Perceptions of Cyber Security Risk of the Norwegian Advanced Metering Infrastructure

Eirik Lien[a], Karl Magnus Grønning Bergh[b] and Sokratis Katsikas[c]
Department of Information Security and Communication Technology,
NTNU - Norwegian University of Science and Technology, Tekonologivegen 22, Gjøvik, Norway

Keywords: Cyber Security, Risk Perception, Advanced Metering Infrastructure.

Abstract: The Advanced Metering Infrastructure (AMI) has contributed to the further digitalization of the energy sector, but has also increased the complexity and the requirements for specialized knowledge to protect the infrastructure and the delivery of power. With different areas of focus and gaps in knowledge, the work of securing AMI can be challenging. This paper aims to provide an overview of the AMI cyber security risk perception as reflected in the research literature on one hand and amongst the stakeholders in the Norwegian energy sector on the other. The findings indicate that there is a gap between these two, both in areas of focus and the understanding of risk. Based on the identified differences, the study proposes solutions to reduce these.

1 INTRODUCTION

AMI is in short an integrated system enabling smart distribution of electricity to endpoints/end-users. This is facilitated by 2-way communication in near real-time, measuring and collecting the electricity flow and usage data (Hansen et al., 2017; Sæle et al., 2019). In terms of risk and the threat picture for AMI, recent reports from the National Security Authority (NSM) (Nasjonal sikkerhetsmyndighet, 2020; Nasjonal sikkerhetsmyndighet, 2021) and the Police Security Service (PST) (Politiets sikkerhetstjeneste, 2020; Politiets sikkerhetstjeneste, 2021) 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 reports from 2020 (Nasjonal sikkerhetsmyndighet, 2020; Politiets sikkerhetstjeneste, 2020), the threats of intelligence operations towards the energy sector 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. In a more global context, there are several incidents that show the potential in Computer Network Operations (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 (Geiger et al., 2020). These examples serve to show that state actors or other adversaries have the motivation, resources, and knowledge to exploit vulnerabilities in an interconnected energy sector.

The digitalization of the society has made the digital value chain dynamic, complex and challenging to grasp, and introduces new vulnerabilities and interdependencies between organizations. And 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 (Nasjonal sikkerhetsmyndighet, 2022). This is also evident for AMI in the energy sector (Asplund and Nadjm-Tehrani, 2016; Frogner et al., 2021). 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 paper explores and compares the state of

[a] https://orcid.org/0009-0005-3573-2206
[b] https://orcid.org/0009-0004-1378-0031
[c] https://orcid.org/0000-0003-2966-9683

Lien, E., Bergh, K. and Katsikas, S.
Perceptions of Cyber Security Risk of the Norwegian Advanced Metering Infrastructure.
DOI: 10.5220/0012414900003648
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 187-194
ISBN: 978-989-758-683-5; ISSN: 2184-4356
Proceedings Copyright © 2024 by SCITEPRESS – Science and Technology Publications, Lda.

AMI security according to literature with the perceptions and attitudes of the stakeholders regarding cyber security. It provides a summary of the work reported in (Lien and Bergh, 2023) . The research conducted addressed the question: What are the attitudes and perceptions of information security risks within AMI in the energy sector of Norway? To answer this question, a set of more specific research questions (RQs) were developed: RQ1) What information security risks are prevalent within AMI according to the literature? RQ2) What information security risks are prevalent within AMI according to stakeholders of AMI 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? RQ4) How can potential divergence between literature and stakeholder perception of information security risks within AMI in Norway be addressed?

The remaining of the paper is structured as follows: Section 2 describes the backround and related work. Section 3 describes the research methods employed and the attendant limitations. Section 4 presents the findings of the Sytematic Literature Review (SLR) performed to answer RQ1, whilst Section 5 those of the interviews conducted to answer RQ2. Section 6 provides the answer to RQ3 by comparing and discussing the findings in sections 4 and 5 and the answer to RQ4 by providing pertinent recommendations. Finally, Section 7 summarizes our conclusions and outlines paths for further research.

2 BACKGROUND AND RELEVANT WORK

A reference model of AMI, based on a review of the relevant literature and further elaborated on in (Lien and Bergh, 2023) is depicted in Figure 1. AMI 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. This model also visualizes the scope of this study, which will focus on information security risks from the interfaces at the SM up to and including the MDMS at the Distribution System Operators (DSO). The end-user or customer domain from the HAN-port is thus considered out of scope.

