CRITICAL INFRASTRUCTURE SECURITY – SMART ENERGY METERING

Smart energy metering and its infrastructure – a survey on vulnerabilities and information security challenges

Written by Eirik Lien, Karl Magnus Grønning Bergh and Kristian Prine Frogner

***Abstract*— The smart grid (SG) is now under full implementation within the society and will lead to even more interconnectedness, controllability and efficiency within the power grid. The introduction of ICT in the SG entails that information security will have a crucial role in ensuring the confidentiality, integrity and availability of the devices and the data in the system. An enabler and basis for the SG is the advanced metering infrastructure (AMI), where 2-way communication is realizing both enhanced control and convenient services for both the end-user and utility provider. However, the introduction of ICT and different communication options within SG in general and AMI in specific, will also introduce new vulnerabilities and attack surfaces that can be exploited. These vulnerabilities and vectors will be present at all levels within the AMI and may potentially have far-reaching consequences and impacts. This survey looks at the vulnerabilities introduced by the AMI, their potential impacts and how they can be mitigated in an overarching manner. The findings suggests that there is no silver bullet solution that addresses all the vulnerabilities. The level of digitization may introduce a concerning level of vulnerabilities that needs to be addressed before reaching a sufficient level of security and trust in the system. Even if the system providers are able to mitigate the vulnerabilities, there will still be residual risks, and the question is if this risk is acceptable within AMI as part of a critical infrastructure. This survey has also identified several future research areas that will improve the ability to mitigate the vulnerabilities to a certain extent, and reduce the risk, but never to zero.**

I. INTRODUCTION

ADVANCED Metering Infrastructure (AMI) has become an integral part of the power grid, and by 2019 has become an imposed part of the energy grid in Norway. With the use of ICT, advanced functionality is enabled with new services and possibilities for both the consumer and the vendor, but also introduced new attack vectors for malicious actors and for unintended faults/mishaps to traverse through. The interconnectedness of AMI and the SG with the extended use of ICT makes the power grid vulnerable to new forms of incidents, both intended and unintended, and this paper will conduct a survey on the most common vulnerabilities and information security challenges within AMI. This section will give the motivation and a short background for the subject. Further, it will state the problem and research questions this paper seeks to address, with a defined scope and an explanation of the most common concepts

A. Motivation

In March 2021, The Office of the Auditor General released a report regarding their audit of the Norwegian Water Resources and Energy Directorate´s (NVE) work in ICT security for the power grid. Their conclusions points to a lack of an overarching and holistic take on ICT security within the power industry of Norway, and that NVE has not fulfilled their task as a controlling agency in such regard [1]. It also revealed vulnerabilities at some of the different utility providers and how they work with ICT security in general. In the threat and risk assessment for 2020, both the Police Security Service (PST) [2] and the National Security Authority (NSM) [3] have highlighted the threat of intelligence operations towards the energy sector in the context of advanced network operations, where the malicious actors in some cases have the capacity to both manipulate and sabotage ICT systems. With these reports in mind, it is evident that vulnerabilities within the AMI can pose a significant threat for the power industry in Norway as a defined critical infrastructure, within all aspects of confidentiality, integrity and availability (CIA-triad). Figure 1 shows an illustration of some of the vulnerabilities and attack vectors within AMI.

B. Background and Introduction to AMI

The AMI consists of different sets of smart meters, data management systems and ICT networks which are interconnected, thus enabling communication between the utility provider and the consumer or endpoint in near real-time [4] [5]. The integrated system with 2-way communication enables different types of data to be collected and transferred between the entities in the AMI and to the general SG. Such data includes real-time measurements of energy demand, load control and field equipment status for the utility providers. The endpoints and consumers have similar abilities in the form of access to own power consumption through different applications and smart devices, an easier integration of renewable sources generated locally, and data about billing and cost.

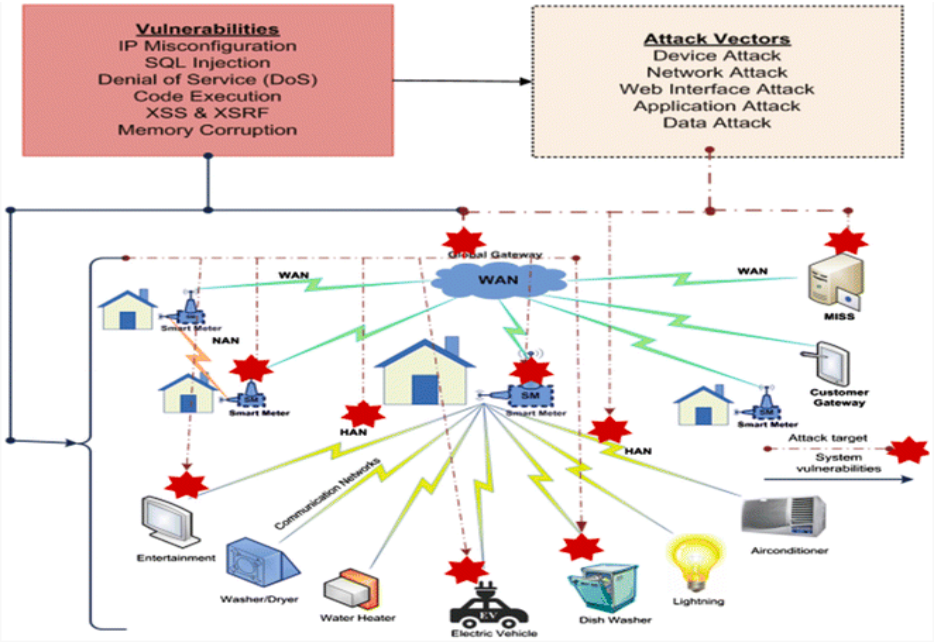

Figure 1 Overview of vulnerabilities and attacks [28]

The main components in the AMI is the smart meters, data collectors (or concentrators), communication networks, and data management systems, as shown in figure 2. The components communicate using different security measures and through various protocols and communication technologies, where fixed radio frequencies are the most common in Norway for the smart meters.

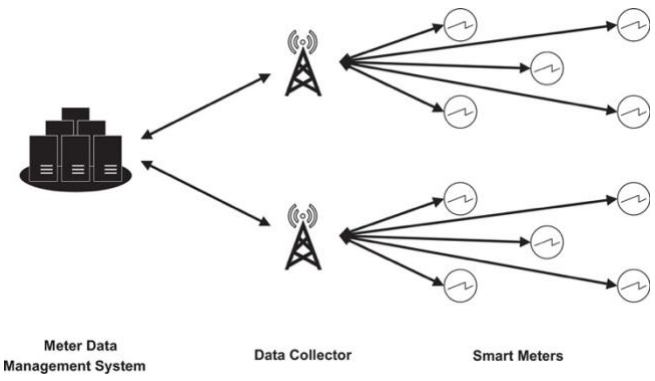

Figure 2 Overview of AMI as presented in [5]

C. Scope

The scope of this survey is to give a general introduction to the recent research on cyber vulnerabilities within AMI, and how they can be exploited to challenge all or parts of the CIA-triad. The focus will be on AMI from the consumer to the business network and management systems of the utility provider, and the metering infrastructure on the transmission and generation side in the SG will not be covered in detail.

