TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

ITI70LT

Eerik Till 106579IVCMM

ICT Risk Assessment of Smart Electricity Meters

Kaugloetavate elektriarvestite IKT riskianalüüs

Master’s thesis

Supervisor:	Prof. Jüri Vain, PhD Director of Department of Computer Science at TUT
Co-supervisor:	Kristjan Kuhi, MSc

Tallinn 2014

Declaration

I hereby declare that I am the sole author of this thesis. The work is original and has not been submitted for any degree or diploma at any other University. I further declare that material obtained from other sources has been duly acknowledged in the thesis.

……………………..   ……………………….

(Date)   (Author’s signature)

Annotation in English

In 2009 the European Commission ordered the Member States to roll out 80% of electricity smart metering systems by 2020 in positively evaluated regions aiming for improved energy efficiency. On the one hand, Advanced Metering Infrastructure two-way communication offers modern and convenient functionalities, such as remote reading of metered values and remote connect/disconnect of a meter. On the other hand, security of this ICT solution seems to have been an afterthought, as the European Network and Information Security Agency has highlighted the lack of risk awareness, regular risk assessments and even a good risk assessment methodology for the Smart Grid. Although ENISA created an inventory of risk assessment methods in 2006, the need for keeping the inventory of risk assessment methodologies up to date is evident.

The objective of the work is to select a risk assessment method suitable for quick analysis of the smart metering ICT security risks and provide prioritization of identified risks based on the chosen method. A selection of widely known risk assessment methodologies is compared from the suitability perspective for the scope of this thesis and a risk assessment is performed using the OCTAVE Allegro methodology. As a result, prioritization of the identified risks is provided based on the method and the most distressing areas of concern are highlighted, which could serve as a starting point for risk assessment initiatives in concerned organizations to prevent large scale cyber-attacks with possibly devastating consequences.

Annotation in Estonian

2009. aastal andis Euroopa Komisjon korralduse juurutada aastaks 2020 80% ulatuses intelligentsed elektri tarbimise mõõtesüsteemid sobivaks hinnatud riikides, et parandada energia efektiivsust. Ühest küljest pakub nüüdistasemel mõõtesüsteemi (Lehtla, 2013) kahesuunaline kommunikatsioon modernseid ja mugavaid võimalusi, nagu mõõtenäitude kauglugemine ja elektriarvestite kauglülitus. Teisalt jääb mulje, et antud süsteemi turvalisusele on hakatud mõtlema alles pärast süsteemi disainimist ja juurutamist, kuna Euroopa Võrgu- ja Infoturbeamet (ENISA) on rõhutanud riski teadvustamise, regulaarsete riskianalüüside ja tarkvõrgu jaoks sobiliku riskianalüüsi metoodika puudumist. ENISA lõi 2006. aastal riskianalüüsi meetodite kogu, kuid tänaseks on see aegunud ja vajab värskendamist.

Töö eesmärk on valida tarkvõrgu kiireks IKT riskianalüüsiks sobilik meetod ja valitud meetodi abil tuvastatud riskid prioritiseerida. Võrreldakse kuut laiemalt tuntud riskianalüüsi metoodikat antud töö skoobi sobivuse seisukohalt ning demonstreeritakse OCTAVE Allegro lähenemist. Tulemuseks on meetodi põhjal tuvastatud riskide prioritiseeritud järjestus ning välja on toodud antud analüüsi põhjal kõige põletavamad probleemid, mis võiksid pakkuda lähtepunkti teemast huvitatud organisatsioonidele, et ennetada laiapinnalisi küberrünnakuid, mille tagajärjed võivad olla laastavad.

Table of Contents

Declaration 2

Annotation in English....3

Annotation in Estonian....4

Table of Contents 5

List of tables....7

List of figures 9

Abbreviations 10

1 Introduction....11

2 Overview of smart metering 13

2.1 Communication technologies 15

2.1.1 Wired technologies....15

2.1.2 Wireless technologies....17

3 Overview of risk management....19

4 Risk assessment methods....21

4.1 Overview of risk assessment methods....22

5 Security risk assessment using OCTAVE Allegro method 27

5.1 Establishing risk measurement criteria....27

5.1.1 Defining a qualitative set of risk measurement criteria....27

5.2 Developing an information asset profile 29

5.2.1 Identifying collections of information assets 29

5.2.2 Identifying critical information assets....30

5.2.3 Critical information asset profiling 30

5.3 Information asset containers....32

5.4 Identifying areas of concern 35

5.5 Threat scenarios....35

5.6 Identifying risks....36

5.7 Analyzing risks....36

5.7.1 Meter Reading message 37

5.7.2 End Device Control message 41

5.7.3 End Device Event message 43

5.7.4 Master Data Management and Data Linkage message 44

5.7.5 Payment Metering Service message 45
5.7.6 Meter configuration 46
5.7.7 DC configuration 47
5.7.8 Historical readings in meter memory 49
5.7.9 Historical readings in DC memory 50
5.7.10 Alarms/events in meter memory 51
5.7.11 Meter firmware 52
5.7.12 DC firmware 53
5.7.13 Meter encryption key 54
5.7.14 DC encryption key 55
5.8 Selecting mitigation approach 56
6 Conclusion 59
References 60

List of tables

Table 1 Risk assessment methods comparison....25

Table 2 Risk measurement criteria....27

Table 3 Risk criteria impact area ranking....28

Table 4 Meter Reading and End Device Control information asset profiling....31

Table 5 Information asset risk environment map (technical)....32

Table 6 Information asset risk environment map (physical)....33

Table 7 Information asset risk environment map (people)....34

Table 8 Meter Reading information asset disclosure risk....37

Table 9 Meter Reading information asset modification risk....38

Table 10 Meter Reading information asset interruption risk....40

Table 11 End Device Control information asset disclosure risk....41

Table 12 End Device Control message information asset modification risk....42

Table 13 End Device Event information asset disclosure and modification risk....43

Table 14 Master Data Management information asset disclosure and modification risk....44

Table 15 Payment Metering Service information asset modification risk....45

Table 16 Meter configuration information asset disclosure and modification risk....47

Table 17 DC configuration information asset disclosure and modification risk....48

Table 18 Historical readings in meter memory information asset disclosure risk....49

Table 19 Historical readings in DC memory information asset disclosure risk....50

Table 20 Alarms/events in meter memory information asset disclosure and modification risk....51