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 (Skotnes, 2015; Larsen et al., 2022). Both (Skotnes, 2015) and (Larsen et al., 2022) 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 is the psychometric paradigm and heuristic and biases (Larsen et al., 2022). In addition, (Skotnes, 2015) 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.

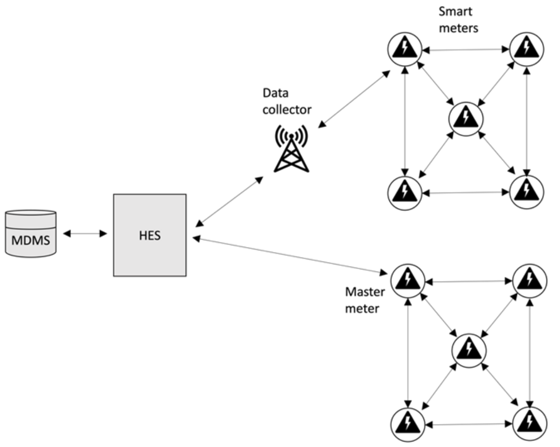

Figure 1: AMI simplified network topology, adapted from (Sæle et al., 2019; Frøystad et al., 2018; Line et al., 2012; Venjum, 2016).

The research most closely related to this study is the work in (Asplund and Nadjm-Tehrani, 2016), where the attitudes and perceptions of risk of IoT in three critical societal services in Sweden were investigated. The study (Asplund and Nadjm-Tehrani, 2016) sought to highlight the risks and perceptions of risk in services where the integration of IoT has been pushed forward by regulatory requirements, by markets and advances in technology, or by a combination of these. 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. To describe the perception of risk, (Asplund and Nadjm-Tehrani, 2016) conducted several interviews based on questions derived from preliminary workshops with actors within the services. The results 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.

The research reported in (Skotnes, 2015) investigated a topic related to that in (Asplund and Nadjm-Tehrani, 2016), looking at risk perception concerning security and safety of ICT systems amongst power supply network companies in Norway.

3 RESEARCH METHODOLOGY

3.1 Research Design

RQ 1 was addressed through a Systematic Literature Review (SLR), conducted by following the steps, phases and principles detailed in (Jesson et al., 2011, p. 103-127) and depicted in Fig. 2. In terms of scope, this work considers 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. The initial search identified 1223 potentially relevant sources. After applying the inclusion and exclusion criteria defined in phases 1-3, 32 sources were left. Details on the interim results of the process can be found in (Lien and Bergh, 2023).

RQ2 was addressed through Semi-Structured Interviews (SSI) utilizing an embedded design with a structured and a semi-structured part. A total of 27 interviews were conducted. The participants mainly consisted of representatives from DSOs (37.0%) and the regulatory authorities (22.2%). The remaining consisted of power vendors (7.4%), AMI service and equipment vendors (7.4%), end users (18.5%), and the group Other (industry organizations and Subject Matter Experts, 7.4%). 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. The semi-structured interviews generated qualitative data which were analyzed using inductive meaning coding and thematic analysis. The relevance of the data was continually evaluated against the research questions during coding and analysis. This led to a total of 8 compiled codes, namely (1) Initial perception on the concept of cyber risk; (2) Cyber risk in operation of AMI; (3) Cyber situational awareness (SA); (4) Likelihood; (5) Prevalent threats; (6) Prevalent vulnerabilities; (7) Prevalent consequences and impacts; (8) Enablers and challenges. The questionnaire and the interview guides used can be found in (Lien and Bergh, 2023).

RQ3 was addressed 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 (Lien and Bergh, 2023). The analysis was conducted by aligning the compiled inductive codes developed in the SSI with the deductive codes developed during the SLR.

3.2 Limitations

3.2.1 SLR

The 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.

3.2.2 SSI

Due to the sample size (N=27), the interview findings may have low generalizability. However, considering the sample composition, the subjects represent 1/3 of the end-users using two out the three of the most common SMs in use in Norway. Thus, their perception of and focus on information security challenges represent those of a considerable part of the AMI actors in Norway.

The analysis and interpretation of the interviews was conducted using inductive meaning coding and compilation into categories. This entailed coding statements as they appeared during the analysis, compiling them, and further condensing the statements before categorizing them. 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.