The survey will first give an introduction to AMI as a system and the information security challenges posed by the vulnerabilities and associated threats. Furthermore, the paper will explore the possibilities for malicious attacks against the system and elements of the technology, and the potential impacts due to breach or loss of service within AMI. The survey will focus on 3 different levels in the system (according to scope) that contain different sets of security challenges and different attack vectors:

- The end-user/consumer
- The communication channel
- AMI as part of critical infrastructure.

The most common characteristics of information to retain its value for organizations, is expressed in confidentiality, integrity and availability. These characteristics will be used when examining the different security challenges, vulnerabilities and threats in regard to information security in AMI. As AMI is part of critical infrastructure, several of the characteristics are important, both in a safety and security perspective, but integrity and availability can be considered preeminent. With loss of integrity, system functionality can be compromised, and untrusted data inserted, which can result in safety critical incidents. With loss of availability to parts of or the whole system, power delivery can be interrupted or denied, and the communication delayed or severed. But confidentiality may also pose severe consequences if breached, such as the confidentiality of information and data, as privacy-related and sensitive information may be exposed or stolen.

D. The Research Questions

In order to survey the defined scope and the vulnerabilities and challenges within AMI, a set of research questions have been defined:

- What are the general ICT vulnerabilities and threats of the different elements within AMI?
- What is the impact of potential attacks?
- How can the information security challenges be addressed in AMI?

II. The methodology

In this section, the authors present the procedure for conducting the literature review, and on what basis the relevant sources and articles were selected and included in the survey.

This review has been conducted according to the principles laid out by Jefferson et al. in [6], where a systematic search and selection process is important to obtain relevant sources, articles and literature. And this was achieved by using several different academic search engines: ScienceDirect, Springer Link, Oria (NTNU online library), IEEExplore and Google scholar (aggregated results). The purpose of using different search engines, it to obtain a more diverse selection of literature from different academic areas, but as this survey is limited in scope and the numbers of surveyed papers, the effect of variation in academic fields is somewhat reduced. In the search engines, the authors used different keywords and combinations of those, such as *critical infrastructure, AMI, protection, security challenge, vulnerabilities.*

The search process is followed by a triage of the literature discovered, where the authors conducted a selection of literature to be included in the survey. Due to a high number of returns in the search process, this selection was based on an evaluation of the relevance of the abstract to our subject of investigation, the number of citations, publisher of the paper and their academic integrity and what year the paper was published. This order of priority reduced the number of articles considerably and eased the task of scrutinizing the papers more thoroughly in terms of structure, content and an overall subjective consideration. And as described in [6], the authors in addition used snowballing search, by utilizing the references used in the selected articles to find related and comparable studies and literature.

III. Classification scheme

Research on critical infrastructure and the introduction of the concepts SGs and smart cities provide a wide range of topics with different focus. The implementation of AMI and smart metering in the general society is one such topic, where vulnerabilities and information security challenges is a more fine-grained issue. The general research trend within information security in AMI seems to deal with different subjects, focusing on both the systems within the system, and AMI as part of the SG and smart cities. The literature search revealed a tendency to focus on one or more of the different elements within AMI: The end-user or consumer, the communication channels, and the AMI as part of the SG and critical infrastructure. Within the different elements, the vulnerabilities and information security challenges are in a majority of the research identified, evaluated against their effect on the CIA-triad.

The end-user or consumer consists of the elements that is on the border of the utility providers reach or network. They involve the smart meter itself and its connection via the Home Area Network (HAN)-connector to the home appliances by different communication standards. Several papers involve this level, and describes the vulnerabilities, threats and attack vectors for the different elements. [5] is one example of research covering this level.

The next area that is frequently researched, is the communication channels and protocols. Several different channels and methods are used for transferring data within the AMI and between the different networks. This involves combining different technologies, requiring interfaces between the networks and technologies. The research identified covers the communication from the smart meter to the head-end, and what vulnerabilities, attack vectors and threats that exists towards the different technologies, standards and protocols used. [7] is one example of research covering this field.

The last identified research area is looking at AMI in the context of the smart grid. This research looks at how shortfalls in AMI security could potentially affect the whole smart grid, being the presumably most vulnerable component in the smart grid. [8] is an example of such research.

The identified research trends will in the course of this survey be used as a classification scheme to structure the review of the identified research sources, where the focus lies within identifying vulnerabilities and threats in the different areas.

IV. Survey on vulnerabilities and information security challenges

A. General ICT Vulnerabilities and Threats in AMI

In this section, the survey will explore possible vulnerabilities and threats within AMI. This will be done by looking at vulnerabilities that may be exploited and result in a breach of confidentiality, integrity and/or availability.

i. End-user (Smart meter, connected consumer electronics)

At the end-user location, the old analogue meter has evolved into a digital minicomputer through the last 20 years, and it is by all means a cyber physical device (CPD, shown in figure 3). Basic smart meter functionality consists of electronics that will measure the load of the consumer circuit and communicate this data back to the grid company at regular intervals, such as 15, 30 or 60 minutes [5]. Other functionality such as power shutoff can be initiated in scenarios like missing payments from the consumer or when security hazards are present, for example an ongoing fire in the building. According to [9] the smart meter can provide functionality such as:

- Real-time power measuring and reporting back to the power utility company, and provide historical data
- Monitor and report on power quality
- Remotely connect and disconnect the consumer from the grid
- Notify utility company about errors or technical problems
- Remotely install updates to firmware or software in smart meter
- Provide load limiting features for non-essential loads

Figure 3 Smart meter [5]

[5], [7] and [10] describes the communication flow, and smart meter usually has two communication flows: one towards the utility company (the head end of the AMI), and one towards the internal network of the consumer (Home, Business or Industry Area Network: HAN/BAN/IAN)). These networks can provide interoperability with consumer devices within a relative short physical range. The interoperability can give functionality such remote visualization of meter data to the consumer or load shedding (LS). LS is a functionality where the grid owner can reduce load on the grid by remotely disconnecting non-essential load at the consumer end, and thus balance the load in high-load scenarios, as an alternative to increasing the capacity in the grid, which can be an expensive solution.

With an increase in renewable energy generation at the consumer end, from products such as solar power and windmills, combined with energy storage in products such as dedicated battery storage or vehicle to grid (V2G), there is an increased need to exchange data to control the power flow in the SG. The smart meter will be the hub of the connected devices at the consumer location and provide data to the control plane which secures the flow of electrical energy in the grid.