Table 21 Meter firmware information asset disclosure and modification risk....52

Table 22 DC firmware information asset disclosure modification risk....53

Table 23 Meter encryption key information asset disclosure risk....54

Table 24 DC encryption key information asset modification risk 56

Table 25 Relative risk matrix 57

Table 26 Mitigation approaches per pool..57

Table 27 Risk prioritization and mitigation strategy...58

List of figures

Figure 1 End-to-End smart grid communications model (IEEE, 2011) 13

Figure 2 PLC communication topology (Landis+Gyr, 2012) 17

Abbreviations

AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading, included in AMI
CIS	Customer Information System
DC	Data Concentrator
DDoS	Distributed Denial of Service (attack)
DSO	Distribution System Operator
ENISA	The European Network and Information Security Agency
HES	Head-End System
IA	Information Assurance
ICT	Information and Communication Technology
IED	Intelligent Electronic Devices
IT	Information Technology
NIC	Network Interface Component
NIST	National Institute of Standards and Technology
P2P	Point-to-Point Communication
PLC	Power Line Communication
RA	Risk Assessment
RM	Risk Management
SLA	Service Level Agreement

1 Introduction

The European Union has taken a commitment in Energy Efficiency Plan 2011 of saving 20% of its primary energy consumption compared to projections by 2020 as a major step towards achieving long term energy and climate goals (European Parliament, 2009). Energy efficiency is one of the cheapest ways to reduce greenhouse gas emissions. According to studies based on real power-consumption data for more than 800 000 United States utility customers, smart grids could cut as much as 115 145 MW off-the-peak, translating to approximate savings of $120 billion (Jackson, 2009). In section 6 of the European Union (EU) Energy Efficiency Plan it is stated that consumer devices – such as smart meters – play a great role in optimizing energy consumption and potentially allow cost savings, as currently only 47% of consumers are aware of how much energy they consume. In 2009 the Commission obliged Member States to assess the roll-out of smart metering systems as a primary measure towards the implementation of smart grids and to launch roll-out in 80% of those regions that have been positively evaluated.

The Plan also foresees that smart grids and smart meters will provide a backbone for smart appliances and new services will be offered to customers to track their energy consumption down to every single appliance. The aim is to enable consumers to save costs during off-peak hours via cheaper energy by, for example, remotely switching appliances on and off. While this may seem as a potential perspective for gaining control over energy consumption in households, it does raise questions whether the smart meters and smart grids are secure enough to handle such critical functions. Vulnerabilities of information technology and communication systems may be abused for financial and political motivation to shut off power to large areas (ENISA, 2012). The roll-out of smart meters in several European countries and publicly known smart grid security breaches create motivation for analysis of the currently known risks embedded in such a smart grid.

ENISA has claimed one of its main objectives to raise awareness of the fact that Risk Assessment if often not performed, even if Risk Management is implemented (ENISA, 2012). Assessing risks and identifying technological gaps are some of the essential challenges that the smart grid will face in the coming years. Raising awareness and knowledge sharing among all the actors are urgent measures needed in this critical information infrastructure to set the ground for making security a top priority. Cyber security is normally considered as an important issue in any smart grid project. However, when it comes to practical implementation, then security is often ignored because of project budgets and lack of expertise.

The analysis begins with giving an overview of the smart metering solution in Section 2 and risk management concepts in Section 3. It is followed by comparison of a selection of well-known risk assessment methodologies in Section 4. In Section 5 the risk assessment methodology OCTAVE Allegro is introduced and implemented. Finally, conclusions are made in Section 6 based on the outcome of the risk assessment.

2 Overview of smart metering

In order to denote areas of advanced metering Information and Communication Technology (ICT) security concerns an overview of the smart grid model, components and mostly used communication methods is provided in this section. In the perspective of energy transmission, smart grid consists of four functional domains, including bulk generation, transmission, distribution and customer, as shown in figure 1 (IEEE, 2011). The transmission system refers to the high-voltage network infrastructure that connects the power generation facilities with the various distribution points (Hossain *et al.*, 2012). At the distribution points the electrical carrier is converted to medium and low-voltage (LV) signals for the distribution systems that connect the customers.

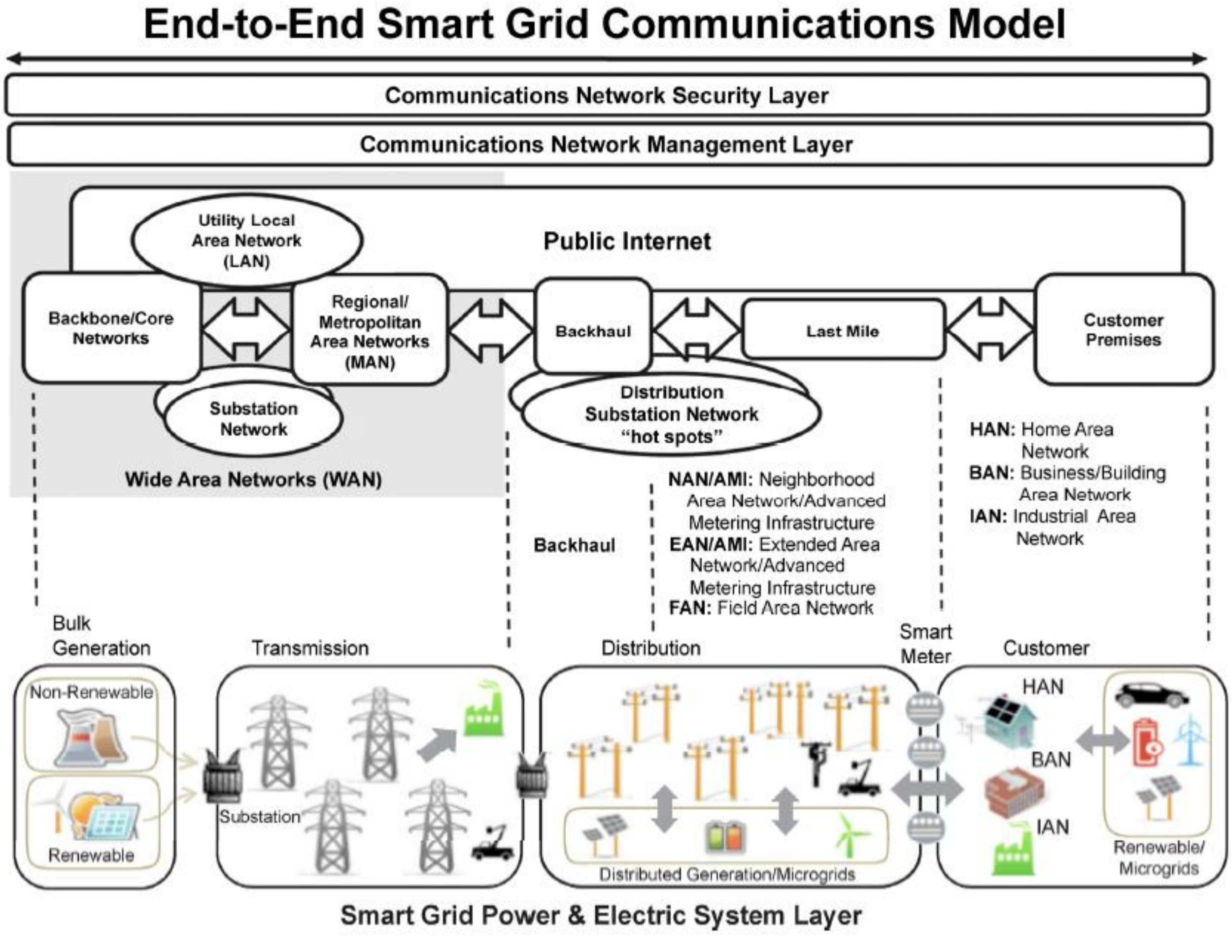
End-to-End Smart Grid Communications Model
Communications Network Security Layer
Communications Network Management Layer
Utility Local Area Network (LAN)
Public Internet
Backbone/Core Networks
Regional/ Metropolitan Area Networks (MAN)
Backhaul
Last Mile
Customer Premises
Substation Network
Distribution Substation Network "hot spots"
Wide Area Networks (WAN)
Backhaul
NAN/AMI: Neighborhood Area Network/Advanced Metering Infrastructure
EAN/AMI: Extended Area Network/Advanced Metering Infrastructure
FAN: Field Area Network
HAN: Home Area Network
BAN: Business/Building Area Network
IAN: Industrial Area Network
Bulk Generation
Transmission
Distribution
Smart Meter
Customer
Non-Renewable
Renewable
Substation
Distributed Generation/Microgrids
HAN
BAN
IAN
Renewable/ Microgrids
Smart Grid Power & Electric System Layer

