkerhet blant aktørene i AMS, og sammenligne oppfattet risiko med risiko identifisert i akademisk vitenskapelig litteratur, og samtidig utforske eventuelle gap mellom disse. Hvis avvik identifiseres, vil studien videre prøve å identifisere årsaker til avvikene, med et søkelys på kunnskap og organisatoriske og regulerende utfordringer. Studien vil også prøve å identifisere hvordan disse avvikene kan bli håndtert og minimert.

Deltakerne er aktørene i AMS i Norge, slik som distribusjonsselskaper, AMS-operatører og produsenter, kunder og regulerende myndigheter.

Deltakelse:

- Studien vil bli gjennomført ved å intervjue deltakere, analysere data og sammenligne funn mot en strukturer litteraturstudie som ser på utbredte trusler og sårbarheter i AMS fra et akademisk ståsted.
- En innledende spørreundersøkelse vil bli presentert for alle deltakerne i hvert intervju for å optimalisere datainnsamlingen og gi mer tid til det muntlige intervjuet.
- Intervjuet vil ta ca. 60 minutter å gjennomføre og vil bli gjort individuelt.
- Intervjuene vil bli tatt opp digital for transkripsjon, og transkripsjonen vil bli sendt til den individuelle deltaker for godkjenning. Deltakeren kan når som helst fjerne informasjon fra intervjuet hvis avgitt informasjon blir ansett som sensitivt.

- Deltakelse i intervjuet er frivillig, og deltakeren kan når som helst trekke seg fra studien. Dette vil medføre at alle opptak og alt innsamlet data fra intervjuet vil bli slettet og utelatt fra studien.

Konfidensialitet og håndtering av data:

- Svar, data, resultater og selve rapporten vil bli anonymisert med tanke på informasjon som kan identifisere den enkelte person og selskap.
- Studien er godkjent av Norsk Senter for Forskningsdata (NSD).
- Innsamlet data vil bli oppbevart og behandlet i samsvar med NSD sine retningslinjer. Dette medfører at all informasjon som kan identifisere den enkelte deltaker og selskap vil bli behandlet som konfidensiell og sensitiv informasjon, og oppbevart separat fra intervju-data som blir innsamlet. Det vil kun være forskerne som vil ha tilgang til denne informasjonen.
- All informasjon som kan identifisere den enkelte deltaker og selskap vil bli slettet når rapporten er godkjent etter innlevering (forventet september/oktober 2023).

Hvis du har mulighet til å delta eller har spørsmål angående studien, så kan du kontakte oss på epost eller telefon: <*NTNU e-post*> eller <*NTNU e-post*>. Det er også mulig å videresende denne invitasjonen til andre du mener burde delta i studien. På forhånd ønsker vi å takke deg og håper vi ser deg som en deltaker om ikke lenge. Med vennlig hilsen Eirik Lien og Karl Magnus Grønning Bergh.

Samtykke til deltakelse i studien:

Jeg har mottatt og forstått informasjonen gitt i dette dokumentet angående studien "*Holdninger til og persepsjon av AMS informasjonssikkerhetsrisiko i energisektoren i Norge"*. Jeg gir herved samtykke til at informasjon avgitt i undersøkelsen kan bli brukt som del av forskningsoppgaven beskrevet i dette dokumentet.

_____ ,

Dato Sign.

Appendix C - NSD Approval

Sikt

Meldeskjema / MIS 4900 Attitudes and Perception of AMI Information Security in th... / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer
412028

Vurderingstype
Automatisk

Dato
06.12.2022

Prosjekttittel
MIS 4900 Attitudes and Perception of AMI Information Security in the Energy Sector of Norway

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Sokratis Katsikas

Student
Karl Magnus Bergh

Prosjektperiode
01.09.2022 - 30.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 30.06.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

Appendix D - Tabulation of SLR

Identified security challenges HW

References	Vulnerabilities	Threats	Attack descriptions	Impact towards CIAPI3A objectives	Impact towards AMI	Likelihood description	Risk evaluation or description
[1], Security analysis of an advanced metering infrastructure, 2017	Does not describe vulnerabilities in specific, but focuses on the potential for vulnerability discovery with the different available interfaces on the SM and the DC and by reverse engineering components and SW/FW	Identifies the attack vectors on SM and DC and describes attacks and threats that can exploit the vectors in the physical and cyber domain by HW/FW/data interception and modification. Threat actors mentioned are nation state actors, however, does not focus on actors or their motivation.	Does not describe the details of how attacks may be conducted, but describes the attack vectors through which attacks may be conducted as physical access to SM and DC, cyber access to SM and DC, and cyber access to SM and collector via compromised supply chain	Confidentiality, integrity, and availability	Theft of data, theft of power, denial of power and disruption of grid	Not described in specific	Not described in specific
[103], A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure, 2015	Describes vulnerabilities as the physical access to devices where attacker can interfere with them, coupled with architecture with poor access controls and design-vulnerabilities in the HW (e.g., resource constrained).	The vulnerabilities may enable the injection of malicious code or physically tampering with the devices to affect FW, commands sent/received or stored data in the devices. Threat actors are not mentioned.	The most common attack type is described as FDI attack to affect the consumption data in the physical memory	Not described specifically, but based on attack types, they can affect confidentiality, integrity, availability, privacy, identification, authentication, authorization, accountability	Not described in specific	Not described in specific	Not described in specific
[104], Communications Systems in Smart Metering: A Concise Systematic Literature review, 2022	Describes the physical access to devices where attacker can interfere with them, coupled with architecture with poor access controls and design-vulnerabilities in the HW (e.g., resource constrained) as key vulnerabilities. These enable modification of or interference with components and data in SM and DC.	The modification can be done by injecting malicious code or physically tampering with the devices to affect FW, commands sent/received or stored data in the devices. Threat actors are not mentioned.	Describes threats that affect the physical HW (manipulating SW, FW, and data)	Not described specifically, but the threats described will affect the confidentiality, integrity, and availability	Not described in specific	Not described in specific	Not described in specific

[105], Advanced metering infrastructures: security risks and mitigation, 2020	Describes the vulnerability of physical access to devices where attacker can interfere with them, coupled with architecture with poor access controls and design-vulnerabilities in the HW (e.g., resource constrained). These enable modification of or interference with components and data in SM and DC.	Threats are overarchingly described as injection of malicious code or data, or physically tampering with the devices to affect FW, commands sent/received or stored data in the devices. Specific threats to HW are mentioned as splashing (bricks the device) and data theft (FW for reverse engineering, and data profiling) Threat actors are generally described as malicious customers, insiders, criminal organizations, terrorists, competing organizations and nation states. The motivation is not discussed.	The most common attacks utilize the attack vectors targeting the endpoints or the communication channel, accomplished by physical or cyber access to the devices or to the supply chain.	Describes the main goal of attacks to be unauthorized access to devices or networks, thus impacting confidentiality, integrity, availability, and privacy.	Describes energy theft and the following financial loss as one of the most considerable challenges.	Does not describe likelihood of threats but describes the use of attack graphs to identify attack paths that are most likely to succeed.	Defines the main cyber risks to AMI security to be energy theft (theft of service), data theft (includes FDIA, interception and eavesdropping), AMI communication and networks and APTs.
[106], A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid, 2015	The study describes the vulnerabilities of the ICS and SM security posture and the inherent weaknesses within the HW. It specifically explores hardcoded credentials and memory errors in devices and poor security implementation (old protocols like DNP3 gives poor encryption and authentication) The focus is also on the digital forensics process toward the HW that resides within the electric power system.	Vulnerabilities can be exploited by FDI, reverse engineering of HW and FW, and supply chain attacks by manipulating HW or FW. Weak encryption and authentication can enable spoofing of data and commands, possibly affecting breaker functionality. Threat actors are not described.	Describes the attacks on HW using the JTAGs for access to devices, searching for exploitable memory vulnerabilities iot to extract FW and data.	Does not consider the impacts regarding security objectives specifically, but the attacks described would affect confidentiality, integrity, privacy, and authentication	Briefly states how DoS conditions may occur when memory errors or vulnerabilities are exploited, causing temporary disruption or persistent system failure.	Not described in specific	Not described in specific
[107], Performance analysis of smart metering for smart grid: An overview, 2015	The vulnerabilities are overarchingly the physical access to devices (SM and DCs) and an exposed supply chain	Threats include exploiting the supply chain or the local interfaces iot Inject malicious code or physically tamper with the devices or its components to affect FW, commands sent/received or stored data in the devices. Threat actors are not described.	The use of social engineering or insiders to affect the supply chain is briefly described	Confidentiality, integrity, availability, privacy, authentication	Does not describe impacts to AMI in detail but mentions the effect from network intrusions as breach of privacy to cascading failures in AMI.	Not described in specific	Describes the risk of HW tampering as high due to the physical access to devices.

[100], Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure, 2015	Identifies the attack surface on HW (SM and DCs), which are defined as the local interfaces and the physical access to the device. In SMs the interfaces are the networking interfaces towards end-user domain (HAN-port) and to DC or head-end (wireless), together with the maintenance interface (optical). Similar surfaces are present at the DC, with interface towards SMs (radio mesh) and towards head-end (GSM or wired). These interfaces and the physical access are considered the main vulnerabilities in HW. Another significant vulnerability is the hard coding of keys and algorithms in HW to obtain security by obscurity	The threats to SMs and DCs consist of local wireless network attacks (radio and optical interfaces) and serial bus attacks (physical access to device). The DC is also subject to TCP/IP attacks depending on the type of backhaul connection to head-end. Such attacks can give access to FW, SW, data and hard-coded keys and algorithms in HW. Describes 3 types of general threats to the power grid as theft of power (attacks on individual SM to enable theft of power from the utility), denial of power (attacks on individual SM to disconnect consumers) and disruption of grid (attacks on a significant number of devices to create transient power behavior) Threat actors are not specifically described, but the general motivation for attacks is seen as disruption of national critical infrastructure, skill testing, industrial espionage and as a launching point for other attacks.	Does not describe attacks specifically	Does not classify the threats regarding security objectives, however the threats describe will affect integrity, availability, confidentiality or privacy of data and devices in AMI.	The potential effects are disabling of power delivery systems and breach of privacy. Attacks on the integrity of data in AMI can result in loss of SA and grid control.	Not described in specific	Not described in specific, but understanding the attack surface is a first step in obtaining cyber security and understanding the concept of risk.
[108], The role of communication systems in smart grids: Architectures, technical solutions and research challenges, 2013	Summarizes vulnerabilities in HW as device vulnerabilities, where the physical access to distributed devices and the interfaces they use for communication are possible attack vectors.	Does not describe how devices can be compromised physically to extract information, but describes how the unprotected physical medium of wireless communication can enable attackers to perform eavesdropping, jamming the medium, and inject false data (FDIA) Threat actors are not described.	Does not provide specific attack descriptions	Considers availability as the most important security objective (in a power network), together with privacy of consumer data. But does not categorize threats into impacts towards the objectives.	Not described in specific	Explains how PRA can be used in risk assessments to account for uncertainties in risk. However, it does not give an evaluation of the vulnerabilities and threats described in this regard.	Describes how trust systems can be used in risk assessments to determine risks and to give weight to those risks (an entity can assess the reliability of another entity before interacting with it)