[5] and [11] looks at the smart meter itself, and identifies multiple potential attack points at the physical level. Smart meters are usually enclosed and sealed off with a unique seal from the utility company, deterring a physical attack at the smart meter, which would break the seal. Opening the meter itself could trigger an alarm to the utility company, indicating that someone is tampering with the device. [11] states that these physical protection mechanisms can usually be bypassed by a dedicated attacker and does not prevent a "hit-and-run" type attack, because the physical protection is mainly targeted against the consumer. If an attacker would break through these mechanisms, either by physical or logical access, they could cause considerable damage. However, [11] argues that physical tampering is easy to detect, and as such a logical attack is more likely (e.g. a cyber-attack). This hardware platform is in general susceptible to multiple attack types and different vulnerabilities according to [5]:

- Firmware/software modification
- Firmware/software vulnerabilities
- Theft of intellectual property or sensitive information such as certificate keys
- Sensor modification
- Communication interception or alteration

Once inside the smart meter, [5] describes further possibilities: The hardware could be reverse engineered, and the resulting information could be used to craft new types of attacks which would not require physical access to other smart meters. For example, reverse engineering could result in information about the radio interface and vulnerabilities that could make it possible for an attacker to gain access to the device using a radio interface remotely.

It is a well-known fact that networked IT-products have a strong tendency to have vulnerabilities brought into daylight as time passes. The vulnerabilities often exist from the beginning or are introduced within the lifecycle of the product, but they might not be discovered until later in the lifecycle. Radio interfaces could have vulnerabilities discovered 20 years into the lifespan and pose a continuous risk if the software cannot be updated to close the vulnerability.

As a summary, using the work of [5], the common attack vectors for a smart meter are described as:

- Requiring physical access:
  - Wired HAN, BAN and IAN-connection.
  - Directly attacking the physical hardware of the smart meter.
- Requiring physical closeness:
  - Wireless HAN, BAN and IAN-connection.
  - Smart meter connection to data collector (wireless, powerline).
- Requiring only internet:
  - IoT device connected to internet and HAN, BAN and IAN.
  - Smart meter connected to internet for utility company control.

ii. The communication channels

One of the main system capabilities of the AMI is the ability to facilitate communication between utility and consumers as visualized in figure 4. Certain data also has real-time requirements, i.e communicated with specific latency requirements, while other information objects can be buffered and delayed without negative consequences. The AMI communication has CIA requirements due to the private and sensitive customer information and the control commands that is frequently exchanged through the communication network, and as such is regulated by [12] in a European context.

In [7], the communication options are detailed and how they accommodate the wide range of meter deployment topologies, e.g., from dense urban settings to sparse rural environments. The AMI is designed with a highly flexible network architecture that can include a mix of different communication technologies. These technologies are based on different inherent properties between wired (PLC, fiber optic,

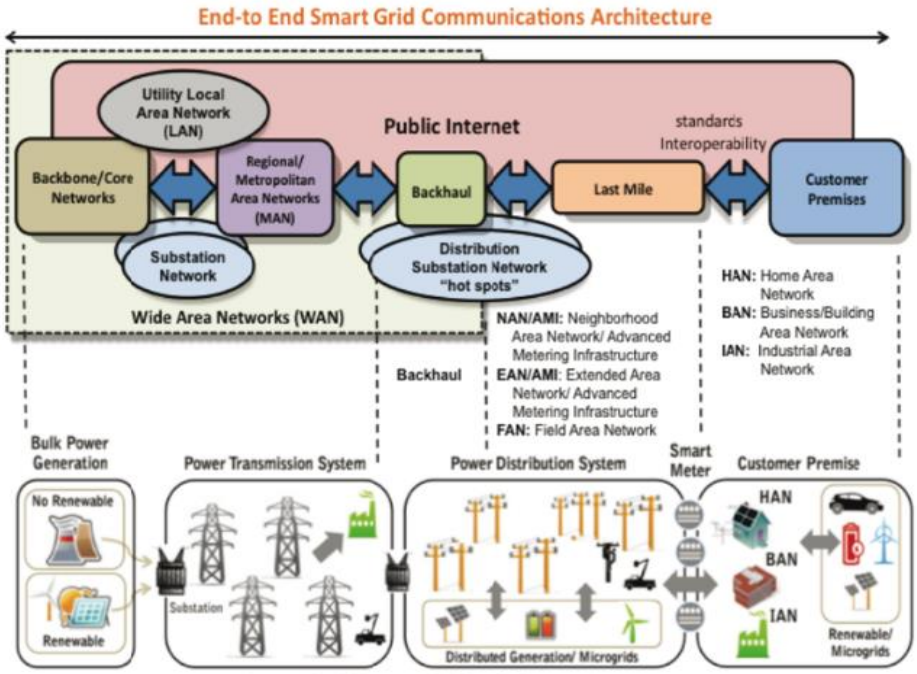

Figure 5 AMI communications architecture [9]

and DSL) and wireless (WPAN/ZigBee, Wi-Fi, WiMAX, cellular and satellite) communication.

The architectures usually follow the same network hierarchy as shown in figure 4 and is described by Mendel in the overview of the SG and its security challenges in [9]. A simplification of the architecture description will be that the wide area network (WAN) connects utilities to a set of gateways in the field and back to the head end of the ecosystem, and then neighbourhood area networks (NAN), also called field area networks (FAN), connect gateways to meters. These networks also include the different network topologies defined as HAN, BAN and IAN.

Further in the work of [7], the different communication technologies are described and how they are utilized in order to create the flexibility that is needed to support the large network of the SG and AMI, shown in table 1. E.g., smart meters can directly include cellular capabilities or even use the customer's Internet connection to bypass the need for separate WANs and LANs in a local communication ecosystem. It briefly mentions the requirement for real-time but does not go into specific detail. However, in [13], some of the real-time requirements are described, as AMI and the SG need communication channels that ensure reliable and timely information exchange within the ecosystem. [10] and [14] goes more into the depth of the requirements for real-time. [14] argues that for the AMI as part of the SG, the need for real-time information exchange is currently not considered as critical for the sustainment of power production and distribution towards the AMI. This is due to the level of integration between AMI and other SG functions. However, [10] also argues that attacks on real-time requirements may impact the efficiency that the SG is seeking to obtain by keeping the production of power at an optimized level to meet the consumers power requirements. It also states that real-time communication and information exchange in AMI will increasingly affect the generation and distribution part of the SG, and will with better integration of Distributed Energy Resources (DER) and other devices at consumer level, be critical to uphold a safe, reliable and optimized power distribution. Therefor the latency and bandwidth needed for all types of real-time information exchanges can be subject for attacks or exploitation in order to reach an attacker's intent.

As [7] details the availability of different communication technology and how it gives the AMI architecture/ecosystem its flexibility and strength, the technology also widens the possible attack vectors. It is giving the attacker a wide array of technologies that can be breached and exploited. The implementation of mesh topology is also described in [7] and [15], and how it brings additional robustness to the communication network, where communication routes can automatically adapt when failures occur. However, [15] also states that mesh technology also represents a challenge for the deployment of an efficient security monitoring solution, such as Intrusion Detection Systems (IDS).