Figure 1 End-to-End smart grid communications model (IEEE, 2011)

The distribution domain includes distribution feeders and transformers to transmit electricity to customers and provides two-way communication between smart meters and local utility centers (i.e., data concentrators) to convey information of power usage, control and pricing (Meng *et al*., 2014). Some data are transmitted in a periodic manner, such as power consumption data of households, while other data must be transmitted in a timely manner, such as controlling or monitoring data.

A *smart grid* is an upgraded power grid depending on two-way digital communication between supplier and consumer that successively give support to intelligent metering and monitoring systems (ENISA, 2012). *Automated Meter Reading* (AMR) is the technology of automatically collecting diagnostic, consumption and status data from energy metering devices and forwarding the gathered data to a central database for troubleshooting, billing and analyzing. *Advanced Metering Infrastructure* (AMI) differs from AMR in that it allows bi-directional communication with the meter (Fang *et al*., 2012). *Smart meters* are electricity meters with added communication module in order to be connected to the AMI network and thus have to integrate basic security features such as authentication and encryption.

The Meter Data Management (MDM) system is a system comprised of several components, of which the customer records database is one of the most important. This database allows the Distribution System Operator (DSO) to manage large amounts of data generated by the meters under the control of the utility. Other processes which are managed by the MDM include managing the transmission of data records from the smart meters up to the back-office where the MDM is located, the storage process, protecting their privacy and integrity, as well as making all these data accessible to third parties such as energy marketers and retailers or energy services providers. To this respect, the MDM has to validate and provide the necessary mechanisms to guarantee that AMI data is complete and accurate despite disruptions in the communications network or at customer premises. (ENISA, 2012)

In 2011, Communication COM(2011) 163 (7) from the European Commission summarized the achievements of Critical Information Infrastructure Protection plan. Emergence of new threats was also recognized, bringing Stuxnet as an example (Falliere *et al.*, 2011), and that smart grids can be affected by complex and targeted cyber-attacks with disruptive purposes. In Communication COM(2011) 202 (1) “Smart Grids: from innovation to deployment” the Commission identified challenges in smart grid deployment and proposed to focus on, among other things, developing technical standards, ensuring data protection, and offering support to innovation for technology and systems.

2.1 Communication technologies

The *last-mile connection* refers to delivering connectivity from the communication provider to a customer (Hossain *et al*., 2012). In smart grid it usually means connecting the substation and customer premises to the high-speed communication core network. Many communication technologies can be used in this last-mile connection. The main focus here is on the two communication technologies being used in European smart meter rollouts: Power Line Communication (PLC) and Point-to-Point (P2P) over cellular network (Landis+Gyr, 2012). However, a variety of other communication technologies exist, which are briefly described in subsections 2.1.1 and 2.1.2.

Running a smart grid solution places requirements regarding the latency, bandwidth and reliability on the communication medium. An on-demand meter reading message is typically 100 bytes in size and requires latency of less than 15 seconds and high reliability of more than 98% (success over a day), whereas a scheduled interval reading may be 1600 – 2400 bytes in size with latency requirement 4 – 6 hours. Firmware updates, however, have latency requirement between 2 seconds to 7 days, as the typical data size is 400 000 – 2 000 000 bytes (Kuzlu *et al*., 2014). Meter remote disconnect is typically 20 bytes in size and tamper notification 64 bytes, while both have delay objective below 2 seconds (Luan *et al*., 2010).

2.1.1 Wired technologies

Dedicated wireline cables could be used to build reliable data communication networks, but the investment cost would be considerable for building up a new infrastructure. The wireline networks include SONET/SDH, Ethernet, DSL and coaxial cable access network. SONET/SDH networks route data packets through high-speed optical fibers with supported data rates between 155 Mbps and 160 Gbps, but are also the most expensive to build. Ethernet is popularly used in homes and workplaces, allowing data rates between 10 Mbps and 10 Gbps. DSL and coaxial mediums allow transmitting data up to 10 Mbps. (Wang *et al*., 2011)

Power Line Communication (PLC) is a widely known and tested communications technology that was at first used for telemetry purposes (Landis+Gyr, 2012). In the late 1990s, energy utilities set out to use PLC technology in the smart metering rollouts, which has turned it into the dominant smart metering communications technology in Europe. PLC physical layer standards utilize either Spread-Frequency Shift Keying (SFSK) or Orthogonal Frequency Division Multiplexing (OFDM) technology. Recent PLC networks employ OFDM modulation in order to increase data throughput rates, efficiency and reliability in implicitly noisy environments like electric grids (Texas Instruments, 2014).

The IEC 61334 standard uses SFSK and is available in band 60-76 kHz contained in CENELEC-A band (CENELEC-A 3-95 kHz is reserved exclusively for energy providers) and provides data rates 1,2 kbps for PLAN and 2,4 kbps for PLAN+. Usually the live and neutral cables are used as the PLC transmission channel, which resembles a close form of the two-wire communication line (Meng *et al.*, 2004). Standards based on OFDM include PRIME (PoweRline Intelligent Metering Evolution), which was designed for low voltage (LV) lines with low noise and targets higher data rates 21-128 kbps while occupying band 42-90 kHz, whereas G3 was designed for medium voltage lines with lower data rates 2.4-34 kbps and occupies band 35-90 kHz. The fastest among OFDM standards is broadband PLC P1901 / G.9960, which occupies band 2-30 MHz and provides data rates higher than 100 Mbps.