[42], Risikovurdering av AMS. Kartlegging av informasjonssikker hetsmessige sårbarheter i AMS, 2012	Vulnerabilities in HW are mainly device vulnerabilities, where the physical access to distributed devices and the interfaces they use for communication are possible attack vectors.	Targeted tampering and manipulation of HW, enabling manipulation of functionality (breaker) and locally produced and stored data. Injection of malware in HW connected to communication channel. Threat actors described are external and internal	Targeted local manipulation of metering data causing erroneous or no measurement data, the use of interfaces for accessing HW.	Does not describe or classify the threats according to security objectives. But the different threats exemplified can breach confidentiality, integrity availability and privacy.	Lack of measurement data and/or its transfer or producing corrupted data affecting billing. Triggering breaker function causing denial of power	Likelihood for targeted attacks is described as combination of the consequence in terms of number of affected units and the complexity of the attack.	Conducts risk assessment of a generic implementation in a Norwegian context, producing a risk matrix for selected incidents.
[43], Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision, 2022	The main vulnerabilities described in HW, are the bidirectional communication between devices and the distribution control center, the resource constrained environment in SMs and DC, and the physical exposure of the devices.	Threats exploiting the bidirectional communication is masquerading as HES/MDMS and issuing malicious commands. The resource constrained environment can be exploited by buffer overflow attacks, while the physical access can be used to tamper with stored data and FW on the devices, e.g using FDIA. Threat actors are not described.	Described overarchingly for all the different threats.	Confidentiality, integrity, availability, privacy	The impacts of threats exploiting the bidirectional communication and injecting commands is the triggering of the breaker functionality, causing denial of power. The buffer overflow can cause instability in SM operation and functionality, while the tampering of data or FW can cause theft of power or SM shutdown.	Not described in specific	Discusses how the increasing numbers of IoT devices (SM and DCs) are increasing the risk. Also underlines the importance of risk assessments to identify vulnerabilities and threats, iot determine if additional countermeasures are needed. However, it does not conduct a risk evaluation based on the described vulnerabilities and threats

[101], Review of Cyber-Physical Attacks and Counter Defence Mechanisms for Advanced Metering Infrastructure in Smart Grid, 2018	Describes one of the most prominent attack surfaces in AMI, and the vulnerabilities it exposes, being the SM and DC. This is due to the physical access and constrained resources (limited defense capabilities) of the devices.	The vulnerabilities open up for meter spoofing and energy fraud attacks by extracting the identification credentials from the SM, authentication attacks by extraction authentication details from SM memory, FDI attacks by injecting malicious data or FW on the SM, and DoS by overwhelming the communication links or tampering with the routing tables. Threat actors are not described.	Not described in specific.	Threats are categorized in terms of impact to security objectives, where DoS impacts availability, FDI impacts integrity, and authentication attacks impacts confidentiality	A DoS can render a SM incapable of responding to requests and may disconnect the SM from the network. Authentication attacks enables future attacks such as spoofing. FDI attacks can cause corrupted measurement affecting billing or the stability in the grid.	Not described in specific	Not described in specific
[102], Attacks, vulnerabilities and security requirements in smart metering networks	Does not describe vulnerabilities in specific, beyond that SMs may have insufficient tampering mechanisms and are resource constrained. Nearly all researched schemes were vulnerable to CMP	Describes threats and attacks towards the SM devices using the node compromise attack (CMP), where hijacking the SM physically by accessing the SM to take control of the communication and gain unauthorized access to the node's sensitive data, including cryptographic keys used. This attack can enable an impersonation attack, FDI, DoS, replay and repudiation attacks. Threat actors are not described.	Not described in specific	Depending on techniques used it can impact all security objectives	Not described in specific	Not described in specific	Not described in specific

[90], Threat Modelling of AMI, 2013	The physical interfaces in SM for maintenance and communications are identified as vulnerable entry points for a set of threats using the STRIDE and Attack Tree modelling techniques. The vulnerabilities to the identified threats depend on the implementation of anti-tampering mechanisms at SMs, how authentication is implemented (is an attacker able to authenticate as maintenance), and the ability to withstand intrusion attacks and detect unauthorized changes.	Based on STRIDE, it identifies data tampering and modification through local maintenance altering SM data or SW and SM reporting wrong data to maintenance. Further, information disclosure (leaking of config. settings, keys, messages or SW/FW), DoS (by physically disabling communications), and lastly, elevation of privileges (at SM and HES). Threat actors are not described.	Does not provide specific attack descriptions	Data tampering and modification impacts the integrity of data, while DoS affects the availability of the SM, and information disclosure affects the confidentiality of data and information stored or received at the SM.	Describes attacker goals by targeting the SMs (based on the Attack Tree) as manipulation of power measurements for economical gain, to attack other SMs, and to limit the ability to control or access SMs. However, it highlights that evaluations of consequences are highly dependent on the individual system.	Explains how evaluations of likelihood are highly dependent on the individual systems and is thus not considered.	Discusses how threat models can be valuable input to risk assessments.
[109], Smart grid security: Attacks and defence techniques, 2022	It does not describe vulnerabilities in specific, other than how the physical interfaces and access to HW makes it vulnerable.	The physical access to the HW itself makes it prone to threats from meter theft and manipulation, where an attacker can extract information or reverse engineer SW and FW. The interfaces are vulnerable to FDI, with the goal of affecting the functionality and data within the SM. Both threats can be combined with or be the basis for other threats such as MitM, spoofing, impersonation, and message replay attacks. Threat actors are not described.	One description is given where FDI is used to take control over a target device for malicious purposes but does not describe the attack in detail.	Confidentiality, integrity, availability, non-repudiation	Not described in specific	Not described in specific	Not described in specific

[86], False data injection threats in active distribution systems: A comprehensive survey, 2022	The article describes the physical access to the SMs, their communication interfaces and insecure protocols as vulnerabilities, enabling illegal connections and meter tampering.	The article classifies FDI threats according to their attack targets, where AMI in terms of communication channels, SMs and distribution control center are defined as targets. Regarding SMs, there are several individual targets described: 1) The energy profile (reducing own consumption) by MitM FDI, 2) Load profile by privacy attack, 3) Disruption of energy consumption data by false load attack (to reduce energy bill), and 4) SM energy generation data by short-term FDI (to report higher energy exports). Threat actors are not described.	Energy profile attack by MitM FDI, where an attacker injects false data in its own SM to reduce own consumption, while compensating the discrepancy by also compromising neighboring SMs. Load profile attacks by privacy attacks, conducted by extracting reactive power data to identify appliances. Disruption of energy consumption data by false load attack, where the load is switched off synchronous with the sampling rate of the SM. SM energy generation data by short-term FDI, where false data is injected in the SM or generator buses to increase the readings of generated energy	FDI attacks generally target the integrity aspect of SM, AMI and SG.	By degrading the integrity of data in SM and AMI, it can impact the reliability and stability of the SG, by affecting the operational decisions in the system.	Not described in specific.	Not described in specific.

Identified security challenges communication channels

References	Vulnerabilities	Threats	Attack descriptions	Impact towards CIAPI3A objectives	Impact towards AMI	Likelihood description	Risk evaluation or description
[1], Security analysis of an advanced metering infrastructure, 2017	Does not describe vulnerabilities in specific, but focuses on the potential for vulnerability discovery with the different available interfaces on the SM and the DC and by reverse engineering components and SW/FW	Identifies the attacks vectors on SM and DC and describes attacks and threats that can exploit the vectors in the communication channels. This includes cyber access to devices through the communication technology used, iot to conduct interception, injection and blocking attacks on data and commands. (DoS, FDIA, sniffing, spoofing, MitM time sync attack). Threat actors mentioned are nation state actors, however, does not focus on actors or their motivation.	Does not describe the details of how attacks may be conducted, but describes the attack vectors through which attacks may be conducted as physical access to SM and DC, cyber access to SM and DC, and cyber access to SM and collector via compromised supply chain	Confidentiality, integrity and availability	Theft of data, theft of power, denial of power and disruption of grid	Not described in specific	Not described in specific
[103], A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure, 2015	Does not describe vulnerabilities in specific, but the threats described implicitly takes advantages of the exposed communication channels and interfaces around the SM.	Describes threats affecting the communication channel by remote network exploitation and using the SMs network interfaces to compromise SM, steal credentials and conduct FDI. Threat actors are not mentioned.	Describes threats that affect the data and the commands within and received on the communication channels and interfaces provided in the SM.	Not described specifically, but based on attack types, they can affect confidentiality, integrity, availability, privacy, identification, authentication, authorization, accountability	Not described in specific	Not described in specific	Not described in specific

[104], Communications Systems in Smart Metering: A Concise Systematic Literature review, 2022	Does not describe vulnerabilities in specific, but the threats described implicitly takes advantages of the exposed communication channels and interfaces around the SM.	Due to the type of communication technology and protocols used, the access to the wireless and wired medium and potential shortfalls in authentication and encryption, they can be exploited by DDoS, DoS, MitM, data tampering and modification, FDIA, sniffing, malware injection, eavesdropping, spoofing/masquerading. Threat actors are not mentioned.	Classifies attacks on the communication channels as data attacks (affecting the communication network traffic) and network attacks (affecting the protocols used and the interconnections between entities in AMI)	Not describe specifically but the threats identified the can affect confidentiality, integrity and availability, depending on how attacks are conducted and the combination of them.	Describes attacks on data by inserting, changing, or deleting data or control commands to fool the smart grid into making incorrect decisions or actions. Attacks like sniffing, MitM, FDI, impersonation are used to impact confidentiality and integrity of the AMI data and to gain unauthorized access to information or disrupt the normal operation of the system.	Not described in specific	Describes how the availability of attacker tools increases the overall risk levels
[105], Advanced metering infrastructures: security risks and mitigation, 2020	The access to the communication medium (wired or wireless), the technology and protocols used makes the communication channels accessible and prominent targets.	The vulnerabilities can be exploited by DoS, MitM, data tampering and modification, malware and virus injection, FDIA, spoofing and masquerading/impersonation of devices. Threat actors are generally described as malicious customers, insiders, criminal organizations, terrorists, competing organizations and nation states. The motivation is not discussed.	The remote connection between SM, DCs and HES/MDMS and the bidirectional communication, makes the entities vulnerable to different attacks aiming at performing denial of data transfer and command execution, data and FW tampering and modification.	Describes the main goal of attacks to be unauthorized access to devices or networks, thus impacting confidentiality, integrity, availability and privacy.	Describes how attacks in the communication network can compromise devices and HES/MDMS, and enable localized or widespread denial-of-power by issuing disconnect commands	Does not describe likelihood, of threats, but describes the use of attack graphs to identify attack paths that are most likely to succeed.	Defines the main cyber risks to AMI security to be energy theft (theft of service), data theft (includes FDIA, interception and eavesdropping), AMI communication and networks, and APTs