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 the operationalization of threats and vulnerabilities. The energy sector (including AMI) in the Norwegian context is considered a critical infrastructure, and as such it is subject to regulations concerning sharing and publication of information i.e., (Energiloven – enl, 1990) and (Kraftberedskapsforskriften, 2012). This prevents actors in the Norwegian energy sector and academia from providing detailed data and information on such categories through open sources and publicly accessi-

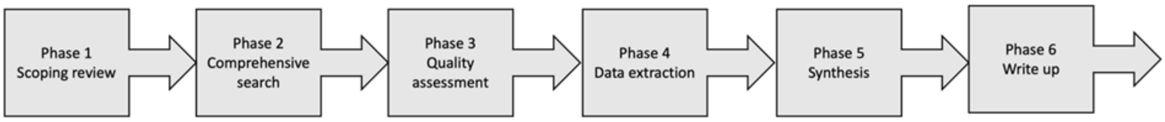

Figure 2: SLR phases.

ble databases used in this SLR. Because of this legal constraint, the study also refrained from probing into technical details regarding the risk elements in the SSI, so as to avoid participants being asked to reveal sensitive and classified information. This has to a certain extent led to blurred and general descriptions of risk elements in the SLR and the SSI. There may also be cases where the participants have withheld specific technical knowledge or other information without notifying the researchers.

4 SLR FINDINGS

The findings in the SLR indicate 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 descriptions 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 risk factors are of a functional nature and lack specific details on how these can be put into operations or how they can be exploited to cause impact to AMI. However, the nature of the factors still makes them valid, as the functional descriptions have the potential to affect any implementation. The elements of risk identified by means of the SLR are summarized and tabulated in Table 5.1 *Identified elements of risk in SLR* in (Lien and Bergh, 2023).

An important observation is the threat from compound and coordinated attacks. As described in (Frogner et al., 2021) and found in (Gunduz and Das, 2020), (Wei and Wang, 2016) and (Husnoo et al., 2023), threats can be realized as attacks both in the physical and the cyber domain via direct or indirect communication and connections. They can occur as single incidents or as compound, combined and highly coordinated attacks. Wei et al. in (Wei et al.,) 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.

5 INTERVIEWS FINDINGS

5.1 Structured Part Findings

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. The results are depicted in Table 4.8 *Comparison of consequence, likelihood and risk* in (Lien and Bergh, 2023), where ”M” stands for ”Mean” and ”SD” stands for ”Standard deviation”.

The findings from the initial analyses show no particular patterns between the different participant groups. By tabulating the risk rankings as shown in Table 4.14 *Risk perception for specific incidents in AMI* in (Lien and Bergh, 2023), 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. 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.

5.2 Semi-Structured Part Findings

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 some 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. This can further be influenced by a lack of detailed system knowledge, their perception and experiences with general ICT-related threats and how they see the system level as more or less IT-based with different interconnections. When consequence and likelihood were combined, the participants still consider the main risks as low, with the end-users yet as outliers, considering the risk both as high and extreme.

Further, the findings in the SSI indicate 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 assessed as a low risk. When the HW, communication and system levels were compared, the level of risk was considered highest at system level, followed by communication, and lastly HW with the lowest perceived risk level. The participants highlighted several vulnerabilities and threats at all levels but believe that the system will be able to handle them.

The perception of factors from the interviews are summarized and tabulated in Table 5.3 *Identified elements of risk in interviews* (in (Lien and Bergh, 2023)), where the participants share functional descriptions of the factors, answering RQ2. The table represents the most prominent vulnerabilities, threats, consequences and risks described as compiled inductive codes.

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 (NOU 2015:13, 2015). The digital value chain, the integration of IT/OT, dependence on others due to outsourcing and a 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. These are also elements put forward by the participants. 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 vulnerability, introducing significant risk to the system and a potential factor of strategic importance to malicious actors. 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 that at the system level. Lastly, the report points out that there may be privacy challenges related to measurement data and how the power consumption is considered Personal Identifiable Information (PII), thus 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 (NOU 2015:13, 2015) and the findings in this study as described in the section above shows that these may be consistent challenges, warranting a persistent focus.

6 DISCUSSION AND RECOMMENDATIONS

6.1 Comparison of the SLR and the SSI Findings - Identifying the Mismatches

The findings indicated how differences exist between the focus in academic research and the perception of stakeholders of AMI in terms of information security risks, answering RQ3. The complete comparison, providing an overview of overlaps and mismatches, was conducted in Section 5.3.1 and tabulated in Appendix E in (Lien and Bergh, 2023) . The following paragraphs discuss the main findings of this comparison.