PLC refers to transmitting data by modulating the standard 50 or 60 Hz alternating current on the existing electrical power lines (Hossain *et al*., 2012). Normally data signals cannot spread through transformers and therefore PLC is limited within each line segment between transformers. The smart meters in PLC network communicate with Data Concentrator (DC), as shown on figure 2. DC typically sends out discovery messages to the network every hour in order to establish connections with newly installed devices (Wang *et al*., 2011). DC is an Intelligent Electronic Devices (IED) that acts as a gateway between MDM and smart meters (ENISA, 2012).

One of the main advantages of using power line network as a communication channel is that the power network reaches every socket in every house, therefore it is a cost effective way of building the communication infrastructure as it uses existing power lines. However, LV power lines present an extremely harsh environment for the high-frequency communication signals. The three critical channel parameters noise, impedance and attenuation are found to be highly unpredictable and hinder reliable communication (Meng *et al.*, 2004). In addition, devices are randomly being plugged and unplugged from the electrical network, making line impedance strongly dependent on frequency and time. Lastly, data sent from one element of the local LV network are visible at all the other components, which can be a potential security risk (Huczala *et al*., 2006).

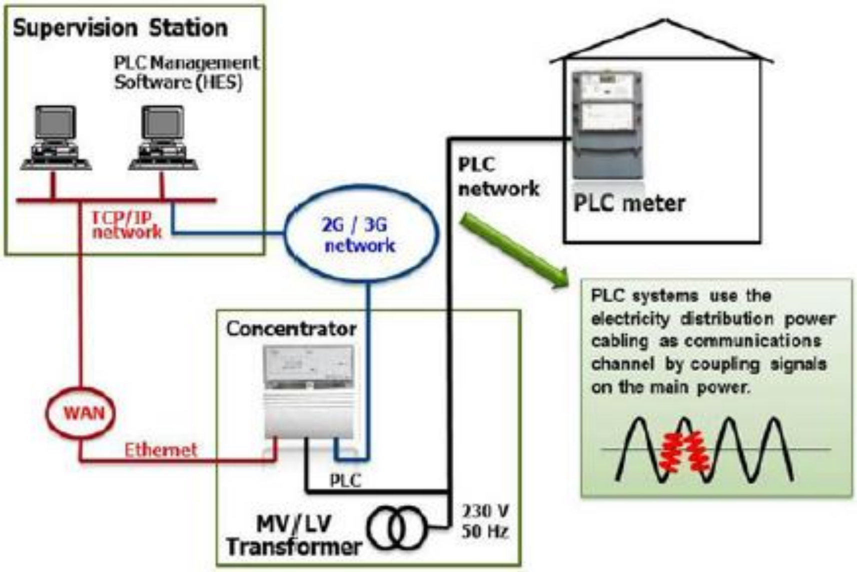
Supervision Station
PLC Management Software (HES)
TCP/IP network
2G / 3G network
PLC network
PLC meter
PLC systems use the electricity distribution power cabling as communications channel by coupling signals on the main power.
Concentrator
WAN
Ethernet
PLC
MV/LV Transformer
230 V 50 Hz

Figure 2 PLC communication topology (Landis+Gyr, 2012)

2.1.2 Wireless technologies

In order to provide connectivity in areas with low density of population, where implementation of PLC is not feasible due to attenuation issues, a dedicated or shared cellular network infrastructure could be considered. Shared network infrastructure may demand accepting restrictions on Quality of Service due to non-exclusive usage of the medium. On the other hand, it uses an already established and working infrastructure as opposed to dedicated cellular network. (Müller *et al*., 2012)

For home area applications IEEE 802.11 WiFi and 802.15 ZigBee networks could be utilized for low cost data exchange providing maximum data rates up to 150 Mbps with maximum distance up to 250 meters or 20 kbps to 55 Mbps with distance of 10 meters respectively. Utilizing these two standards, wireless mesh has been the winning technology in the US and Australia while gaining interest in Europe as it is easy-to-deploy, self-healing due to redundancy and imposes lower costs. For broadband wireless Internet access, 802.16 networks can provide data transfer rates up to 100 Mbps in a range of 50 km. (Wang *et al*., 2011)

Among wireless technologies, cellular solutions for P2P communications with individual meters are often used in Europe. Today primarily second-generation 2G and third-generation 3G cellular technology options are used. Most cellular P2P smart metering infrastructures utilize Global System for Mobile Communications (GSM) networks and the General Packet Radio Service (GPRS) data service. New cellular smart metering infrastructures are likely to make use of more bandwidth and higher connection speeds of Enhanced Data Rates for GSM Evolution (EDGE) technology. The higher data rates of 3G are mostly needed for connecting data concentrators to the HES, while for small messages 3G is an unnecessary expense. The main benefits of cellular technology are that the network deployment can be outsourced and implementation is fast due to existing cellular network, global coverage and proven technology. (Pauzet, 2010)

In general, wireless signals are significantly subject to transmission attenuation, environmental interference and security issues due to the shared and accessible nature of the medium. As a result, wireless networks typically allow short distance connections with relatively low data rates (Wang *et al*., 2011). An additional concern is the impact of increasing number of smart grid entities on voice data on the same cell. Blocking probability of machine-to-machine traffic increases significantly with very high cell load (above 95%) on a specific network cell. It is noted, however, that at least initially smart meter traffic would utilize a small percentage of resources, in case LTE is used, and that the application would rather be coverage limited than capacity limited (Souryal *et al*., 2011). Nevertheless, simulation results have shown that delays start to accumulate substantially when the number of smart meters increases, which may create a need for the prioritization of metering messages and control commands (Salam *et al*., 2012).

3 Overview of risk management

Every organization is exposed on a daily basis to an endless number of novel or changing threats that may affect its operation or the fulfillment of its objectives (ENISA, 2006). Identification, analysis and evaluation of these threats are the only way to understand and measure the risks involved. If for no other reason, many organizations obtain a security risk assessment simply because it is required by regulations, such as HIPAA, GLBA, FERC Cyber Security Standards, ISO 17799, OMB A-130 (Landoll, 2005).

Asset is anything that has value to the organization. It can be a tangible or intangible component of an information system. *Threat* is any action or event with the potential to lead to damage. Threats have the following categories: environmental, organizational, human errors, technical failures and deliberate acts. Sources of threats could be espionage, vandalism or just accidents or human mistakes. In the first two cases the criticality of the threat can result from two main factors: the motivation of the threat and the attractiveness of the asset, which can be considered high in the smart grid domain. *Vulnerability* is a weakness of an asset that could be taken advantage of by one or more threats. (ENISA, 2006)

Several experts in the smart grid field consider that DSOs should be obliged to conduct mandatory risk assessments to indicate the most critical assets and threats, which should be based on a formal methodology. However, experts claim that there is no good methodology for assessing risks of the smart grid. (ENISA, 2012)

In 2006 the Technical Department of ENISA Section Risk Management identified problems at the European level (ENISA, 2006):

1. Low awareness of risk management (RM) activities within public and private sector organizations was brought out, as organizations implementing RM often tend to neglect risk assessment (RA).
2. Lack of a “common language” in RM domain to facilitate communication among stakeholders was highlighted, as RM terms are used with different meanings in various standards, best practices and tools.
3. Although many methods and tools are available in this domain, there were no inventories that were structured based on a set of common properties.