[106], A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid, 2015	The weakness of unsecured communication protocols within the ecosystem is overarchingly described. Highlighting the lack of encryption in old but widely used Modbus and DNP3 protocols. The paper describes, in brief, the lack of authentication within some of the ICS that is used in the electric power system.	The threats that can exploit the described weaknesses are common FDI attacks, by spoofing commands and data, and poisoning the control algorithms. Threat actors are not described.	Only provides general descriptions of poisoning attacks in the communication channel exploits weak protocols.	Does not describe impacts towards security objectives specifically, but by exploiting the vulnerabilities described, they can affect confidentiality, integrity and availability.	The impacts towards AMI as a system is described overarchingly as physical damage and persistent denial of service conditions such as engaging the breaker functionality.	Not described specifically, however describes how it is common for several segments of the power grid to employ old and unsecure communication protocols	Not described in specific
[13], Cyber-security on smart grid: Threats and potential solutions, 2020	The paper focuses on network and communication vulnerabilities in the SG, where AMI is a central communication channel. Does not describe specific vulnerabilities for AMI but considers general vulnerabilities for the SG such as the access to the wired and wireless communication channels used, and the use of internet-based protocols and public solutions.	The threats are classified in terms of security objectives they affect. Confidentiality: Social engineering, eavesdropping, traffic analysis, MitM, sniffing, replay, masquerading, FDI Integrity: Tampering, replay, wormhole, FDI, spoofing, data modification, MitM, time synchronization, masquerading, load-drop attacks Availability: Jamming, wormhole, DoS, buffer overflow, teardrop, smurf, puppet, time synchronization, masquerading, spoofing, MitM attacks. Threat actors not described.	Describes attacks according to the security objectives they breach but does not give descriptions on how the different attacks can be performed. But claims that SG attacks are usually coordinated, targeting all security objectives and SG components (e.g AMI devices)	Threats are described with a focus on breach of the security objectives (CIA). Categorizes attacks based on the objectives.	Considers availability as the prominent security requirement, where attacks can affect the real-time communication and information exchange, thus affecting the balance between power generation and consumption in SG.	Describes the challenges with PRA (PRA) for energy control systems, due to the lack of historical data and statistical examples.	Not described in specific

[110], Data-centric threats and their impacts to real-time communications in smart grid, 2016	The vulnerabilities described are the inherent properties in the communication technology used, such as the accessibility of wireless channels and the physical access to the distributed elements (SM and DCs). It further details how vulnerable the AMI is to composite attacks, such as a combination of FDIA and DDoS, and Load Redistribution attack and MitM	The threat described is the effectiveness of composite attacks, which targets the head-end and control center rather than the distributed elements of AMI. Threat actors are not described.	The FDIA and DDoS attack is carried in tandem to delay the communication and commands from the control center (DDoS) based on actions provoked by the FDIA. The Load Redistribution and MitM attack is similarly carried out in tandem, where a compromised DC redirects commands and communication from the control center (MitM), which are issued based on the effects of the Load Redistribution attack using compromised SMs	The FDIA and MitM mainly affects the confidentiality and integrity of information, while DDoS affects availability	The composite attacks have the potential to affect the stability of the grid, by delaying communications from the control center. The composite attacks described had 10x times the voltage collapse compared to single attacks of Load Redistribution attacks and FDIA	Not described in specific	Not described in specific
[107], Performance analysis of smart metering for smart grid: An overview, 2015	Describes threats to AMI communication based on the inherent vulnerabilities associated with communication and networked systems. The type of communication medium (wired or wireless) and the technology and protocols used gives way to different vulnerabilities, however they are not described in detail.	Describes 3 main categories cyber-physical threats, including DoS (communication link flooding by spoofing packets or engaging breaker functionality), MitM (eavesdropping with the option of FDI, rerouting or blocking/delaying data and commands) and data integrity threats (data modification, FDI and data replay) Threat actors are not described.	Does not describe how the main categories of threats can be performed in detail	The main categories of threats will affect confidentiality (MitM), integrity (MitM, data integrity attacks), availability (MitM, DoS)	Does not describe impacts to AMI in detail but mentions the effect from network intrusions as breach of privacy to cascading failures in AMI.	Not described in specific	Describes briefly how the dependence of vulnerable communicatio n and networked systems increases the risk of compromising power system operation.

[100], Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure, 2015	The geographical dispersion of the network and use of multiple communication technologies (e.g wired Ethernet and wireless radio mesh), coupled with resource constrained devices with long lifespan expectancy in the network provides ample cyberattack surfaces and potentially persistent vulnerabilities. The communication links in the network also uses a wide range of protocols, which may contain inherent vulnerabilities, such as ANSI C.12.22 (weak encryption) and SEP 2.0.	The threats to the communication channel consist of threats to the wireless channels (radio mesh or cellular) or exploiting the vulnerabilities in the different protocols. Describes 3 types of general threats to the power grid as theft of power (attacks on individual SM to enable theft of power from the utility), denial of power (attacks on individual SM to disconnect consumers) and disruption of grid (attacks on a significant number of devices to create transient power behavior). Threat actors are not specifically described, but the general motivation for attacks is seen as disruption of national critical infrastructure, skill testing, industrial espionage and as a launching point for other attacks.	Does not describe attacks specifically	Does not classify the threats regarding security objective, however the threats describe will affect integrity, availability, confidentiality or privacy of data and devices in AMI.	The potential effects are disabling of power delivery systems and breach of privacy. Attacks on the integrity of data in AMI can result in loss of SA and grid control.	Not described in specific	Not described in specific, but understanding the attack surface is a first step in obtaining cyber security and understanding the concept of risk.
[108], The role of communication systems in smart grids: Architectures, technical solutions and research challenges, 2013	The vulnerabilities in the communication channels are based on the use of publicly available communication standards and open network architectures.	The threats are overarchingly described as similar to those of other open architectures adopted by telecom networks. Examples of threats are malicious modification of routing protocols, DoS-type attacks and MitM. Threat actors are not described.	Does not provide specific attack descriptions	Considers availability as the most important security objective (in a power network), together with privacy of consumer data. The threats described affects the confidentiality (MitM), integrity (MitM, routing table poisoning), availability (DoS) and privacy (MitM)	Not described in specific	Explains how PRA can be used in risk assessments to account for uncertainties in risk. However, it does not give an evaluation of the vulnerabilities and threats described in this regard.	Describes how trust systems can be used in risk assessments to determine risks and to give weight to those risks (an entity can assess the reliability of another entity before interacting with it).

[42], Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS, 2012	Describes different scenarios and incidents, where GSM/GPRS, RF and PLC can be used for communication. Does not describe specific vulnerabilities within the solutions. However, describes how the use of standard commercial devices and a level of interconnectedness with a connection to internet, makes AMI vulnerable to regular ICT threats. Further describes how the use of 3rd party infrastructure for communication makes AMI vulnerable to attacks on this party. .	Describes targeted and non-targeted threats as the main categories towards ICT and AMI but provides only some examples of specific threats in these categories concerning communication. DoS is described as both a targeted and non-targeted threat in the communication, which can be caused by malware or automated tools. Targeted threats can be eavesdropping and interception of data in transit and traffic analysis of end-users causing privacy breaches. Threat actors described are external and internal	Describes five different scenarios, and the potential incidents causing them: 1) Large number of SMs out of operation (breaker not engaged) caused by malware accessing HW in communication channel. 2) End-user manipulation of consumption data causing erroneous data for billing. 3) Insider manipulation of functionality and data, injection of malware, extraction of data. 4) Targeted attack on a specific geographical area by remote attacks, insider or a combination. 5) 3rd party access providing additional vectors for attack	Does not classify threats according to security objectives. But the threats exemplified can affect confidentiality, integrity, availability and/or privacy	Lack of measurement data and/or its transfer or producing corrupted data affecting billing, estimation of load for planning and causing instability in operation of grid. Attacks affecting 3rd party service can impact AMS if they use the same infrastructure, such as unavailable communication channel.	Likelihood for targeted attacks is described as combination of the consequence in terms of number of affected units and the complexity of the attack.	Conducts risk assessment of a generic implementation in a Norwegian context, producing a risk matrix for selected incidents. Does not assess incidents in the communication channel specifically.

[43], Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision, 2022	The main vulnerabilities in the communication channels are based on the communication medium used (wired or wireless), the technology used for the medium and the security implemented in the technology. Different media and technologies will produce different vulnerabilities, but the most significant is the use of wireless communication between SMs and DCs due to the large distance between the devices. Another	The use of wireless communication medium can be exploited by session hijacking and is susceptible to DoS attacks, while the wireless technology and its security posture can enable MitM and FDI attacks due to the direct connection between HES and SMs and the remote updating feature of FW/SW. Threat actors are not described.	Described overarchingly for all the different threats.	Considers attacks modifying applications or data running in the AMI to affect the integrity of the system, while attacks compromising the customer data affects both confidentiality and integrity of the data. Attacks tampering with FW or SW is considered to affect confidentiality, integrity and availability	The impacts of session hijacking and MitM can be data and FW manipulation or theft, while DoS can congest the bandwidth and cause loss and congestion of data.	Not described in specific	Discusses how the increasing numbers of IoT devices (SM and DCs) are increasing the risk. Also underlines the importance of risk assessments to identify vulnerabilities and threats, iot determine if additional countermeasures are needed. However, it does not conduct a risk evaluation based on the described vulnerabilities and threats