[16] describes some of the known attack techniques towards the AMI communication and its communication protocols (standards). The Smart Energy Profile 2.0 (SEP 2.0) protocol is a set of interoperability standards defined by the ZigBee Alliance from 2014 and regulates how the consumer side of the AMI connects to the HAN side of the smart meter device. SEP 2.0 together with the TCP/UDP packet layer of the protocol has known vulnerabilities which can be exploited by different attack techniques to get the desired effect. This is visualized in figure 5. The communication link provided by the *smart meter to data collector* (SMDC) interface on the smart meter is of particular interest. The link connects the smart meters to the rest of the AMI network by 2-way communication, in the form of ethernet or unsecured serial ports, as well as medium-range RF communications (e.g WiMAX, cellular communication). As such, it provides several possible attack surfaces an adversary may utilize to gain access to the network.

Comprehensive list of communication technologies used in the smart grid.

Tech.	Standards	Data rate	Distance	Network	Advantage	Disadvantage
Wireline technologies						
PLC	• NB-PLC: ISO/IEC 14908-3,14543-3-5, CEA-600.31, IEC61334-3-1, IEC 61334-5 (FSK) • BB-PLC: TIA-1113 (HomePlug 1.0), IEEE 1901, ITU-T G.hn (G.9960/ G.9961) • BB-PLC: HomePlug AV/Ext., PHY, HD-PLC	• NB-PLC: 1–10 kbps for low data rate PHYs, 10–500 kbps for high data-rate PHYs • BB-PLC: 1–10 Mbps (up to 200 Mbps on very short distance)	• NB-PLC: 150 km or more • BB-PLC: about 1.5 km	• NB-PLC: NAN, FAN, WAN, large scale • BB-PLC: HAN, BAN, IAN, small scale AMI	• Already constructed wide communication infrastructure • Physical disconnection opportunity according to other networks • Lower operation and maintenance costs	• Higher signal losses and channel interference • Disruptive effects caused by appliances and other electromagnetic interferences • Hard to transmit higher bit rates • Complex routing
Fiber optic	• AON (IEEE 802.3ah) • BPON (ITU-T G.983) • GPON (ITU-T G.984) • EPON (IEEE 802.3ah)	• AON:100 Mbps up/down • BPON:155–622 Mbps • GPON: 155–2448 Mbps up, 1.244–2.448 Gbps down • EPON: 1 Gpbs	• AON: up to 10 km • BPON: up to 20–60 km • EPON: up to 20 km	• WAN	• Long-distance communications • Ultra-high bandwidth • Robustness against electromagnetic and radio interference	• Higher installing costs (PONs are lower than AONs • High cost of terminal equipment • Not suitable for upgrading and metering applications
DSL	• ITU G.991.1 (HDSL) • ITU G.992.1 (ADSL), ITU G.992.3 (ADSL2), ITU G.992.5 (ADSL2+) • ITU G.993.1 (VDSL), ITU G.993.1 (VDSL2)	• ADSL: 8 Mbps down/1.3 Mbps up • ADSL2: 12 Mbps down/ 3.5 Mbps up • ADSL2+: 24 Mbps down/ 3.3 Mbps up • VDSL: 52–85 Mbps down/16–85 Mbps up • VDSL2: up to 200 Mbps down/up	• ADSL: up to 5 km • ADSL2: up to 7 km • ADSL2+: up to 7 km • VDSL: up to 1.2 km • VDSL2: 300 m–1.5 km	• AMI, NAN, FAN	• Already constructed wide communication infrastructure • Most widely distributed broadband	• Communication operators can charge utilities high prices to use their networks • Not suitable for network backhaul (long distances)
Wireless technologies						
WPAN	• IEEE 802.15.4 • ZigBee, ZigBee Pro, ISA 100.11a (IEEE 802.15.4)	• IEEE 802.15.4: 256 kbps	• ZigBee: Up to 100 m • ZigBee Pro: Up to 1600 m	• HAN, BAN, IAN, NAN, FAN, AMI	• Very low power consumption, low cost deployment • Fully compatible with IPv6-based networks	• Low bandwidth • Limitations to build large networks
Wi-Fi	• IEEE 802.11e • IEEE 802.11n • IEEE 802.11s • IEEE 802.11p (WAVE)	• IEEE 802.11e/s: up to 54 Mbps • IEEE 802.11n: up to 600 Mbps	• IEEE 802.11e/s/n: up to 300 m • IEEE 802.11p: up to 1 km	• HAN, BAN, IAN, NAN, FAN, AMI	• Low-cost network deployments • Cheaper equipment • High flexibility, suitable for different use cases	• High interference spectrum • Too high power consumption for many smart grid devices • Simple QoS support
WiMAX	• IEEE 802.16 (fixed and mobile broadband wireless access) • IEEE 802.16j (multi-hop relay) • IEEE 802.16 m (air interface)	• 802.16: 128 Mbps down/ 28 Mbps up • 802.16 m: 100 Mbps for mobile, 1 Gbps for fixed users	• IEEE 802.16: 0–10 km • IEEE 802.16 m: 0–5 (opt.), 5–30 acceptable, 30–100 km low	• NAN, FAN, WAN, AMI	• Supports huge groups of simultaneous users, longer distances than Wi-Fi • A connection-oriented control of the channel bandwidth • More sophisticated QoS than 802.11e.	• Complex network management is • High cost of terminal equipment • Licensed spectrum requirement
GSM	• 2G TDM, IS95 • 2.5G HSCSD, GPRS • 3G UMTS (HSPA, HSPA+) • 3.5G HSPA, CDMA EVDO • 4G LTE, LTE-Advanced	• 2G: 14.4 kbps • 2.5G: 144 kbps • HSPA: 14.4 Mbps down/ 5.75 Mbps up • HSPA+: 84 Mbps down/ 22 Mbps up • LTE: 326 Mbps down/86 Mbps up • LTE-Advanced: 1 Gbps /500 Mbps	• HSPA+: 0–5 km • LTE-Advanced: optimum 0–5 km, acceptable 5–30, 30–100 km (reduced performance)	• HAN, BAN, IAN, NAN, FAN, AMI	• Supports millions of devices • Low power consumption of terminal equipment • High flexibility, suitable for different use cases, • Open industry standards	• High prices to use service provider networks • Increased costs since the licensed spectrum
Satellite	• LEO: Iridium, Globalstar, • MEO: New ICO • GEO: Inmarsat, BGAN, Swift, MPDS	• Iridium: 2.4–28 kbps • Inmarsat-B: 9.6 up to 128 kbps • BGAN: up to 1 Mbps	• 100–6000 km	• WAN, AMI	• Long distance • Highly reliable	• High cost of terminal equipment • High latency

Table 1 Communication technologies used in SG [7]