The literature 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. This can aid in 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 with regards to both technical and organizational aspects, implies the need for a comprehensive approach to information security to alleviate the complexity and uncertainties.

6.2 Comparison of the SLR and the SSI Fndings - the Need to Address the Divergence

The comparison and further the evaluation of the divergence have identified a difference in perception of the level of risk and the absence of holistic risk assessments in the SLR (Lien and Bergh, 2023). 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.

6.3 Proposed Solutions to Reduce 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 incentivizing research and facilitating the exchange of information and 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. Such an effort could be organized under the regulatory authority to ensure legal compliance regarding power sensitive information and the sharing of information and findings accordingly.
2. **Centralized and Enhanced Information Security Governance – Reducing Complexity.** Establishing a centralized approval entity 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. By placing the entity 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.

7 CONCLUSION

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.

Several aspects could be the subject for further research:

- Extending the present study to cover other countries.
- 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.
- 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.
- Research could provide a better basis for decisions concerning measures to protect AMI PII data, potentially improving already implemented measures such as encryption and authentication or provide additional measures.
- 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.

- 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 of AMI.
- 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. 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.

ACKNOWLEDGEMENTS

This work was supported by the Research Council of Norway [grant number 310105 ”Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS”].

REFERENCES

Asplund, M. and Nadjm-Tehrani, S. (2016). Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access*, 4:2130–2138.

Energiloven – enl (1990). Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven).

Frogner, K. P., Lien, E., and Bergh, K. M. G. (2021). Smart energy metering and its infrastructure – A survey on vulnerabilities and information security challenges. Department of Information Security and Communication Technology, NTNU.

Frøystad, C., Jaatun, M. G., Bernsmed, K., and Moe, M. (2018). Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA. Report 978-82-410-1789-6, NVE.

Geiger, M., Bauer, J., Masuch, M., and Franke, J. (2020). 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)*, volume 1, pages 1537–1543. IEEE.

Gunduz, M. Z. and Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169.

Hansen, A., Staggs, J., and Shenoi, S. (2017). Security analysis of an advanced metering infrastructure. *International journal of critical infrastructure protection*, 18:3–19.

Husnoo, M. A., Anwar, A., Hosseinzadeh, N., Islam, S. N., Mahmood, A. N., and Doss, R. (2023). False data injection threats in active distribution systems: A comprehensive survey. *Future Generation Computer Systems*, 140:344–364.

Jesson, J., Matheson, L., and Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. Sage, London.

Kraftberedskapsforskriften (2012). Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften).

Larsen, M. H., Lund, M. S., and Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research*, 3:100065.

Lien, E. and Bergh, K. M. G. (2023). Attitudes and Perception of AMI Information Security in the Energy Sector of Norway. Master thesis, NTNU.

Line, M. B., Johansen, G. I., and Sæle, H. (2012). Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS. Report 8214052807, SINTEF.

Nasjonal sikkerhetsmyndighet (2020). Risiko 2020. Accessed on 2021-09-20.

Nasjonal sikkerhetsmyndighet (2021). Risiko 2021. Accessed on 2021-09-20.

Nasjonal sikkerhetsmyndighet (2022). Risiko 2022. Accessed on 2023-04-02.

NOU 2015:13 (2015). Digital sårbarhet - sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden. Accessed on 2022-12-11.

Politiets sikkerhetstjeneste (2020). Nasjonal trusselvurdering 2020. Accessed on 2022-09-10.

Politiets sikkerhetstjeneste (2021). Nasjonal trusselvurdering 2021. Accessed on 2022-09-11.

Skotnes, R. Ø. (2015). Risk perception regarding the safety and security of ICT systems in electric power supply network companies. *Safety Science Monitor*, 19(1):Article 4.

Sæle, H., Ingebrigtsen, K., and Istad, M. (2019). Fremtidens avanserte måle og styringssystem (ams): Forventet utvikling 2-5 år frem i tid. Report 978-82-410-1921-0, SINTEF Energi AS.

Venjum, A. (2016). Smarte målere (AMS): Status og planer for installasjon per 1. halvår 2016. Report 978-82-410-1532-8, NVE.

Wei, L., Rondon, L. P., Moghadasi, A., and Sarwat, A. I. 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)*, pages 1–9. IEEE.

Wei, M. and Wang, W. (2016). Data-centric threats and their impacts to real-time communications in smart grid. *Computer Networks*, 104:174–188.