[101], Review of Cyber-Physical Attacks and Counter Defence Mechanisms for Advanced Metering Infrastructure in Smart Grid, 2018	Describes one of the most prominent attack surfaces in AMI, and the vulnerabilities it exposes, being the communication network. This is due to the use of publicly available communication networks and technologies and the geographical dispersion of the network.	The vulnerabilities open up for FDIA to insert random and corrupted data, DoS to prevent communication between SM, DC and HES, MitM to enable, de-pseudonymization attacks, authentication attacks by session hijacking to enable spoofing, and disaggregation attacks (privacy attack by profiling the customer). Threat actors are not described.	Not described in specific.	Categorizes the impacts in terms of security objectives, where FDIA impacts integrity, DoS impacts availability, MitM impacts confidentiality and integrity, and authentication and disaggregation attacks impact confidentiality.	Overarchingly the attacks are claimed to have the potential to disconnect electricity from consumers and cause significant failures in the SG. FDIA can cause corrupted measurements and disruptions in the network. DoS interrupts the traffic between the distributed devices and HES, affecting distribution of commands and data. MitM enables further attacks on the data and devices in the grid by spoofing, FDIA, disaggregation and authentication attacks. Authentication attacks enables spoofing and disaggregation attacks tries to profile customer energy consumption	Not described in specific	Not described in specific
[87], Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts, 2022	The communication systems and architecture of AMI (particularly the wireless channels) have inherent vulnerabilities, where an attacker can eavesdrop, inject false data and perform DoS. Considered one of the most vulnerable targets in the SG	The communication systems are susceptible to threats to data confidentiality, availability and integrity by FDI attacks to enable e.g., energy theft and privacy attacks. Considers Load Redistribution attacks as a severe attack in terms of FDI, which can create biased load estimates and cause instability. Threat actors are not described.	Describes the requirements for stealthy FDI attacks, where rendering power system unobservability, partial network information, a minimal set of attack vectors, attack specificity and requirements on influence of attack on security objectives and impact to AMI and SG is detailed.	Loss of data confidentiality, integrity and availability. The most common are attacks targeting the integrity of data.	The impact ranges from the secure operation and the reliability of the power grid (injections causing overload scenarios and working outside acceptable limits), energy theft (altering measurements) and privacy violations	Describes and calculates the probability of attack detection but does not describe the likelihood of a threat's capability of exploiting vulnerabilities.	Describes how FDI attacks are one of the major risks to inducing cascading failures (briefly describes the generation and transmission attacks in this regard).

[102], Attacks, vulnerabilities and security requirements in smart metering networks, 2015	Does not describe vulnerabilities in specific, beyond that the communication channels are highly dependent on publicly available communication technologies and standards, such as the internet and telecommunication infrastructure, both of which are considered unsecure. The devices taking part in the communication also have resource constraints, making most of the general-purpose IT countermeasures not applicable.	Describes the threats and attacks towards the communication channels as mostly internet-based in the form of eavesdropping, FDI, DoS, MitM, replay and repudiation attacks. Most attacks occur in the NAN-domain. Threat actors are not described.	Not described in specific	Depending on techniques used it can impact all security objectives	The impacts from the attacks ranges from manipulation of data integrity, potentially affecting the secure and reliable operation of the grid (FDI, MitM, replay), data leakage of customer data enabling profiling and traffic analysis (MitM, eavesdropping) to congesting the communication channel iot delay/block data and commands (DoS, MitM)	Not described in specific	Not described in specific

[90], Threat Modelling of AMI, 2013	The communication between HES – SM and SM – SM are vulnerable entry points for a set of threats identified using STRIDE and Attack Tree modelling techniques. The vulnerabilities to the identified threats depend on how authentication is implemented (is an attacker able to authenticate as a SM or HES?) and the presence of detection mechanisms, the security of the communication protocol and infrastructure, how integrity protection of messages are implemented, and the capacity of communication lines and entities in the network.	Based on stride, it identifies spoofing (HES and SM), data tampering and modification through tampering with the communication link between SM-HES and SM-SM, and repudiation where entities can deny receiving or sending messages. Further, information disclosure by leaking of configuration settings, keys, messages or SW/FW in the communication channel, and DoS by disabling or reducing the availability of communication between HES and SMs by malware causing DoS conditions or congesting the channel with requests. Threat actors are not described.	Does not provide specific attack descriptions	Data tampering and modification together with spoofing and repudiation impacts the integrity of data, DoS affects the availability of nodes and the communication channel, and information disclosure affects the confidentiality of data and information stored or sent through the communication channel and entities.	The spoofing of SM and HES may give the attacker the ability to send malicious commands to the network and increased access to information. Data tampering and modification can impact meter readings, cause unauthorized changes and malicious configuration settings and messages. Information leakage can breach confidentiality by revealing keys, messages, SW and consumption data. DoS affects the availability of data, commands and nodes in the network.	Explains how evaluations of likelihood are highly dependent on the individual systems and is thus not considered.	Discusses how threat models can be valuable input to risk assessments.
[109], Smart grid security: Attacks and defence techniques, 2022	The vulnerabilities in the communication channels are not specified, other than the inherent vulnerabilities in publicly available communication technology and standards	The communication architecture is vulnerable to DDoS, spoofing, MitM, impersonation, sniffing, message replay, FDIA (in combination with MitM, spoofing, impersonation and message replay), session key exposure attacks, and time synchronization attacks (on meter data). Threat actors are not described.	Provides attack examples for all threats in the communication channel. Refer to the article for detailed descriptions	The different threats described have the potential to affect all security objectives.	Not described in specific	Not described in specific	Not described in specific

[60], Smart Meter Modbus RS-485 Spoofing Attack Detection by LSTM Deep Learning Approach, 2022	Modbus RS 485 protocol used for physical layer communication in SMs does not support any encryption or authentication mechanisms.	Due to the lack of basic security mechanisms in the Modbus RS-485, an attacker can compromise SMs effortlessly by injecting critical attacks, i.e., DoS (jamming), spoofing, sniffing and FDIA, with low-cost intelligent attacking tools. Threat actors are not described.	Focuses on the spoofing attack, where the expected response from the server is altered. The attacker attaches to the communication channel used, reads the server ID and the requested register address of the client (SM) within the server. Then the attacker performs DoS by inserting jamming signal, forcing the server to not validate the request. Then the attacker responds as the server to the client, sending false data.	Does not describe the security objectives compromised in specific, but the attack and threats described will impact confidentiality, integrity and availability.	Not described in specific	Does not describe likelihood of the threats defined.	Not described in specific
[89], Communication Security for Smart Grid Distribution Networks, 2013	The article describes vulnerable entry points or attack vectors in HAN and NAN networks. In HANs, WLANs (based on 802.11, does not have a default authorization mechanism), Zigbee (based on LR-WPAN, vulnerable to jamming), and femtocells (link is IP-based) are considered. In NANs, WiMAX (radio links can be compromised, scrambling and jamming, insufficient frame freshness), LTE (dependent on publicly available communication channel, with accessible air-interface and base stations), and PLCs (considered shared media and no default security protocols are provided by PLC medium access control standards for access control) are considered.	The entry points are vulnerable to different threats: eavesdropping (WLAN, PLC), FDI (WLAN), MitM (WLAN, PLC, WiMAX), session hijacking (WLAN), replay (WLAN, WiMAX), DoS (WLAN, WiMAX, LTE) and traffic analysis (WLAN, WiMAX, LTE) attacks. Threat actors are not described.	WiMAX: DoS by radio frequency jamming and scrambling where an adversary injects interference while the system transmits management data. MitM by replaying certain messages towards the HAN, as there is a lack of message timeliness. LTE: DoS by jamming the radio frequencies used, traffic analysis by intercepting traffic over-the-air, and attacks on base station (eNB) and core network. PLC: Due to the shared networking media, external attackers can eavesdrop on exchanged data by a MitM attack between NAN and HAN communication.	Attacks on the communication technologies could breach the following security objectives - WLAN: Confidentiality (traffic analysis), availability (session hijacking, DoS), integrity (FDI). WiMAX: Availability (DoS), confidentiality (traffic analysis) LTE: Availability (DoS in air interface and attacks on core network and eNB), confidentiality (traffic analysis, attacks on core network and eNB, and user tracking)	Describes impacts briefly based on breach of all the different communication technologies. Refer to article for details.	Not described in specific	Not described in specific

[61], By-design vulnerabilities in the ANSI C12.22 protocol specification, 2015	The study analyzed the protocol specification iot discover design vulnerabilities in the ANSI C12.22 communication protocol, and not on specific implementations of the protocol. It discovered vulnerabilities in the Extended Protocol Specification for Electronic Metering (EPSEM) logon service, security service, read service and resolve service.	Performed attack experiments based on crafted attack messages in a simulated environment with the following threats: DoS (operator lockout, routing table poisoning), masquerading (operator lockout), FDI (routing table poisoning) and data theft (flawed password storage). This was done by manipulating EPSEM services by sending EPSEM service requests to devices on the communication channel. Threat actors are not described.	Operator lockout was performed as the EPSEM logon service request enables an attacker to masquerade as a valid user and creating a session without logging on, and thus preventing further logon requests, locking all others out. Password guessing can be conducted after operator lockout by issuing the EPSEM security service request and guessing passwords. The protocol also has a flawed password storage which can be read with the required permission issuing the EPSEM read service request to transfer the table over the network. Further, the EPSEM resolve service request enables routing table poisoning and buffer exhaustion. Poisoning can be conducted by a malicious node replying to broadcast messages and making itself a relay node, potentially controlling the communication and enabling modifications of messages. Buffer exhaustion can be conducted by a malicious node performing a large number of registrations with different ApTitles.	It does not categorize threats according to security objectives breached, however the threats will affect confidentiality, integrity and availability.	Not described in specific	Not described in specific	Not described in specific

[115], Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures), 2022	The widespread use of wireless technologies is seen as a major contribution of vulnerabilities in AMI and the SG communication infrastructure. The components in the network also have limited resources to incorporate sufficient security measures. The use of ML techniques for securing the networks against traditional threats also have inherent vulnerabilities in how they are trained and tested, making it possible for an attacker to misguide and falsify the decision-making system. In addition, ML techniques are costly in terms of resources and thus leading to the use of edge computing and a centralized server, to compensate for limited resources in network-devices. Further, this leads to large amounts of data sharing to train the algorithms, which can induce privacy challenges for the participating users and strain on the communication channels.	Analyzes both traditional threats inherited from wireless technologies and AML-based ones and categorizes them as either active or passive. The most prominent threats considering network vulnerabilities are as follows: Passive attacks: Eavesdropping and traffic analysis. Conventional active attacks: (D)DoS (jamming, puppet or blackhole attack), MitM (iot eavesdrop, FIDA and DoS), message replay. AML active attacks aim at misleading ML systems used in AMI and SG, e.g., for energy pricing, attack detection and load forecasting. They are classified as 1) poisoning attacks, where an attack attempts to falsify the ML algorithm during training by injecting wrong inputs or parameters, and 2) evasion attacks, where an attacker tries to mislead the ML algorithm in the testing phase to produce wrong decisions. Privacy threats in SG and AMI are defined in 3 classes: 1) personal information leaks, such as latency attack (location disclosure) eavesdropping, sniffing and traffic analysis, 2) identity theft by masquerading, spoofing or impersonation, and 3) social engineering attacks such as phishing. Threat actors are not described.	Provides attack examples for all threats in the communication channel. Refer to the article for detailed descriptions	Passive attacks threaten mainly the network and data confidentiality, whereas active attacks primarily impact the availability and integrity. Based on threats, confidentiality is affected by eavesdropping and traffic analysis, integrity is affected by MitM and FDI, whereas availability is impacted by (D)DoS. Privacy attacks impacts authentication, authorization and accountability services, where information leaks mainly target the authentication criteria, identity theft targets authorization and social engineering attacks targets accountability.	Eavesdropping and traffic analysis can reveal important system data or commands, and privacy information, which can be an important step for other attacks. Next, DoS attacks can reduce AMI performance and deny the sending or receiving of important information and commands. Further, FDI attacks can mislead the system and cause power theft, load reduction and delay or blocking of data. MitM attacks enable other attack-types such as FDI, DoS and eavesdropping, controlling communication and causing potentially devastating impacts on the system. Lastly, message replay of authorized messages can lead to incorrect energy pricing and forecasts for power generation. AML attacks can affect the state estimation (reducing FDI detection accuracy), load forecasting (reduce load forecasting accuracy)	Claims to describe the most probable cyber-threats to the SG, but does not give any description of likelihood	Not described in specific