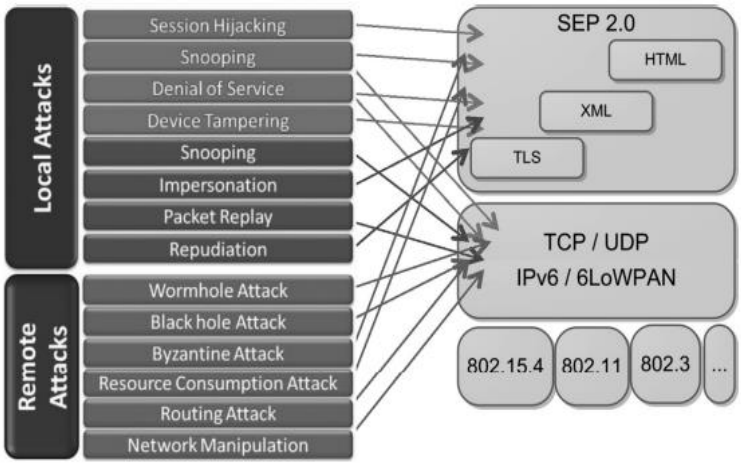

Figure 6 SEP 2.0 and packet layer attack surface [16]

Another inherent vulnerability within the communication channels is the hard-coding of specific secure communication implementations within the hardware. [15] describes this, where many AMI devices rely on proprietary and secret code and algorithms that is embedded in the hardware in order to obtain security through obscurity. Such security techniques may be well protected by the vendors and are usually specific to the make and model of the device, but in the end, it will not provide a consistent level of security. Once breached, all related equipment would need to be replaced or updated.

This section has described a myriad of protocols and capabilities for communication within the AMI ecosystem and some of the potential vulnerabilities. Based on the research surveyed in this area, it is this study´s assumption that these vulnerabilities can to a certain degree be related to a cost-driven development, where security has been bolted on at a later stage. The partly constrained environment that devices and the communication channels in AMI is operating in, is also assumed to be a direct consequence of this, where security solutions now have to be tweaked and adapted to this environment.

iii. AMI as part of the SG

When looking beyond the different components and the architecture in AMI, the next level is the SG itself. A system of system to a greater extent than AMI, but with security challenges both introduced to and received from AMI.

The SG consists of a complex architecture with different communication methods as described in the previous section. The sheer complexity makes it challenging to maintain awareness and oversight of the potential vulnerabilities the

complexity is entailing. [17] is describing the NIST conceptual model for a SG consisting of 7 domains as shown in figure 6. Each domain has actors and applications, where actors are devices and systems, and applications are tasks performed by actors in one domain. Both [17] and [10] recognizes the importance of and the vulnerabilities within the applications, where AMI, SCADA (Supervisory Control and Data Acquisition) and the intelligent substation stands out in this regard.

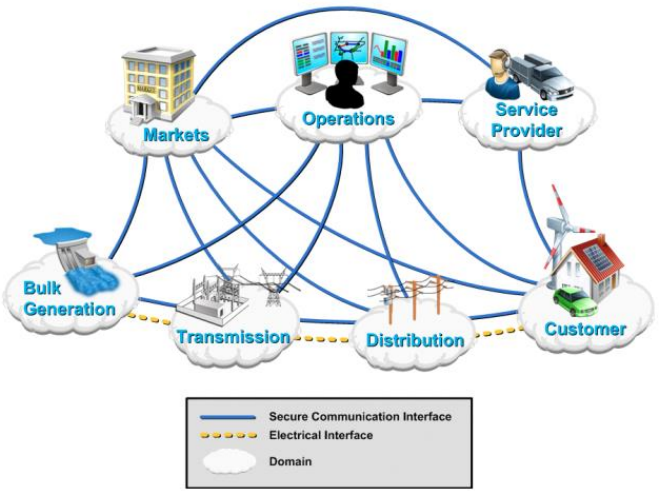

Figure 6 Conceptual model of the SG [31]

In regard to vulnerabilities and attack vectors affecting AMI from the SG, NIST in [18] describes some overarching risks with the SG, such as introducing common vulnerabilities to systems in which it interacts or interoperates with. In essence, the complexity of the SG and the extensive use of networked components with bidirectional flows of data, is introducing vulnerabilities that can challenge the integrity, availability and confidentiality of the data transmitted. However, it is assumed that the motives and intentions when attacking the SG (e.g. on the transmission side), the maximized utility would be obtained by exploiting the Industrial Control Systems (ICS) or its communication channels (e.g. causing wide-spread blackouts by Distributed Denial of Service, DDoS). It would be a cumbersome path to take by attacking ICS or other parts of the SG only to gain access to and exploit the CIA-triad of the AMI. A more efficient attack vector could be to enter the network where head end and the AMI management systems resides where the potential impact would be greater in regard to affecting the CIA of the AMI as a whole. Several possibilities are examined in [19], where vulnerabilities exploited in the management systems could be used creatively, and described below. An example affecting the integrity, is exploiting the Demand Response (DR) signalling between the demand response management systems (DRMS) and the smart meter and its connected devices, either by message modification or false synchronization attacks. By doing this an attacker could reschedule device operation timings (message modification) or affect the DR system as a whole. An example affecting the availability is exploiting the LS signalling from the Load Management System (LMS). By manipulating the LS schedule or making the LMS signalling unavailable or delayed (e.g ransomware on the LMS), the grid´s availability is at stake. The last examples are regarding the confidentiality of customer related data, where an adversary could exploit third-party services. These services are utilizing the data collected through AMI to provide data to the customer based on the consumption, and to act as a smart home integrator where different appliances are connected, and their usage scheduled. By impersonating a service provider or eavesdropping, an adversary could gain access to customer data and possibly disrupt the communication between third-party services and the customer.

In regard to vulnerabilities and attack vectors introduced into the SG from AMI, [8] looks at some of the vulnerabilities affecting the CIA-triad of the SG. The article describes the usage of the data collected through AMI within the SG, such as real-time monitoring of the grid and energy management. It also describes the vulnerabilities in the communication channels transmitting the data, where both the confidentiality, but more importantly, the integrity and availability of AMI data can be compromised. False data injection and RF jamming is mentioned as sources that affects integrity and availability of the data and as such will affect the real-time monitoring and management. In specific, it lowers the ability to reduce the peak-to-average ratio and prevention of overloading in the distribution network. By affecting enough smart meters or data concentrators, attackers can potentially cause physical effects in the SG by injecting false metering data or by DoS-attacks in the form of jamming the signal or communication channels in the AMI network. Similar vulnerabilities and the propagation of them into the SG is described in detail in [19].

B. What are the impacts of potential attacks/threats?

When addressing the different vulnerabilities of the AMI, the impacts when exploiting those will have different effects on the confidentiality, integrity and availability of data and systems in the infrastructure. In contrast to traditional ICT systems where the confidentiality, integrity and availability are often prioritized in the order written, the AMI and SG generate and facilitate the delivery of a critical commodity to the consumers: electric power. As such, it often prioritizes integrity, availability and then confidentiality when facing trade-offs in the network [20].