4. Lack of interoperability of RM solutions and difficulties in integration of RM and RA with corporate governance is pointed out. This gave ENISA the motivation to create such an inventory.

4 Risk assessment methods

A risk assessment based on formal methodology is appropriate if an organization has IT systems with moderate or high criticality to the business (ENISA, 2006). Even though the necessity for regular risk assessments is acknowledged, there is still no consensus on a proper formal methodology for carrying out the assessments in the smart grid realm. In this section a selection of risk assessment methods will be compared for the suitability of being performed by an individual with the level of smart grid expertise that can be obtained from currently available material on the topic and without access to specific financial figures for determining cost values.

In 2006, ENISA created an online inventory of 17 risk management/risk assessment methods, which does not even cover all methods and standards dealing with IT risks (ENISA, 2014). A template with 21 attributes was used in order to describe each of the methods. The template highlights the risk assessment phases supported: risk identification, risk analysis and risk evaluation. In addition, the scope section defines most suitable target organizations, geographical prevalence and level of detail. Lastly, the users viewpoint is analyzed as to the skills needed to perform the assessment, external consultancy necessity, regulatory and IT standards compliance, tools supporting the method, organization processes integration and whether the method allows use of sector adapted knowledge databases.

A risk assessment methodology typically includes a risk assessment process, an explicit risk model defining key terms, an assessment approach (e.g., quantitative, qualitative), and an analysis approach (e.g., threat-oriented, asset/impact-oriented or vulnerability-oriented) (NIST, 2012):

- Quantitative assessments typically employ a set of methods or principles for assessing risks based on the use of numbers. This type of assessment supports cost-benefit analysis of alternative risk responses most effectively. However the meaning of the results may not always be clear and determining exact cost may be time-consuming and costly.
- Qualitative assessments, on the other hand, employ a set of methods based on non-numerical categories or levels. This type of assessment supports communicating risk results to decision makers. However, due to the subjectivity of experiences, different assessors will produce different qualitative results.

- Semi-quantitative assessments use bins, scales or representative numbers. The bins or scales translate easily into qualitative terms, while also allowing relative comparisons between values in different bins or within the same bin, which also allows relative prioritization among results than in purely qualitative approach.

For this analysis, the main criteria for selection of methodology are:

- Cost, which should be free of charge, due to limited resources of an university student;
- Approach, either qualitative or semi-quantitative, as quantitative can be too cumbersome, especially for an individual with limited timeframe, in addition to the difficulty of determining exact costs;
- Level of expertise needed to implement the method, which should not be a specialist level and should not require external consultancy;
- Documentation available in English;
- Volume of assessment and assessment team setup suitable to be carried out by an individual.

The outlined criteria are relatively robust and pragmatic but sufficient for wide spectrum of practical cases to be able to complete the steps of a formal risk assessment method with limited resources. Large corporations would probably define a different set of criteria for risk assessment method selection. The following is in a way an arbitrary array of some of the risk assessment methods outlined in ENISA online inventory (ENISA, 2014), as well as some additional methods not specifically mentioned in the inventory. However, ENISA inventory of risk assessment methods feels outdated, e.g. many of the links to method vendors are broken, and seems as if the information has not been updated since 2006.

4.1 Overview of risk assessment methods

CRAMM (CCTA Risk Analysis and Management Method) was initiated by British Central Communication and Telecommunication Agency (CCTA). It is a qualitative risk analysis and management tool developed to provide public sector’s institutions with a method for IT systems security evaluations and to examine conformity to BS7799 (the British standard for information security management). The downside of implementing CRAMM methodology is that the CRAMM tool requires trained and experienced users of the tool. Moreover, CRAMM is focusing on managerial level at its risk assessment, thus system specific technical vulnerabilities are not addressed by the tool. (Yazar, 2002)

HMG Information Assurance Standard No.1 (IS1) provides a process for identifying and assessing the technical risks that an ICT system, handling, storing and processing government information, is exposed to, but is also recommended to wider Public Sector. The key output is a list of prioritized risks that can be used as a foundation for risk handling requirements and options for managing the risks. The included definitions of Business Impact Levels are aligned with a number of UK sectors, such as military, economy and the Critical National Infrastructure. The HMG IA Standard No.2 Risk Management and Accreditation of ICT Systems and Services (IS2) describes the risk management lifecycle. Appropriate application of the methodology will require a high level of skill, judgment and experience in the field of Information Assurance (IA). (CESG, 2009)

RiskSafe Assessment is a cloud-based qualitative risk assessment tool that is fully compliant with ISO 27001 (Platinum Squared, 2014). This method aims to build on the strengths of CRAMM while incorporated in a software tool that has been built using modern technology and can be offered as a “software as a service” solution. RiskSafe Assessment provides a method which allows users to analyze systems in a fashion that is consistent with the approach set out by IS1&2 and its supplement. RiskSafe Assessment supports an established method for business impact assessment and threat and vulnerability assessment (ENISA, 2006). In addition to risk identification phase, risk analysis and risk evaluation are also covered in this risk assessment method. The most appropriate types of organizations for this method are large and small companies, as well as governmental agencies. Users from management, operational and technical domains are targeted by the method and no particular skills are needed to introduce this method. However, the access to the cloud-based tool requires a subscription and is not free of charge.

The US National Institute for Standards and Technology (NIST) Special Publication 800-30 gives very detailed guidance and identification of what should be reflected on in risk management and risk assessment in computer security. There are detailed checklists, graphics and formulas, as well as references that are primarily based on US juridical issues. The method is targeted at large as well as small enterprises and governmental agencies and users mainly from operational and technical domains. SP800-30 is free to use and standard level of skills is suggested in order to introduce this method. (ENISA, 2006)

IT-Grundschutz (IT Baseline Protection Manual), conceived by German Federal Office for Information Security (BSI) for public authorities in 1994, allows an organization a quick entry into establishing an information security management system and securing IT systems and protecting information on the basis of best practices. The method covers not only technical but also organizational, human and structural aspects, so that a security level appropriate and adequate for normal requirements can be reached quickly and economically. In many projects with service providers from the private sector, German authorities demand the implementation of IT-Grundschutz. The standard presents a suitable risk analysis method for organizations operating according to IT-Grundshutz, which complicates using this method in an organization where IT-Grundshutz is not followed in processes and daily operation. (BSI, 2013)