					and energy theft detection ML algorithms		
[112], Threat Modelling of Wireless Attacks on Advanced Metering Infrastructure, 2019	The article utilizes STRIDE threat modelling to identify vulnerabilities and entry points within AMI and the communication channel. Based on the AMI-model used, it identifies the HES, master SM, slave SM, third party equipment, and maintenance personnel as entry points or interfaces vulnerable to wireless attacks.	Primarily concerned towards wireless communication threats, focusing only on DoS (traffic flooding, ARP spoofing, jamming), DDoS, FDI, MitM (using a rogue access point, ARP-, DNS- and MDNS-spoofing) and de-pseudonymization attacks. These types are claimed to be the most prevalent in AMI. The threats are mapped to STRIDE based on the entities being affected by the wireless attacks. In addition, DREAD modelling is used to conduct a risk analysis by ranking the risk of each threat into the categories of damage, reproducibility, exploitability, affected clients and discoverability. Each threat is given a value between 1-3 in each category and based on the sum of all of its categories, each threat is then rated as low, medium or high risk. Threat actors are not described.	Not described in specific	Threats are not classified in terms of security objective breached	The impacts of DoS and DDoS attacks are delayed or blocked data, commands or services in AMI. Further, FDI attacks aims at misleading state estimations in AMI, while de-pseudonymization attacks targets user privacy. MitM attacks enable eavesdropping, interception and FDI, controlling the communication between entities in the network.	Briefly describes how most attack occurrences on AMI are of wireless nature (e.g., DoS, FDI). However, does not further describe likelihood of attacks	Describes attack risk ratings using DREAD risk categories, to rate the attacks between low, medium and high-risk attacks. DoS, MitM, FDI and de-pseudonymization attacks are rated as medium risk, while DDoS is rated as high risk.

[114], Cyber-security in smart grid: Survey and challenges, 2018	The underlying communication infrastructure uses a variety of protocols for communication, such as ZigBee and Z-wave in HAN, and WiMAX and PLC in NAN, and WiMAX, cellular, DSL and satellite in WAN. The shared nature of the communication channels, inherent vulnerabilities within the protocols and vulnerabilities in SW or OS creates entry points for potential threats.	Classifies threats and attacks according to the attack cycle with reconnaissance, scanning, exploitation and maintaining access. At each step, different techniques are used to compromise the security criteria to reach their intended target. Reconnaissance includes traffic analysis and social engineering. Scanning includes IP-, port-, service- and vulnerability scanning. Exploitation includes malware, DoS (SYN, buffer overflow, teardrop, smurf, puppet, TS attacks), MitM (intercept and/or alter data, eavesdropping), replay (intercept authentication messages), jamming (type of DoS, exhausting bandwidth), popping the HMI (installing a remote shell, exploiting vulnerabilities in SW or OS), masquerade, integrity violation (FDI), and privacy attacks. Maintaining access includes backdoor access through malware to obtain permanent access to the target. Threat actors are not described.	Reconnaissance threats seeks to obtain credentials and to map out the network. Scanning threats is used to discover the network and its entities with addresses. Exploitation threats seeks to exploit the vulnerabilities in the AMI and SG to obtain control over entity and/or data at rest or in motion. Maintaining access seeks to maintain permanent access to entities and/or data iot launch other attacks.	Describes the how different attacks affect the security objectives, which are prioritized as availability, integrity, accountability and confidentiality. Reconnaissance and scanning threats impact mainly the confidentiality of data and network topology. Exploitation impacts different aspects: malware (can breach all security objectives, depending on type). DoS and jamming impacts availability. MitM (depending on type) will affect confidentiality, integrity and availability. Replay impacts authentication. Popping the HMI and masquerade (based on objective and motivation) can affect confidentiality, integrity, availability and accountability.	Reconnaissance and scanning do not immediately affect the performance and security of AMI but is used as steps prior to exploitation to gain knowledge about the target. Exploitation can affect the security and reliability of the AMI and the SG, with severity depending on the type of attack. Similarly, maintaining access is depending on the type of attacks to be performed after gaining a foothold within the system.	Describes the combination of likelihood of the attack being performed and impact (severity of attacks based on the prioritized security objectives) in a matrix. Likelihood is explained as a combination of attack complexity and the exposure of the vulnerability/attack target, and is a qualitative unit set to low, medium, high for each threat. Similarly, the impact is a qualitative unit set to low, medium, or high	Produces a matrix of likelihood and severity of attacks (impact on security objectives), similar to a risk matrix.

[88], Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure, 2015	The article analyzes the vulnerabilities in the communication network of AMI by DDoS attacks, using the network simulation tool NeSSi. The overarching initial vulnerabilities in AMI are described as the massive deployment of SMs, the IT-nature of the components and the communication channels in AMI, and the data-intensive nature of AMI. The ubiquitous presences make them easy targets to reach, the IT-nature of the systems makes them vulnerable to regular IT-threats, while the data-intensive nature makes them easy target to disrupt through the communication channels. DDoS attacks is partly a resource competition, where an attacker seeks to overcome the defender's ability to counter DDoS, and the ability to exploit vulnerabilities or faults in the network protocols or applications in the target network. In this article, DDoS exploits the assumed infrastructure design focusing on moving packets from destination to host in an end-to-end paradigm, with the intermediate network conducting simple packet forwarding.	DDoS exploits the end-to-end paradigm in the infrastructure design, where there is no policing in between the source or destination, and the packets are forwarded by the intermediate network. The DDoS threat is categorized as either flooding or vulnerability attacks, where flooding consists of SYN, UDP and ICMP flooding, exploiting vulnerabilities in the protocols. Vulnerability attacks are performed with malicious packets that exploit vulnerabilities in the protocols or application faults in the target devices iot to exhaust its resources. Threat actors are not described in specific, but mentions insiders, industrial espionage and terrorists.	The attack performed in the study utilizes a DDoS UDP flooding attack performed by a bot network on the DSO server, which is responsible for collection of metering data from SMs and is connected to internet for billing purposes. The attack brought down the server, forcing it to drop all incoming packets. Due to the prerequisite in the simulation that the energy network and power production are purely dependent on the usage data from AMI to plan production, the energy network and power production are also brought down.	DoS attacks mainly targets the availability of data, information and entities in the AMI system.	The impact on SG and the security of supply of energy in this simulation is significant, as the power production is brought down. In AMI, it causes unavailability of data, and forces the SM and DSO server (assumed MDMS) to drop packets and disconnect from the network. The simulated environment is therefore highly vulnerable to DDoS attacks, however the network topology and degree of connectivity at the DSO MDMS is an unlikely scenario in a Norwegian context.	Not described in specific	Not described in specific

[116], 5G as an Enabler for Secure IoT in the Smart Grid: Invited Paper, 2019	The article briefly explains two significant vulnerabilities inherited from 5G when used as a communication channel in AMI and SG. The first is the inherent properties of wireless communication, which makes 5G vulnerable for attacks exploiting the access to the wireless communication. The second is the Mobile Edge Computing Host (MECH) and its related interfaces to the RAN and SG control center, which are exposed to third party applications hosted in MECH and there is a risk of user plane attacks within.	The article utilizes a threat model which categorizes the threats into two types: local wireless attacks and remote attacks targeting 5G or SG. In local wireless attacks the adversary can intercept or sniff 5G wireless communication, with both active and passive attacks, where the goal is to intercept or modify 5G traffic, or to block 5G communication services. In remote attacks an adversary targets SG infrastructure elements including 5G network. The vulnerabilities described can be exploited by fake base station attacks (e.g IMSI catching) to intercept signaling and geolocate devices, and to create DoS conditions (by accessing the wireless channel). Attacks can also be performed through user plane in MECH and 3rd party API to exposed core network functions. Threat actors are not described.	Not described in specific.	The threats and vulnerabilities are not categorized in terms of security objectives they impact.	Not described in specific	Not described in specific	Not described in specific

[111], Authentication for Smart Grid AMI Systems: Threat Models, Solutions, and Challenges, 2019	Describes vulnerable and insecure authentication mechanisms, where impacts are dependent on the authentication scheme used and attacks performed. A general concern is the resource constrained environment of the distributed entities (SMs and DCs), which limits what and how the authentication scheme is implemented, forcing through trade-offs between providing authentication and the attacks it can protect against.	The most prevalent attacks on authentication schemes used are MitM (interception, FDI, replay), impersonation, unknown key share, insider and DoS attack. Threat actors are not described.	MitM can be performed by an adversary intercepting data and information (e.g., consumption patterns from SMs) from network communication in AMI, modifies or replays the data, and then forwards the data (e.g., towards HES/MDMS). Further, impersonation attacks concern identity theft, e.g., in the supply chain of AMI to gain access to SM data. Unknown key share attack is based on creating different perception of how the communication key is shared between entities.	The attacks seek to affect the authentication objective; however, the different attacks will also affect other security objectives depending on the attacker's motive, intent and resources (e.g., impersonation, unknown key share and insider attacks). MitM and replay attacks can affect the confidentiality and integrity of data, and privacy of consumer information. DoS (flooding or vulnerability attack) affects the availability objective	Not described in specific, but authentication attacks have the potential to affect all security objectives and thus cause significant impacts in AMI in terms of SG and AMI stability by affecting consumption data, event information, commands and real-time requirements in the system. Further, it can have an economic impact on both consumers and SG operators by impacting billing and price signaling	Not described in specific	Not described in specific
[113], An information security model for an IoT-enabled Smart Grid in the Saudi energy sector, 2022.	As a part of developing a security model, the article identifies the different access points SG, where the SM and the AMI are identified as two of the seven access points most likely to be exploited in attacks. One key vulnerability is the use of IP-based communication networks, making them susceptible to a wide array of threats.	The article conducts threat modelling using STRIDE, where the internet-based threats are grouped according to their STRIDE classification. The most common threats are identified through literature search and then mapped to the different access points. The mapping is based on the functionality, operations and information systems present at the points, and how the different threats could affect them. SM can be affected by spoofing attacks, eavesdropping/traffic analysis/MitM, replay attack, data tampering, DoS and malware injection. The AMI communication infrastructure has similar threats, in addition SQL injection and FDI. Threat actors are not described.	The attacks are briefly explained in the article, but are in general based on IP-connectivity to devices in AMI (SM, DC, and HES/MDMS)	The threats are categorized according to the security objective they impact: 1) Confidentiality (eavesdropping/traffic analysis/MitM), 2) Integrity (replay, data tampering, malware injection, SQL injection, FDI), 3) Availability (DoS, malware injection), 4) Authentication and authorization (spoofing), 5) Non-repudiation (FDI)	Not described in specific.	Not described in specific.	Not described in specific.