The impacts will vary depending on the adversaries and the threat they pose (level of access, intention and resources available), the vulnerabilities exploited (e.g., management systems, the embedded systems or the communication channels) and the target(s), as described in [21]. In order to evaluate the level of impact from different threats, a method used is the FIPS 199 impact level assessment criteria [22], both adopted by [21] and [19]. In this method, the security objectives is based on the CIA-triad, and defines a level from low, medium to high. This survey will present an overarching summary of threats and impacts, by selecting threats specific to the scope of this paper (AMI from the consumer to the business network) from [23], [21], [16], [24], [19] and [5]. The security objectives will be the CIA-triad. The levels or categories defined is i) system level, where the metering network as a system is targeted, ii) end-user, consisting of the smart meter and connected smart home appliances, and iii) communication channels. The sheer number of possible attacks and different

impacts is not feasible to describe in this section alone, but what this survey perceives are the most significant ones in potential of impact will be mentioned.

i. Threats and impacts at system level

At system level, attacks may have the potential to take down whole or parts of the network in AMI or the SG. Examples of this are adversaries with access to management systems that can disconnect customers´ smart meters, or other control devices in the grid. This study looks at 2 different threat categories at this level, based on [21] and [19]. Both will give high impacts and consists of *compromise of head end and management systems, and DDoS*.

Compromise of head end at system level can be achieved by several types of attacks, but more commonly are social engineering-types. With access to management systems, the attacker can either issue malicious commands to the AMI systems (e.g power disconnect at smart meter) or propagate further into the control system of the grid (such as in the Ukrainian power grid attacks [25]). As such, the impact is considered high, and can affect all elements of the CIA-triad.

DDoS is the degradation or denial of a service within the AMI and targets the availability objective. E.g by attacking the utility server during critical peak hours, the Demand-Response functionality can be made unavailable, thus reducing the ability to conduct load shedding when grid reaches its maximum capacity. By affecting a large enough number of smart meters during peak hours, damage can be inflicted on the grid. As such, the impact of DDoS can potentially be high.

ii. Threats and impacts at end-user level

The work of [5] describes the most typical threat at the end-user level being theft of power, by manipulating either the smart meter itself, or by rerouting the power around the smart meter. This is done to avoid being billed the consumed power, and is usually performed by the consumer for financial reasons and will thus only impact the utility company financially. [5] also states that if the attack is turned "around", it could also be possible to modify the smart meter itself to report a larger power consumption than what is actually consumed. Competing businesses could use such an attack to gain competitive advantage over each other by increasing the energy bill of the competitor. Such attacks on the integrity of the data can is assessed to have an overall low to medium impact.

In [16] and [5], the power switch in the smart meter is highlighted as another vulnerability. As the smart meter contains a remotely operated power switch, different attacks can be launched to deny the end user power, by remotely switching off the power switch by utilizing different communication channels to the smart meter. This can be done from the head end of the solution, which is managed by the utility company, but there is also a possibility that this can be done using the HAN/BAN/IAN interface if it is not secured against attacks. If vulnerabilities are found in the HAN/BAN/IAN interface, this could also be exploited at a large scale, e.g. if many users have IoT-devices connected to the smart meter, and as such could have a high impact.

As a discussion point in this section, this study would also add the possibility of upstream-attacks originating from the smart meter. Depending on the communication protocols between the smart meter, data collector and head end, the smart meter could be seen as a gateway into the AMI. If the protocols between the different devices are feature-rich, it could be possible for an attack to be launched upstream with the smart meter serving as a gateway for an attacker. The attacker could be local to the smart meter, or remote if the smart meter is compromised from the HAN/BAN/IAN interface via an IoT device. If such attacks are successful and reaches the head end and the management systems, it could have potentially high and widespread impacts.

iii. Threats and impacts towards communication channels

The communication channels within AMI provides ample attack surfaces and vulnerabilities. Impacts towards the CIA-triad is assumed to be possible to obtain through all the different channels. The threats regarding the communication channels is described in [23] and supported by [24], to revolve around privacy attacks, data attacks, device attacks and network availability attacks. [24] also includes web interface and application attacks. In [23], privacy attacks aims at affecting the confidentiality objective, by obtaining end-user private data using metering data. Further, data attacks attempts to affect the integrity objective of data by inserting, deleting and altering data in the network traffic. Network availability concerns the availability of the communication channels, which can be affected by e.g DDoS attacks. Device attacks can affect several objectives, as it is often an initial step for other attacks. According to [24], the attacks can manifest themselves as RF jamming, wireless scrambling, eavesdropping and message/packet modification/injection as some examples. The impacts can be reduced service availability, financial losses, privacy breaches, and affect overall grid optimization and reliability. By this the impacts can reign from low to high in regards to the customers, the utility provider and the SG itself.

C. How can the Information Security Challenges be Addressed in AMI?

The authors would like to start off with the common fact that there appear to be no single "silver bullet" solution or answer that will magically secure the AMI against attacks. Depending on the vulnerability and threat actor, the survey have shown that there are however multiple concepts that will greatly reduce the risk within the AMI. There is rarely a possibility to reduce the risk to zero within IT systems, and it is more a question of controlling the risk and knowing where your weak spots are.

The communication between the different devices in AMI can be addressed by encryption standards, ensuring the confidentiality and integrity of the data, and are discussed in several papers, such as [10], [17], [19], [26] and [27]. In [19], different schemes are discussed, with different areas of application. Public key infrastructure (PKI) could be deployed to protect the integrity of the data, while symmetric encryption could be used for confidentiality, is one suggestion presented in [19]. However, devices in the AMI will need to have sufficient processing capabilities to handle the added overhead with the encryption schemes. In [26] similar and other schemes are presented, but it also argues that in general, asymmetric schemes would be preferable, as studies have revealed that symmetric key schemes used at large scale within a system is

unsecure and costly. In addition to confidentiality and integrity, encryption schemes could also address challenges such as validation and authentication of devices, in which both [26] and [19] discuss several encryption schemes.

Further, in regards to secure communication, [19] discusses the need for universal security standards in communication protocols and data types, and how this can enable interoperability and secure communication. This approach can aid in reducing the challenges posed by the different subsystems and devices in AMI and the smart grid and their cooperation. Both [28] and [16] indirectly supports this view, as they describe the challenges with closed standards and proprietary solutions, and the need for open standards to better ensure integration and enhance security. Open standards can also lead to avoiding a vendor lock-in situation, making it easier to change equipment vendors at a slow pace instead of having to replace all equipment at the same time. And a low threshold to change equipment vendor can also help in making security a competitive advantage when a utility company can replace an equipment vendor with a low security stance.