The OCTAVE Allegro method is a trimmed version of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method that addresses information assets. The current OCTAVE Allegro approach, where allegro means quickly, is designed to allow extensive assessment of an organization’s operational risk domain with the aim of providing more pragmatic results without the need for detailed risk assessment expertise. Like previous OCTAVE methods, developed by the Carnegie Mellon Software Engineering Institute, OCTAVE Allegro can be performed in a collaborate workshop-style, but also meets the requirements of individuals who want to conduct a risk assessment without substantial organizational involvement, competence or input. The ability to connect organizational targets to IT security objectives is the key advantage of OCTAVE. Moreover, the collaborative aspect provides an interdisciplinary perspective to the risk identification, assessment and mitigation processes. (Caralli *et al*., 2007)

OCTAVE Allegro is most suitable of the described risk assessment methods due to its focus on the information assets and ability to provide risk prioritization quickly via its semi-quantitative nature. Concentrating on information assets successfully limits the amount of data that must be gathered, processed, organized, analyzed and understood, which has been an impediment in moving forward with analyzing and mitigating risks for many organizations so far. In addition, there is no requirement that the organization processes should follow a specific framework in order to perform risk assessment based on this method. It is also important that Allegro method is developed rather recently compared to the other methods, while being free of charge and building on the experience and lessons learned from the earlier OCTAVE methods. The novelty of the method also means that the recent changes in the landscape of information security risks that must be managed by organizations have been considered compared to most of the older methods outlined here. Lastly, the reduced training requirements and number of worksheets to be filled in ease the implementation of the method by an individual researcher.

Table 1 Risk assessment methods comparison

	CRAMM	**IS1**	**RiskSafe**	**NIST SP800-30**	**OCTAVE Allegro**	**IT-Grundschutz**
Origin	UK	UK	UK	US	US	Germany
Analysis approach	Qualitative	Qualitative	Qualitative	Qualitative	Semi-quantitative	Qualitative
Suitable for assessment by an individual	No, requires consultant	No	No, different roles in software	No, defines various roles	Yes	No, due to volume of material and limited time
Suitable for SME	No	Yes	Yes	Yes	Yes	Yes
Expertise level required	Specialist	IA practitioner	Standard	Standard	Standard	Standard
Available in languages	EN, NL, CZ	EN	EN	EN	EN	DE, EN
Cost	Not free	Free	Not free	Free	Free	Free
Used in EU member states	Many	UK	UK	N/A	N/A	Many
Compliance to IT standards	ISO/IEC IS 17799	ISO 27001	ISO 27001 ISO 27005	N/A	N/A	ISO/IEC IS 17799 ISO/IEC IS 27001

	CRAMM	**IS1**	**RiskSafe**	**NIST SP800-30**	**OCTAVE Allegro**	**IT-Grundschutz**
Released (updated)	1985 (2003)	1998 (2012)	2012	2002	2007	1994 (2005)
Level of detail	Management, operational, technical	Technical	Management, operational, technical	Operational, technical	Management, operational	Management, operational, technical

5 Security risk assessment using OCTAVE Allegro method

In this paragraph the compulsory steps of OCTAVE Allegro method are followed step-by-step. As mentioned in paragraph 4.1, OCTAVE Allegro methodology focuses on information assets of the organization. It is also noted, that the assessment provides most utility when it is focused on the information assets that are most important to the organization (Caralli *et al*., 2007). Therefore the aim in this work is not to outline a full plethora of (information) assets in a smart metering ICT solution, but rather to analyze a selection of the essential information assets that possess value for the utility organization.

5.1 Establishing risk measurement criteria

Risk measurement criteria should reflect management's risk tolerance and should be universally applicable across the organization for comparability. Risk measurement criteria are a set of qualitative measures against which the consequences of a realized risk can be assessed and lay the foundation of an information asset risk assessment. (Caralli *et al*., 2007)

5.1.1 Defining a qualitative set of risk measurement criteria

Risk measurement criteria are listed in table 2 and corresponding impact levels are described in columns. The impact areas of reputation, finance, productivity, safety and penalties are considered. A DSO's reputation can be damaged if the smart metering system is compromised. A compromise of the grid may lead to financial consequences or even loss of lives due the importance as well as hazardousness of electricity supply. Lastly, the longer the recovery of normal service takes, the more staff hours are spent on recovery actions and more financial indemnities have to be paid to customers for power outage.

Table 2 Risk measurement criteria

Impact area	Low	Moderate	High
Risk measurement criterion - Reputation			
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged and some effort is required to recover.	Reputation is irrevocably destroyed or damaged.

Impact area	Low	Moderate	High
Risk measurement criterion - Financial			
Operating costs	Increase of less than 10% in yearly operating costs.	Yearly operating costs increase by 10 to 20%.	Yearly operating costs increase by more than 20%.
Revenue loss	Less than 10% yearly revenue loss.	10 to 20% yearly revenue loss.	Greater than 20% yearly revenue loss.
Risk measurement criterion - Productivity			
Staff hours	Staff work hours are increased by less than 10% for 1 to 7 days.	Staff work hours are increased between 10% and 20% for 1 to 7 days.	Staff work hours are increased by greater than 20% for 1 to 7 days.
Risk measurement criterion - Safety			
Life	No loss or significant threat to customers' or employees' lives.	Customers' or employees' lives are threatened, but they will recover after medical treatment.	Loss of customers' or employees' lives.
Risk measurement criterion – Penalties			
Indemnity	Indemnities less than 1000 EUR have to be paid to customers.	Indemnities between 1000 EUR and 10 000 EUR have to be paid to customers.	Indemnities greater than 10 000 EUR have to be paid to customers.

The risk measurement impact criteria areas from table 2 are ranked in table 3, where the area with most significance has the highest ranking. Safety is given the highest rank as long periods of electricity outage may cause loss of lives, especially in hospitals. Safety is followed by financial, penalties, reputation and productivity criteria.

Table 3 Risk criteria impact area ranking

Priority	Impact areas
3	Reputation
4	Financial

Priority	Impact areas
1	Productivity
5	Safety & Health
2	Penalties

5.2 Developing an information asset profile

Information asset can be characterized as information or data that possesses value to the organization. Such assets may exist in physical form (on paper, discs or other media) or electronically (stored in databases, files or personal computers). An information asset profile is a characterization of an information asset expressing its unique qualities, features, characteristics and value. (Caralli *et al.*, 2007)

5.2.1 Identifying collections of information assets

Considering which information assets are of most value to the DSO in the domain between the Head End System (HES) server and a smart meter, the following assets could be noted. Information assets have been derived with the help of considering the European Commission report on the set of universal required functionalities of the smart meter (European Commission, 2011):

- Meter configuration
- Data Concentrator (DC) configuration
- Historical readings in meter memory
- Historical readings in DC memory
- Alarms/events in meter memory
- IEC61968-9 message types (Goodrich, 2011):
    - End Device Event message (outage and voltage threshold detection, tamper detection, meter health)
    - Master Data Management and Data Linkage message (initialization, synchronization, assign device ID, add to service and inventory, change customer information, configure objects)