[85], Security of Power Line Communication systems: Issues, limitations and existing solutions, 2021	The vulnerabilities in large is caused by the nature of PLC being a shared networking medium, making it vulnerable to internal and external threats. The threats further exploit the vulnerabilities within the PLC technology used, where networking, signal interception, interruption and injection issues can arise based on the type and standard of PLC in use.	The article explores the security and privacy issues arising from misconfiguration, malicious code/data injection, wiretapping and data interception. The threat sources are considered as insiders, criminals, nation state actors and terrorists. The main threats to PLC systems are categorized as malware (trojans, virus, worms, logic bombs, spyware and ransomware) and malicious applications (buffer overflow, zero-day exploit and web-interface exploit). The threats can manifest as attacks exploiting different security issues in PLC: 1) Signal interception issues caused by eavesdropping, wiretapping or sniffing, 2) Signal interruption caused by MitM, replay, wormhole, sinkhole, blackhole, Sybil and DDoS attacks, 3) Signal injection issues caused by MitM or malware used to intercept packets and modify the data by injecting malicious payloads or false data, 4) Authentication issues caused by insider attacks, and 4) Network issues caused by vulnerabilities in the type and standard of PLC in use. The article also considers specific attacks towards network membership keys (NMK) in PLCs as interception, sniffing, brute force/dictionary attack and identity forgery (MitM). Threat sources describes some threat actors, such as malicious insiders and spies (with motives to do cyber-crime, cyber-terrorism, cyber-warfare, hacktivism and industrial espionage), nation states (cyber military operations to affect national critical infrastructure), criminal groups (hacktivism or financial gain),	Not described in detail.	The security issues and accompanying threats and attacks impacts different security objectives: Confidentiality is impacted by wiretapping, eavesdropping and sniffing. Integrity is impacted by MitM and malware. Availability is impacted by signal interruption attacks. Authentication is impacted by insider threats	Not described in specific.	Not described in specific.	Briefly discusses the importance of risk evaluation of likelihood and impact of cyberattacks in the design phase of PLC security solutions. However, does not consider risk in terms of likelihood and impact of attacks.

		terrorists and regular disgruntled insiders (motivated by lust, greed or dissatisfaction).					
[99], Exploration of Smart Grid Device Cybersecurity Vulnerability Using Shodan, 2020	The article explores how the use of publicly available communication channels and the connection to the internet, combined with poor security implementation makes AMI devices vulnerable to open-source mapping using the Shodan tool. Open-source mapping is an essential part of the reconnaissance phase for preparation for attacks in the attack cycle. Both SG and AMI devices and DERs may have connections making them exposed on the internet, and how their security is configured, such as the ability to access the devices and read status information or affect device configurations remotely, make them potentially vulnerable. Specific vulnerabilities are lack of password protection or the use of default usernames and passwords, and the ability to conduct uploads of own FW/SW	The threats are based on the ability to read device status or change configuration settings remotely. Passive attacks can be performed in the reconnaissance phase by reading the status information, obtaining network information and addresses, and the maintenance status. Active attacks can be performed in the exploitation phase by changing configuration on devices, uploading FW/SW, create DoS conditions and inject false data (FDI). Threat actors are not described.	Using the Shodan tool and a set of specific search queries based on devices to target, will find exposed devices. Based on their security configuration, an attacker can read status information or change configuration settings, depending on its intention and motivation, as part of a reconnaissance or exploitation.	The impact on security objectives depends on the motivation and intentions of the attacker, but with the ability to read status and change configuration settings, it can affect confidentiality (reading status information and data from the device), integrity (injection of false data and FW/SW) and availability (bricking the device with erroneous FW/SW, or perform operator lock-out by changing password)	Not described in specific	Does not describe likelihood of the threats from Shodan, however it is a database of devices that is continuously updated, and is available to everyone	Not described in specific.

[86], False data injection threats in active distribution systems: A comprehensive survey, 2022	The article highlights the publicly available and shared communication channels and the 2-way communication as prominent vulnerabilities, exposing data to FDI threats. In addition, the complexity of AMI and weaknesses within protocols such as ZigBee and ModBus adds to increasing the attack surfaces and overall vulnerability.	The article classifies FDI threats according to their attack targets, where AMI in terms of communication networks, SMs and distribution control center are defined as targets. In the communication networks of AMI, the data packets between SMs and distribution control center, and the communication message integrity are described as targets. It describes the threat targeting data packets as puppet DoS attacks to exhaust the bandwidth and resources of a node. The threat targeting the integrity of communication messages is described as MitM short-term FDI. Both data packets and information messages include price signaling and messages in AMI, which when corrupted or delayed can cause mismatch between energy supply and demand. Threat actors are not described.	The puppet DoS attack is conducted by flooding a puppet node in the network with malicious route request packets to exhaust both the bandwidth of the network and the resources at the node, ultimately reducing the packet delivery rate drastically. The communication message integrity attack is not described in specific	FDI attacks generally target the integrity aspect of SM, AMI and SG.	By degrading the integrity of data in SM and AMI, it can impact the reliability and stability of the SG, by affecting the operational decisions in the system.	Not described in specific.	Not described in specific.

Identified security challenges at system level

References	Vulnerabilities	Threats	Attack descriptions	Impact towards CIAPI3A objectives	Impact towards AMI	Likelihood description	Risk evaluation or description
[105], Advanced metering infrastructures: security risks and mitigation, 2020	The exposure of distribution control center and HES/MDMS to the internet or other networks	Worm and viruses that can propagate from infected devices to other components in AMI. Threat actors are generally described as malicious customers, insiders, criminal organizations, terrorists, competing organizations and nation states. The motivation is not discussed.	Injecting computer worms or viruses by exploiting the connections the utility center has to other networks.	Confidentiality, integrity, availability	Widespread denial-of-power	Does not describe likelihood, of threats, but describes the use of attack graphs to identify attack paths that are most likely to succeed.	Defines the main cyber risks to AMI security to be energy theft (theft of service), data theft (includes FDIA, interception and eavesdropping), AMI communication and networks, and APTs
[100], Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure, 2015	The HES and MDMS resides within the DSO or AMI operator's premises and is such protected by corporate cyber security policies. However, this means that, as an enterprise computing platform, it may be vulnerable to regular internet-based threats due to the interconnections within the corporate WAN.	Does not describe specific threats to the corporate WAN and HES/MDMS, other than internet-based threats. Threat actors are not specifically described, but the general motivation for attacks is seen as disruption of national critical infrastructure, skill testing, industrial espionage and as a launching point for other attacks.	Does not describe attacks specifically	Does not classify the threats regarding security objective, however the threats describe will affect integrity, availability, confidentiality or privacy of data and devices in AMI.	The potential effects are disabling of power delivery systems and breach of privacy. Attacks on the integrity of data in AMI can result in loss of SA and grid control.	Not described in specific	Not described in specific, but understanding the attack surface is a first step in obtaining cyber security and understanding the concept of risk.

[42], Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS, 2012	Describes how the system level or central system can be vulnerable due to its interconnections (internet) and regular non-targeted and targeted ICT-related threats. Further, vulnerabilities in SW can be exploited due to lack of patching, e.g, becoming bots. .	Describes targeted threats towards the central system or frontend (HES and MDMS). The general description of threats and attacks concerns incidents with manipulation of data, manipulation of breaker functionality and theft of data (encryption key). Examples of specific threats are DoS towards central system and injection of malware at the management system exploiting vulnerabilities in SW. Also highlight non-targeted threats to central system as regular ICT threats (malware, keylogging, profiling, eavesdropping and social engineering) Threat actors described are external and internal	Describes five different scenarios, and the potential incidents causing them: 1) Large number of SMs out of operation (breaker not engaged) caused by malware accessing HW in communication channel. 2) End-user manipulation of consumption data causing erroneous data for billing. 3) Insider manipulation of functionality and data, injection of malware, extraction of data. 4) Targeted attack on a specific geographical area by remote attacks, insider or a combination. 5) 3rd party access providing additional vectors for attack Also describes how compound attacks can be used to increase the effect or in tandem to hide activity	Does not classify threats according to security objectives. But the threats exemplified can affect confidentiality, integrity, availability and/or privacy	Lack of measurement data or producing corrupted data affecting billing, estimation of load for planning and causing instability in operation of grid. Triggering breaker function causing denial of power for a larger group of end-users. Theft of data and encryption keys can lead to manipulation of measurement data affecting the operation of the grid or functionalities (breaker)	Likelihood for targeted attacks is described as combination of the consequence in terms of number of affected units and the complexity of the attack. The likelihood is based on a 5-point Likert-scale, where targeted attacks are default set to likely (3), as targeted attacks will require specialized competence and will target several end-users due to utility.	Conducts risk assessment of a generic implementation in a Norwegian context, producing a risk matrix for selected incidents.