At the end-user, [5] describes how a local device such as the smart meter and data concentrator can be attacked physically, compromising the meter itself. There are multiple ways to reduce the risk of a compromise of the device, and [9] brings forth some techniques from consumer electronics such as cellular phones, where signed code and hardware security devices could be used to protect the integrity of the device. While in [15], IDS is discussed as an option to counter physical tampering with devices such as smart meters and concentrators, however, the prevalence of IDS in AMI is currently low [8]. Another significant measure brought up in [14], is the need to secure the HAN/BAN/IAN interface at the smart meter. It is assumed that IoT-devices with internet access will be connected to this interface on a large scale. Making sure the different commands are well defined and secured, and that input validation is performed at the interface, will reduce the possibility of interface exploitation. However, [14] also argues that with the current integration, upstream attacks from the smart meter will have limited reach in the network, as it assumes the head end and management systems will be heavily protected. When it comes to local physical attacks with the purpose of reducing the energy bill for the consumer, they can be more challenging to protect against. To counter this, the smart meter itself can be hardened with different measures as described earlier. However, there will always be a way to reroute power around the smart meter, and is probably an easier way to do this, rather than modifying the smart meter itself. [5] looks at a general approach to theft of power, where a proposed solution could be to apply algorithms at the data management system, with the ability to analyse sudden changes in power consumption over time. This could trigger warnings of possible power theft, indicating they need further investigation.

In regard to the devices in AMI in general, with software and hardware vulnerabilities popping up at an alarming rate globally, it will be increasingly important to maintain a possibility to securely upgrade the software in devices in an efficient manner, down to all components in the AMI. Remote software update is probably the only way to update the software in the smart meters themselves, with millions of physical devices locked into private homes. In this regard, [10] describes the similarity in requirements for IoT and AMI as part of SG, and the need to be able to securely and remotely update devices. [26] supports this view and discusses 3 options for this, using encryption, high assurance boot or secure validation software. With extremely long life expectancy, it is important that the system manufacturers will provide updates to the equipment if needed during the life span of the devices.

In order to detect inconsistent behaviour and anomalies within networks, different types of IDS´ can also be deployed within the AMI itself, in which [8] and [10] gives several examples of. Both host and network-based IDS can be deployed, but with many components being similar to OT-equipment with limited processing capacity, network-based IDS could be the best option, giving more value for the money. A well-defined network topology could make it easier to also deploy a host-based IDS. In [15], several solutions of IDS implementation are assessed, where cost and system constraints are key factors.

As a final point, the study would like to address the need to acknowledge that information security incidents will inevitably occur. The importance of resilience in this regard is highlighted in [10], as one of several additional requirements to the CIA-triad, to ensure a reliable, stable and safe delivery of service. This can take the form of built-in fault tolerances and fallback-functionality to a secure equilibrium, maybe with lower functionality and higher operation costs, but providing minimum services to the consumers. Planning for incidents and training for recovery can save valuable time and provide a faster recovery. This would be aligned with the NIST cybersecurity framework detailed in [29], more specifically the *Respond* and *Recover* pillars.

V. Discussion

Section *IV* has given an overarching introduction to the vulnerabilities and impacts of threats exploiting the vulnerabilities. Based on this, it is timely to ask why the AMI has been introduced in the first place. With the number of vulnerabilities and the potentially high and widespread impacts, one could to some extent say that it may introduce a concerning level of vulnerabilities.

With AMI, the utility provider has the ability to reduce the margins in the grid, by extensive real-time measurement of all parts of the SG. This enables better load balancing and load shedding and eases the introduction of DERs such as solar and windmills at the end-user and within the general grid. In addition, an AMI would not only benefit the level of services and control in the developed world, but is assumed to also have significant impact in countries with low capacity in an underdeveloped grid. With better real-time overview and the consumption of power, they can to a larger extent control the grid and plan for rolling blackouts, rather than having random and uncontrolled blackouts caused by sudden and uncontrolled congestion in the grid.

However, the possibilities introduced with AMI for both utility provider and end-user can also mean more possibilities for adversaries to affect a critical infrastructure. Each new device and communication channel would mean an additional attack vector for the adversaries. With a complex system of systems, it can be challenging to have complete oversight of the

assets and their vulnerabilities, and the threats seeking to exploit the vulnerabilities. Such systems may have dependencies and interdependencies that can be difficult to map out, where attacks could lead to cascading effects.

An approach that to some extent may handle the ever-increasing threats and security challenges and complement the purely technical measures, can be the adoption of the *zero trust* mindset in AMI and the SG. This study believes that with increasing knowledge around information systems and security, there is always a possibility to compromise parts of the infrastructure. With the zero-trust mindset, the impact of a specific compromise can be reduced, and it may be easier to perform detection and recovery with a lower incident cost. The zero-trust mindset is based upon the fact that no device, user, interface, communication channel etc., should be trusted by default. All values in the AMI should prove that they are in fact what you think they are, and this should be verified. There is no single solution to achieve this, but with this mindset the authors believe a higher level of security can be achieved. This mindset is now starting to be operationalized in a US critical infrastructure, the Department of Defense, as described in [30].

As a summary of the different vulnerabilities, threats and impacts, it is worth noting that the research surveyed often explores in detail single occurrences, but to a lesser extent look at the effects and impacts caused by coordinated attacks. Attacks can happen both in the physical space and in cyber space, by direct connection or indirect connection, and combined and coordinated. [15] to some extent details the possibilities with coordinated attacks and suggests different implementations of IDS to better detect those. This is supported by [8], where more extensive and detailed implementation of behavioural IDS (called IADS) used with Coordinated Cyber-Attack Detection System (CCADS). Coordinated attacks can affect all of the security objectives by exploiting different vulnerabilities with different attacks, and as such could have severe impacts on AMI and the SG. In order to counter such attacks, sufficient protection at each element, in depth and in all network layers may be required. [10] gives insights into the vulnerabilities and mitigative actions at each network layer, but does not go into detail regarding the potential impacts such attacks can have.

VI. Conclusion

The topic of vulnerabilities and information security challenges in AMI shows a vastly complicated system with different protocols, devices and communication channels. The different elements of AMI need to be considered both alone, but also as part of a system, in order to get a holistic view of the challenges. By highlighting the vulnerabilities and threats to the different assets in the system, and the system as a whole, the first step in a common risk assessment is underway and will enable the different stakeholders to better implement mitigating measures.

This survey has briefly touched up on some of the vulnerabilities and information security challenges in AMI. The road ahead in terms of securing the CIA-triad seems to have several issues which needs to be addressed in order to reach an acceptable level of security. Two main issues can be inferred from this survey, where lifetime expectancy and a constrained environment is one of them. Utilizing the vast deployment of AMI devices and networks as a basis, the equipment and software need to be designed with long lifetime expectancy simply due to the cost of implementation. However, new vulnerabilities and threats will be discovered in the future, and as such the AMI and the SG must be designed to account for future discoveries. This will require both to a greater extent utilizing hardware and software designed with long lifetime expectancies, but also with a high degree of updatability. Without this ability, the systems and software will be outdated relatively fast, incurring more cost in replacements and cumbersome updates when critical vulnerabilities are discovered in the future. The ability to conduct updates and improvements needs to consider the constraints in the operating environment, where security solutions need to be tailored to the environment they are operating within, while still adhering to the real-time requirements and sufficient through-put of data.