    - Meter Reading message (set up meter reading schedules, perform all types of meter readings, e.g. on-demand or bulk)
    - End Device Control message (connect/disconnect, load control, demand reset and real-time pricing commands)
    - Meter Service Request message (includes MeterServiceWork item(s) due to adding new customer, removing customer, switching suppliers, etc.)
    - Metering System Event message (includes human-readable and more detailed problem description than End Device Event message)
    - Payment Metering Service message (typically prepayment meters and token vending machines)
- Meter firmware
- Meter encryption key
- DC firmware
- DC encryption key

5.2.2 Identifying critical information assets

Although most of the information assets outlined in previous section 5.2.1 are important for the functioning of the smart meters, the primary objective of the DSO is to get the meter readings from the meter and issue remote connect/disconnect commands (End Device Control) in order to save field service costs. The impact on the DSO would be adverse if these types of messages would be modified without authorization, lost in the communication channels or disclosed to unauthorized people and therefore a structured risk assessment should be performed on them (Premaratne *et al*., 2008). According to Allegro methodology, in the next steps only one critical information asset can be analyzed at a time (Caralli *et al*., 2007). For other critical information assets the profiling has to be done repeatedly for each asset.

5.2.3 Critical information asset profiling

Since various advanced metering message types have similar asset profiles, then profiling each message type separately will be skipped as it would not provide considerable additional value for the following analysis. Meter reading and End Device Control information assets are profiled in table 4. A similar profile can also be extended to firmware, memory contents and cryptographic keys of the AMI components, all of which are analogous in that they require confidentiality, integrity and availability, while integrity is the first priority.

Table 4 Meter Reading and End Device Control information asset profiling

<table>
<tr><th colspan="2">(1) Critical asset</th><th colspan="2">(2) Rationale for selection</th><th colspan="2">(3) Description</th></tr>
<tr><td colspan="2">Meter Reading message
End Device Control (disconnect/connect) message</td><td colspan="2">Obtaining automated readings is one of the main functions of smart meters. Therefore if readings cannot be retrieved from meter, then the AMR system loses most of its value. Whereas remote disconnect is one of the primary functionalities of AMI.</td><td colspan="2">Meter reading contains at minimum: unique meter ID (e.g. serial number), reading timestamp and the metered value.
End Device Control message includes meter ID and message type code (Goodrich, 2011).</td></tr>
<tr><td colspan="2"><b>(4) Owner</b>:</td><td colspan="4">DSO billing department</td></tr>
<tr><td colspan="6"><b>(5) Security requirements:</b></td></tr>
<tr><td colspan="2">☒ <b>Confidentiality</b></td><td colspan="4">Only authorized persons can read the information asset.</td></tr>
<tr><td colspan="2">☒ <b>Integrity</b></td><td colspan="4">Only authorized persons can edit the information asset.</td></tr>
<tr><td colspan="2">☒ <b>Availability</b></td><td colspan="4">This asset must be available (successfully retrievable from meter by HES) so that the maximum downtime in a year is less than 1.83 days meaning at least 99.5% availability.</td></tr>
<tr><td colspan="6"><b>(6) Most important security requirement:</b></td></tr>
<tr><td>□ <b>Confidentiality</b></td><td colspan="2">☒ <b>Integrity</b></td><td colspan="2">□ <b>Availability</b></td><td>□ <b>Other</b></td></tr>
</table>

Since meter reading messages contain the unique ID of a meter, the message can be tracked down to a physical person. Therefore the confidentiality of metering data has to be assured. The correctness of the meter reading values is most crucial, since this is the basis for billing the customers and modification of the metering values could lead to erroneous financial bills. The robustness or availability is also required as the availability is usually expected to be above 99%. On the contrary to typical IT security requirements, where availability and integrity security requirements are low to moderate and confidentiality requirement is high, in SCADA systems the integrity and availability requirements are higher than the confidentiality requirement (Yang *et al*., 2012).

5.3 Information asset containers

Containers describe the places where information assets are stored, transported and processed. The information asset inherits all the risks to the containers in which the information asset lives. (Caralli *et al*., 2007)

In the case of on-demand meter reading or meter remote disconnect the request is normally generated in Customer Information System (CIS) or by MDM system. CIS or MDM requests AMI Head-End (HES) to create an on-demand Read Request message, which is then sent to the Network Interface Component (NIC) of the corresponding meter unit via the AMI network, containing DC in case of PLC. NIC relays the on-demand read request to the meter metrology board, which retrieves the meter reading and returns it to the NIC. The meter reading travels then via AMI network to the AMI HES and from HES to CIS. End Device Control messages follow the same chain of components, while firmware updates, configuration changes and cryptographic key handling are initiated from HES. (Simmins *et al*., 2011)

The steps involving internal and external technical containers are outlined in table 5. When some parts of the AMI network are outsourced, then third party service providers manage the containers that contain the information assets and they may not be aware of the security requirements of the assets (Caralli *et al*., 2007). Other information assets, besides on-demand meter reading and remote disconnect are processed, transferred and stored in the same containers. They mostly differ in which container they are initiated from and what is the final container. For example, End Device Event is initiated by the meter and usually terminates at the operational data store (Mullenmaster *et al*., 2011), while meter or DC firmware update can be initiated from the AMI HES or by a field technician over meter's optical port using vendor meter programming tool (Simmins *et al*., 2011).

Table 5 Information asset risk environment map (technical)

Internal		
#	**Container description**	**Owner**
1	Meter's NIC transfers the meter reading message from meter metrology board to AMI network.	Operations

#	Container description	Owner
2	Data Concentrators aggregate PLC meter reading messages and may cache the readings in memory.	Operations
3	HES communication servers mediate meter reading messages.	IT
4	HES processes meter reading messages.	Operations
5	HES stores the meter readings in database.	IT
6	MDM system processes meter reading messages.	Operations
7	CIS system generates invoices based on meter reading messages.	Billing
8	MDM, AMI HES and CIS systems run on (dedicated) servers.	IT
External		
#	**Container description**	**Owner**
1	P2P meter reading messages are transferred via telecom operator's switches and base stations.	Telecom operator
2	PLC meter reading messages are transferred via electrical cables and telecom operator's switches and base stations.	DSO, telecom operator

Containers are mostly of technical kind, but in case the information object is stored in physical form, such as on paper, then physical aspect has to be considered as well. Since meter reading messages, as well as other types of messages outlined in Section 5.2.1, are not stored on paper, then the list of physical containers in table 6 is rather short. When servers' backup tapes are managed by third party suppliers, then it is important to ensure that the tapes are handled according to the security requirements of the information assets that are stored on the tapes. One exclusion could be devices' firmware which is sometimes initially published on manufacturer's website, thereby turning the website into an asset container as well.