[43], Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision, 2022	Considers the vulnerability of poor access control and security policy at the DSO and where the HES and MDMS resides. Another vulnerability is the use of IP-based systems at the server-side, making them vulnerable to regular IT-threats. Coupled with the interconnectedness in the corporate WAN, significantly expands the vulnerable vectors an attacker can use.	A poorly implemented or insufficient security configuration at the HES/MDMS can enable an internal attacker (insider) to conduct data manipulation at the server side. This is also possible by a remote attacker due to the interconnections in the corporate WAN, making it susceptible to regular internet-threats. Threat actors are not described.	Not described in specific	The modification of applications, data or commands running in the AMI affects the integrity of the systems, whereas attacks compromising the customer data affects both confidentiality and integrity of the data. Attacks tampering with FW or SW is considered to affect confidentiality, integrity and availability	The impact from manipulation of data, SW and control systems in HES and MDMS can potentially affect the AMI system, by controlling the commands sent to the distributed elements. Instability of the grid or widespread denial of power are some scenarios.	Not described in specific	Discusses how the increasing numbers of IoT devices (SM and DCs) are increasing the risk. Also underlines the importance of risk assessments to identify vulnerabilities and threats, iot determine if additional countermeasures are needed. However, it does not conduct a risk evaluation based on the described vulnerabilities and threats
[101], Review of Cyber-Physical Attacks and Counter Defence Mechanisms for Advanced Metering Infrastructure in Smart Grid, 2018	The HES and MDMS resides within the DSO or AMI operator's premises and are protected by corporate cyber security policies. However, this means that, as an enterprise computing platform, it may be vulnerable to regular internet-based threats due to the interconnections within the corporate WAN.	Does not describe specific threats to the corporate WAN and HES/MDMS, other than internet-based threats exploiting the interconnected nature of the corporate enterprise WAN. Threat actors are not described.	Does not describe attacks specifically	The internet-based threats and attacks are categorized to impact confidentiality; however, it is deemed to have the potential to affect all security objectives based on the type of threat or attack	The impact from manipulation of data, SW and control systems in HES and MDMS can potentially affect the AMI system, by controlling the commands sent to the distributed elements. Instability of the grid or widespread denial of power are some scenarios.	Not described in specific	Not described in specific

[117], Analysis of the impact of data granularity on privacy for the smart grid, 2013	The article describes how the level of data granularity in AMI can affect the privacy of end-users, and how it can be used to identify the individual user. The vulnerability lies with the increased volumes of data communicated within SG and AMI, its high granularity and detail, and the timespan of data stored at the DSO, making the data susceptible to attacks aiming at inferring privacy-related information from the data.	The threat lies in an attacker's ability to identify individual customers when given a large dataset of consumption traces from SMs. Threat actors are not described.	By using both low-frequency SM datasets (used for billing) and high frequency datasets (used for grid operations) and matching the datasets with each other, taking in to account the granularity of the data and the timespan of it, it is evident that higher granularity and longer timespans makes it easier to re-identify the individual customer.	(Confidentiality), Privacy	The impact resides with the end-user of AMI and SG, as their privacy is breached, potentially impacting the individual and their trust in the system.	To be able to reason for the attacker's capabilities and possibilities of success in de-anonymizing the end-users, the article develops a probabilistic framework.	Not described in specific.
[86], False data injection threats in active distribution systems: A comprehensive survey, 2022	The incorporation of DERs and transition to sustainable energy sources introduced Distributed System State Estimation (DSSE), which estimates variables in the distribution systems in real-time. This induced vulnerabilities in the state estimation from the CVR, which is used to optimize the distribution system voltages without compromising quality.	The article classifies FDI threats according to their attack targets, where AMI in terms of communication channels, SMs and distribution control center are defined as targets. At the distribution control center, a DSSE is one of the basic functions, which can be affected by FDI and a load redistribution attack on SM measurement data. Threat actors are not described.	In an unbalanced 3-phase distribution network with DERs, a load redistribution attack on a closed-loop CVR can be performed by using MILP to inject malicious SM measurement data into the communication, affecting CVR and its proposed solutions.	FDI attacks generally target the integrity aspect of SM, AMI and SG.	By degrading the integrity of data in SM and AMI, it can impact the reliability and stability of the SG, by affecting the operational decisions in the system. In this case, the attack affects the CVR and the On-Load Tap Changer (OLTC), causing incorrect CVR solutions. This led to increased feeder voltage profile and the total 3-phase active power flow at the substation, in addition to voltage violations in some of the nodes in the grid.	Not described in specific.	Not described in specific.

[118], Survey in smart grid and smart home security: Issues, challenges and countermeasures, 2014	The article explores how vulnerabilities at the management level in HES can impact the system as a whole. The main vulnerabilities described is weak platform configuration (poorly defined policies and cyber hygiene), the availability of open information regarding the system and vulnerabilities in SW.	The article describes scenarios where HES is the main target, where the goal is to obtain information (reconnaissance) or access into it. The threats described are categorized according to intent of attackers: 1) Steal data (Open-source intelligence, malware, insiders, weak platform config, and SW flaws) 2) Gain control of server (Open-source intelligence, weak platform config, SW flaws, malware, message fabrication, replay) 3) Take down server (Eavesdropping, traffic analysis, MitM, message modification, replay, device impersonation, DoS) 4) Attacks against measurements (FDI and malware) Threat actors are not described.	Steal data can be done by accessing public information or use open-source tools to scan networks. This can also be done by insiders, exploiting poor cyber hygiene or policies, or using social engineering. The information obtained can be used for further attacks, such as malware or DoS, taking control of or taking down the server. Attacks against measurements are considered one of the most impactful, as FDI attacks here targets and manipulate measurements from SMs heading for the HES and state estimation.	Attacks stealing data from distribution servers and controlling the servers can affect confidentiality, integrity, availability, authorization and authenticity. In addition, attacks aiming at control will also seek to impact the ability for non-repudiation. Attacks aimed at taking down the server will impact confidentiality, integrity, availability, authentication and authorization. Attacks against measurements will impact integrity and availability.	Attacks stealing data will enable future, more targeted and impactful attacks on AMI and SG. And with sufficient information and access to the server, malware could modify or delete files (e.g., Load Shedding (LS) prioritization), enable key logging, engage breaker functionality at SM, threatening system availability and reliability. The impacts from FDI at measurements could impact the state estimation of the grid, forcing HES to take erroneous decisions, such as engaging LS or Demand Response (DR) at wrong times.	Not described in specific.	Not described in specific.

Appendix E - Tabulation of comparison SLR and SSI

Identified vulnerabilities

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Vulnerabilities	HW	**DV1.1**	Physical	The physical access to HW and interfaces makes them vulnerable for physical and logical tampering	**IV1.1**	Physical	The physical access to HW and interfaces makes them vulnerable for physical tampering and access to interfaces
		DV1.2	HW design	Resource constrained HW with limited ability to handle security controls and/or handle attacks	**IV1.2.1**	HW design	Resource constrained HW with limited ability to handle security controls and updates (updateability)
		Not present			**IV1.2.2**		Technical lifespan can be outpaced by ICT development
	Communication	**DV2.1.1**	Technology and protocol design	The technology used may have inherent vulnerabilities in its protocols or specifications	**Not present**		
		DV2.1.2		Limited bandwidth	**IV2.1.1**	Technology	Limited bandwidth for data and updates
		Not present			**IV2.1.2**		Technical lifespan can be outpaced by ICT development
		DV2.2	Medium	The public access to the medium (wired or wireless) makes it susceptible to attacks	**Not present**		
	System level	**DV3.1**	SW/FW	SW/FW may have faults/vulnerabilities and needs to mature in design, testing and operation	**IV3.1**	SW/FW	SW/FW may have faults/vulnerabilities and needs to mature in design, testing and operation
		DV3.2	Platform	Interconnections between systems from MDMS and to the corporate WAN	**IV3.2**	Platform	Interconnections between systems from MDMS and to the corporate WAN
		DV3.3	Technology	IP-based communication between networks	**IV3.3**	Technology	IP-based communication between networks
	Organizational	**Not present**			**IV4.1.1**	Complexity	Technological and cognitive complexity challenges the ability for a comprehensive overview of vulnerabilities, threats and consequences

		DV4.1	Management	Policy, procedures, and training insufficient or lacking (weak security policy and poor cyber hygiene)	**IV4.1.2**	Management	Inadequate knowledge and training in information security creates lack of experienced personnel
		Not present			**IV4.2**	Service providers	Dependence on third parties (outsourcing of competence and data value chain)
		DV4.2	Complex supply chain	High vendor diversity and a long supply chain increases complexity and potential vectors	**IV4.3**	Supply chain and market	Small market with few vendors entails low redundancy of service providers and HW (supply chain)

Identified threats

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Threats	HW	**DT1.1**	Physical	Physical tampering and modification	**IT1.1**	Physical	Physical tampering and modification in operation and supply chain
		DT1.2	HW design	Attack different layers in the protocol stack, often by physical access to device	**Not present**		
		DT1.3	Data and information	False data injects, interception and modification of data	**IT1.2.1**	Data and information	False data injects, interception and modification of data in transit
		DT1.4		Extraction of data and information	**IT1.2.3**		Extraction of data and information
		DT1.5		Delay or deny availability of data	**IT1.2.4**		Deny or delay availability of data (DoS)
		Not present			**IT1.2.2**		Disaggregation and de-pseudonymization of data
		DT1.6	SW/FW	Extraction of SW or FW	**IT1.3.1**	SW/FW	Extraction of SW or FW
		DT1.7		Manipulation and tampering in supply chain	**IT1.3.2**		Manipulation and tampering in supply chain
		DT1.8	Signaling and commands	Delay or deny signaling and/or commands	**Not present**		
	Communication	**DT2.1**	Technology	Technology-specific attack (Attack different layers in the protocol stack)	**Not present**		
		DT2.2	Medium	Medium-specific attack (wired or wireless)	**Not present**		
		DT2.3.1	Signaling and commands	Interception and modification of commands in transit	**IT2.1.1**	Signaling and commands	Interception and modification of commands in transit
		DT2.3.2		Delay or deny signaling and/or commands	**IT2.1.2**		Delay or deny signaling and/or commands
		DT2.4.1	Data and information	False data injects, interception and modification of data in transit	**IT2.2.2**	Data and information	False data injects, interception and modification of data in transit

		DT2.4.2		Disaggregation and de-pseudonymization of data	**IT2.2.3**		Traffic analysis and profiling by disaggregation and de-pseudonymization of data
		DT2.4.3		Extraction of data and information	**IT2.2.4**		Extraction of data and information for traffic analysis and profiling
		DT2.4.4		Deny or delay availability of data	**IT2.2.5**		Deny or delay availability of data (DoS)
		DT2.4.5	SW/FW	Extraction of SW or FW	**IT2.3**	SW/FW	Extraction of SW or FW
	System level	**DT3.1.1**	SW/FW	Malware or malicious code in servers	**IT3.3.2**	SW/FW	Manipulation and tampering in supply chain
		DT3.1.2		Extraction of SW or FW	**IT3.3.1**		Extraction of SW or FW
		DT3.2.1	Data and information	False data injects, interception and modification of data in servers	**IT3.2.1**	Data and information	False data injects, interception and modification of data in servers
		DT3.2.2		Disaggregation and de-pseudonymization of data	**IT3.2.2**		Profiling by disaggregation and de-pseudonymization of data
		DT3.2.3		Extraction of data and information	**IT3.2.3**		Reconnaissance: Extraction of data and information on infrastructure
		DT3.3.1	Signaling and commands	Modification of commands	**IT3.1.1**	Signaling and commands	Modification of commands
		DT3.3.2		Delay or deny signaling and/or commands	**IT3.1.2**		Delay or deny signaling and/or commands
		DT3.4	Targeted	Targeted and compound threats derived specifically to affect AMI through HES	**IT3.4**	Targeted	Tailored attacks to enable traversal into HES and MDMS
	Threat actor	**DT4.1**	Local	Insider or use of open-source tools for social engineering	**IT4.1**	Local	Insider or use of open-source tools for social engineering
		Not present			**IT4.2**	Nation state actor	Competence and resources to target AMI by cyber, insider or open-source tools