The second issue is the level of interconnectedness and interdependency between critical infrastructures in the general society. AMI was introduced as a tool enabling real-time control of the SG, resulting in more efficient use of the grid and stability in the supply of energy. However, it may prove to be just as an efficient tool for adversaries with the intent of affecting both the control and stability of the grid and other dependent critical infrastructure. AMI will introduce new possibilities for both the SG operators, but also possibilities for malicious actors. The interconnectedness provided by the AMI in the SG may prove to incur vulnerabilities that can have catastrophic impact on the society as a whole when facing competent attackers with sufficient resources, intent and motivation. Due to the abovementioned challenges, an argument can be made to either limit the level of digitization of the grid and the use of AMI, or to always have analogue back-up solutions to ensure control of the grid and the stability of delivery, both in peace, crisis and war. As of today, this survey has not been able to identify solutions that feasibly addresses all of the different vulnerabilities and threats that is known in AMI, and certainly not those not yet discovered, and as such some of them can potentially affect the whole SG and other dependent critical infrastructures.

VII. Future work

Based on the vulnerabilities and threats discussed, it appears to be ample room for future research to be conducted in order to enhance information security in the AMI and SG. Research on these areas will be a continuous effort, and may aid in reducing the risk, but never remove it completely. Based on the findings in this survey some interesting topics could be:

- Continued research regarding the use of IDS in AMI, providing both sufficient security and cost-efficient solutions.
- The implementation of zero-trust within AMI.
- Developing cyber security strategies to combat coordinated attacks and employing a combination of security solutions.
- Research regarding privacy and security in a constrained environment, and how to account for both with real-time requirements.
- The standardization of crucial elements in the AMI.

- Secure communication protocols.
- Equipment and requirements to ensure a sufficient operational environment.
- How to assess the performance of IDS in AMI

Acronyms

AMI	Advanced Metering Infrastructure
BAN	Business Area Network
CCADS	Coordinated Cyber-Attack System
CIA	Confidentiality, integrity and availability
CPD	Cyber Physical Device
DER	Distributed Energy Resources
DR	Demand Response
DRMS	Demand Response Management System
DoS	Denial of Service
DDoS	Distributed Denial of Service
FAN	Field Area Network
HAN	Home Area Network
IAN	Industry Area Network
IADS	Intrusion Anomaly Detection System
ICS	Industrial Control System
IDS	Intrusion Detection System
LMS	Load Management System
LS	Load Shedding
NVE	Norges Vassdrags- og Energidirektorat (The Norwegian Water Resources and Energy Directorate)
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PLC	Power Line communication
SCADA	Supervisory Control and Data Acquisition
SEP	Smart Energy Profile
SMDC	Smart Meter to Data Collector

References

[1] The Office of the Auditor General, "Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen," Riksrevisjonen, Oslo, 2021.

[2] Police Security Service, "National Threat Assessment 2020," PST, 2020. [Online]. Available: https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/. [Accessed September 2021].

[3] National Security Authority, "Risk 2020," 2020. [Online]. Available: https://nsm.no/getfile.php/131421-1587034764/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf. [Accessed September 2021].

[4] R. Mohassel, A. Fung, F. Mohammadi and K. Raahemifar, "A survey of advanced metering infrastructures," *International Journal of Electrical Power and Energy Systems,* vol. 63, pp. 473-484, 2014.

[5] 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.

[6] S. M. Jefferson, K. Petersen and E. Mendes, "Survey Guidelines in Software Engineering: An Annotated Review," in *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement,* New York, 2016.

[7] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews,* vol. 57, pp. 302-318, 2016.

[8] C.-C. Sun, A. Hahn and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018.

[9] J. Mendel, "Smart Grid Cyber Security Challenges: Overview and Classification," *E-Mentor,* vol. 2017, no. 1(68), pp. 55-66, 2017.

[10] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, 14 March 2020.

[11] 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.

[12] European Commission, "European Programme for Critical Infrastructure Protection," 12 December 2006. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260. [Accessed 02 November 2021].

[13] V. Namboodiri, V. Aravinthan and W. Jewell, "Communication needs and integration options for AMI in the smart grid," Power Systems Engineering Research Center, 2012.

[14] H. Farhangi, "Cyber-Security Vulnerabilities: An Impediment Against Further Development of Smart Grid," in *Smart Grids from a Global Perspective: Bridging Old and New Energy Systems,* Springer International Publishing, 2016, pp. 77-93.

[15] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Càrdenas and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in *IEEE Third International Conference on Smart Grid Communications (SmartGridComm),* 2012.

[16] C. J. Foreman and D. Gurugubelli, "Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure," *The Electricity Journal,* vol. 28, no. 1, pp. 94-103, 2015.

[17] 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.

[18] NIST, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," NIST, 2010.

[19] 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.

[20] A. V. Jha, B. Appasani, A. N. Ghazali, P. Pattanayak, D. S. Gurjar, E. Kabalci and D. K. Mohanta, “Smart grid cyber-physical systems: communication technologies, standards and challenges,” *Wireless Networks,* vol. 27, no. 4, pp. 2595-2613, 2021.

[21] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues,” *IEEE Communications Surveys Tutorials,* vol. 21, no. 3, pp. 2886-2927, 2019.

[22] NIST, “Standards for Security Categorization of Federal Information and Information Systems,” NSIT, 2004.

[23] X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, “IEEE Communications Magazine,” *Securing smart grid: cyber attacks, countermeasures, and challenges,* vol. 50, no. 8, pp. 38-45, 2012.

[24] S. Tweneboah-Koduah, “Evaluation of Cybersecurity Threats on Smart Metering System,” in *Information Technology - New Generations. Advances in Intelligent Systems and Computing,* Springer, 2017, pp. 199-207.

[25] R. . M. Lee, M. J. Assante and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” E-ISAC, 2016.

[26] J. Lui, Y. Xiao, S. Li, W. Liang and P. C. L. Chen, “Cyber Security and Privacy Issues in Smart Grids,” *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* vol. 14, no. 4, pp. 981-997, 2012.

[27] A. Anzalchi and A. Sarwat, “A survey on security assessment of metering infrastructure in Smart Grid systems,” in *SoutheastCon 2015,* 2015.

[28] S. Tweneboah-Koduah, “Evaluation of Cybersecurity Threats on Smart Metering System,” in *Information Technology - New Generations. Advances in Intelligent Systems and Computing,* Springer, 2017, pp. 199-207.

[29] NIST, “Cybersecurity framework,” NIST, April 2018. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed November 2021].

[30] D. Gunderman, “Bankinfosecurity,” Bankinfosecurity, 12 November 2021. [Online]. Available: https://www.bankinfosecurity.com/us-department-defense-to-launch-zero-trust-office-a-17905. [Accessed 20 November 2021].

[31] Electric Power Research Institute , “Report to NIST on the Smart Grid Interoperability Standards Roadmap,” NIST, 2009.