Identified impacts and consequences

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Impact and consequences	HW	**DI1.1**	Physical	Rendering HW inoperable (e.g., bricking of device)	**II1.1**	Physical	Rendering HW inoperable (e.g., bricking of device)
		DI1.2.1	Integrity	Theft of power	**II1.2.1**	Integrity	Local theft of power (false consumption data)
		DI1.2.2		Denial of power	**II1.2.2**		Local denial of power
		DI1.3	Data and information	Theft of data	**II1.3**	Confidentiality	Local theft of data for profiling and extraction of PII
		DI1.4	Availability of service	Hindering or blocking commands (DoS) locally	**II1.4**	Availability of service	Hindering or blocking communications (DoS)
	Communication	**DI2.1**	Power	Theft of power	**II2.1.1**	Integrity	Local theft of power (false consumption data)
		DI2.2	Data	Theft of data	**II2.2**	Confidentiality	Local theft of data for profiling and extraction of PII
		DI2.3.1	Availability of service	Denial of power	**II2.1.2**	Integrity	Local denial of power
		DI2.3.2		Hindering or blocking communications (DoS)	**II2.3**	Availability of service	Hindering or blocking communications (DoS)
		DI2.4	Operation	Unreliable and insecure operation of the grid or devices	**Not present**		
		DI2.5	Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))	**Not present**		
	System level (AMI and SG)	**DI3.2**	Data	Theft of data	**II3.2**	Confidentiality	Theft of data for profiling and extraction of PII
		DI3.3	Availability of service	Denial of power	**II3.1**	Availability of service	Breaker-functionality (denial of power)
		DI3.4	Operation	Unreliable and insecure operation of the grid or devices	**II3.3**	Operation	Unreliable and insecure operation of the grid or devices
		DI3.5	Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))	**II3.4**	Financial	Financial loss incurred by breach (e.g., theft of power, loss of reputation or fines due to privacy breach (GDPR))

Identified likelihood

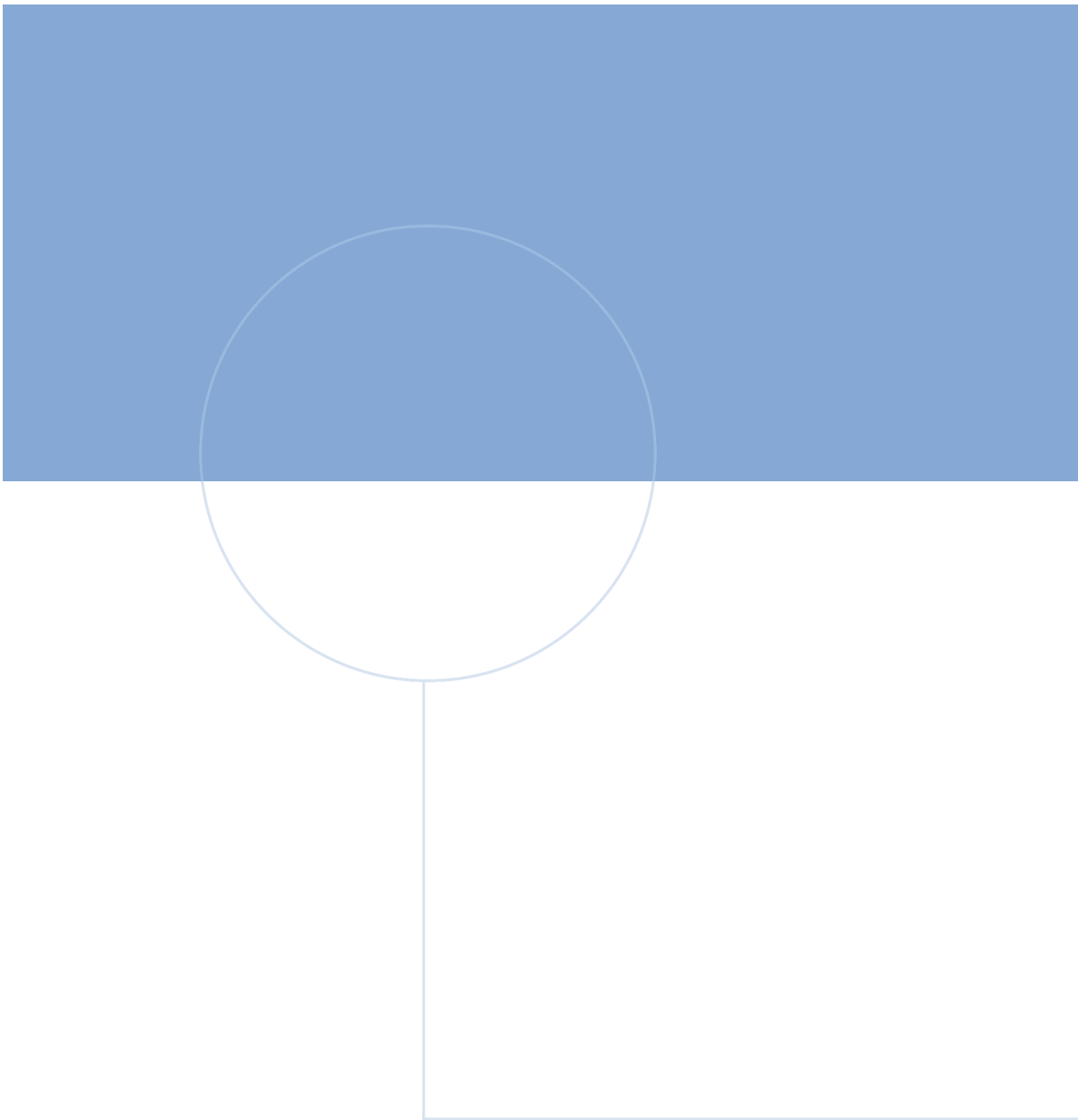
		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Likelihood	HW	**DL1.1**	Accessibility	The access to the medium can increase attempts	**IL1.1**	Accessibility	The access to the medium can increase attempts
		DL1.2.1	Quantitative data	Lack of statistical and historical data	**IL1.2**	Quantitative data	Lack of statistical and historical data
		DL1.2.2		System and implementation dependent	**Not present**		
	Communication	**DL2.1**	Accessibility	The access to the medium can increase attempts	**IL2.1**	Accessibility	The accessibility of HW can increase attempts
		DL2.2.1	Quantitative data	Lack of statistical and historical data	**IL2.2**	Quantitative data	Lack of statistical and historical data
		DL2.2.2		System and implementation dependent	**Not present**		
	System level	**DL3.1**	IP-platform	IT-nature of systems and IP-based communication increases likelihood	**IL3.1**	IP-platform	IT-nature of systems and IP-based communication increases likelihood
		DL3.2	Interconnections	The interconnections between systems and to internet at top-level increases likelihood	**IL3.2**	Interconnections	The interconnections between systems and to internet at top-level increases likelihood
		DL3.3.1	Utility	Higher pay-off for attacker increases likelihood for attempts	**IL3.3.1**	Utility	Higher pay-off for attacker may increase likelihood for attempts
		DL3.3.2		Higher utility entail higher security (reduces likelihood for successful attacks)	**IL3.3.2**		Higher utility entail higher security (reduces likelihood for successful attacks)
		DL3.4.1	Quantitative data	Lack of statistical and historical data	**IL3.4**	Quantitative data	Lack of statistical and historical data
		DL3.4.2		System and implementation dependent	**Not present**		
	General	**DL4.1**	Complexity	Attack complexity in terms of knowledge and resources may affect likelihood	**IL4.1.1**	Complexity	Attack complexity in terms of knowledge and resources may affect likelihood for attempts

		Not present	**IL4.1.2**		The complexity of the system and uncertainties in capabilities of threat actors make predictions on likelihood challenging
		Limited descriptions	**IL4.1.3**	Utility	Low likelihood perception at all levels

Identified risks

		Deductive codes SLR			Inductive codes SSI		
Category	**Name**	**Code**	**Detail**	**Definitions**	**Code**	**Detail**	**Definitions**
Risk	HW	**DR1.1.1**	Supply chain	Increased risk of HW tampering	**IR1.2.2**	Supply chain	Long and complex supply chain increases attack vectors and risk
		DR1.1.2		Vendor diversity increases complexity and risk	**IR1.2.1**		Low vendor diversity increases risk
		DR1.2	Ubiquitous	Increased presence and widespread use will increase risk (will be scrutinized by both malicious and non-malicious actors)	**IR1.3**	Ubiquitous	Increased presence and widespread use will increase risk for attempts (will be scrutinized by both malicious and non-malicious actors)
		Not present			**IR1.4**	Ease of access to HW	Lack of safe disposal
		Limited descriptions			**IR1.1**	Utility	Low risk perception (low likelihood and consequence)
	Communication	**Limited descriptions**			**IR2.1**	Utility	Low risk perception (low likelihood and consequence)
		DR2.1	Utility	Increased data and information can increase utility and overall risk for breach of availability and confidentiality	**Not present**		
		DR2.2	Ubiquitous	Increased presence and widespread use will increase risk (will be scrutinized by both malicious and non-malicious actors)	**IR2.2**	Ubiquitous	Increased presence and widespread use will increase risk for attempts (will be scrutinized by both malicious and non-malicious actors)
	System level	**DR3.1**	Utility	Aggregated data and information can increase utility and overall risk for breach of availability and confidentiality	**IR3.1.1**	Utility	Aggregated data and information can increase utility and overall risk for breach of integrity and confidentiality
					IR3.2	Confidentiality	Profiling and big data analytics from aggregated data
		Limited descriptions			**IR3.1.2**	Utility	Low risk perception (high consequence but low likelihood)
					IR3.6	Breaker functionality	Breach of integrity and further functionality increase severity in terms of physical impacts to end-users

		DR3.2	Consequence	Breach at system level will increase severity and reach of consequences	**IR3.5**	Consequence	Breach at system level will increase severity and reach of consequences
		Not present			**IR3.3**	Integrity of data	Erroneous operation of grid and settlements
		Not present			**IR3.4**	Availability	Lack of access to data may disturb market operations and settlements
	Organizational	**Not present**			**IR4.1**	Risk assessments	Challenging to share and disseminate confidential and time-critical information



NTNU

Norwegian University of
Science and Technology