Table 6 Information asset risk environment map (physical)

Internal		
#	**Container description**	**Owner**
1	N/A (no physical copies are typically stored due to the high volume of messages)	N/A

External		
#	**Container description**	**Owner**
1	Servers' backup tapes are managed and stored by a third party.	Third party backup provider
2	Firmware may be available on manufacturer's website.	Device manufacturer

When internal or external persons become aware of the meter reading data in the messages or configurations of devices, then they become information containers as well. In our scenario a disgruntled employee or an outsider could intercept the metering messages or a customer service agent may initiate an on-demand reading out of personal interest when there is no actual business need for it. The human containers are brought out in table 7.

Table 7 Information asset risk environment map (people)

Internal personnel		
#	**Name or role/responsibility**	**Department or unit**
1	System administrators can monitor/intercept meter reading messages on communication servers, in MDM or AMI HES.	IT
2	CIS users may request on-demand readings for interesting customers without necessity.	Customer support
External personnel		
#	**Contractor, vendor, etc.**	**Organization**
1	Telecom operator's personnel having access to base stations can intercept meter reading messages (C4 Security, 2012).	Telecom operator
2	An attacker with appropriate hardware could intercept PLC or P2P traffic on the power cables or mobile network.	An individual
3	A sub-contractor's troubleshooting engineer could intercept PLC traffic while analyzing noise on the cables.	Sub-contractor
4	A sub-contractor's engineer might know devices' configurations by heart.	Sub-contractor

5.4 Identifying areas of concern

Areas of concern are possible conditions or situations that can threaten an organization's information asset. Risk in OCTAVE Allegro is a combination of a threat (a condition) and the resulting impact of the threat if acted upon (a consequence) (Caralli *et al*., 2007). Although smart meters are physically located in customers' premises and out of control of the DSO, the risk of physical tampering is typically mitigated by sealing the meter case, while AMI adds additional tampering events monitoring functionality (McLaughlin *et al*., 2010). Security of the DCs is usually provided by locking of substation housing, but motivated attackers will inevitably find their way past these physical safeguards.

5.5 Threat scenarios

The areas of concern recorded in the previous step are developed into threat scenarios that further detail the properties of a threat and additionally a broad range of other threats are considered (Caralli *et al*., 2007). This step involves identifying possible threat scenarios and determining their probability in Information Asset risk table (tables 8-24) column (6). Since there is not much experience in the probabilities and consequences of various advanced metering threats, then different risk assessments can have different estimations. The Allegro method provides four threat trees to simplify identification of a broad range of threat scenarios. The threat scenarios extracted from the areas of concern relate to a branch in these threat trees:

1. Human actors using technical means
    - Inside or outside
        - Accidental or deliberate
            - Disclosure, modification, interruption, destruction/loss
2. Human actors using physical means
    - Inside or outside
        - Accidental or deliberate
            - Disclosure, modification, interruption, destruction/loss
3. Technical problems
    - Software defects, system crashes, hardware defects, malicious code
        - Disclosure, modification, interruption, destruction/loss
4. Other problems

        - Power supply, telecommunications, third-party, natural disasters
            - Disclosure, modification, interruption, destruction/loss

Threats could also be catalogued as conventional, including natural and accidental threats, and unconventional, including malicious threats and emerging threats. Bompard *et al*. (2013) define *conventional threats* to be the potential encounters that have endangered power systems for a long time, for example the development of power systems. Whereas *unconventional threats* are potential incidents that are becoming apparent or important lately due to the interior or exterior elements, such as terrorism, the evolution of power systems and the innovation of technology. As market penetration increases, so do the potential risks associated with the novel technology and unprecedented unconventional threats will likely emerge in the future (Rice *et al*., 2014). While natural threats inevitably impact the AMI, the focus here is on malicious and emerging threats.

As far as critical information infrastructure is concerned, new and technologically sophisticated threats have emerged (European Commission, 2011). Their global geo-political dimension is becoming progressively clearer and a trend towards using ICT for political, economic and military predominance can be observed. The European Commission even highlights destruction as a possible future threat emerging from smart grids.

5.6 Identifying risks

After identifying threats in the previous step, the consequences to an organization if a threat is realized are captured (Caralli *et al*., 2007). The consequences are described in Information Asset risk table (tables 8-24) column (7). According to OCTAVE Allegro the risk equation would be: Threat (condition) + Impact (consequence) = Risk, which correlates to [Section 5.4 and Section 5. 5] + [Section 5.6] = Risk.

5.7 Analyzing risks

A simple quantitative measure of the extent to which the organization is impacted by a threat is computed. The relative risk score is obtained by studying the extent to which the consequence of a risk affects the organization considering the relative importance of the defined impact areas, and the probability (Caralli *et al*., 2007). The relative risk score is calculated in Information Asset risk table (tables 8-24) based on impact area scores in column (8). While risks to the “dumb” grid are well known and there is a lot of experience in that field, smart metering is still a new era and most of the future threats are unknown at this point of time. It is claimed, however, that the probability of hacking the smart grid is 100% (Spoonamore *et al*., 2009). Thus most of the following risks are assumed to have high probability, which is also owing to the fact that it would be financially motivating to hack part of the critical information infrastructure, but also because there is little or no real world experience in analogous attacks to smart grids.

5.7.1 Meter Reading message

As customers do not want their electricity consumption to be revealed to other parties (NIST, 2010), then the privacy concern is described in table 8. In columns (1) to (7) of table 8 the first area of concern is described and developed into a threat scenario. In column (8) the risk measurement criteria from table 2 have to be considered when determining severity values. The score for each impact area is calculated by multiplying the impact area rank (from table 3) by the impact value. Impact values are assigned quantitative values as follows: High – 3, Medium – 2, and Low – 1. The relative risk score is calculated by totaling the impact area scores. In OCTAVE Allegro method the differences between risk scores are not considered. The aim is to prioritize different risks compared to each other (Caralli *et al*., 2007).

Table 8 Meter Reading information asset disclosure risk

Information Asset Risk	**Threat**	Information asset	Meter reading message		
		Area of concern	An individual with suitable PLC equipment can intercept the meter reading messages in an apartment building.		
		(1) Actor	An individual (outsider)		
		(2) Means	Snooping traffic with a modem and traffic analyzer (ST, 2013), etc.		
		(3) Motive	Gain knowledge of another person's electricity consumption pattern and plan a theft of the apartment, for example.		
		(4) Outcome	☒ **Disclosure** ☐ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security requirements	Confidentiality of customers' electricity consumption would be breached.		
		(6) Probability	☒ **High**	☐ **Medium**	☐ **Low**

	(7) Consequences	(8) Severity		
	The electricity consumption readings of one customer are disclosed to another person. It is possible to make conclusions on the customer's electricity consumption patterns and possibly the times when the customer is at home. Based on gathered information a robbery could be planned. If such a scenario would happen, then it could result in a lawsuit filed against the DSO. This would also damage the reputation of the DSO.	**Impact area**	**Value**	**Score**
		Reputation	Moderate	6
		Financial	Moderate	8
		Productivity	Low	1
		Safety & Health	Low	5
		Penalties	Moderate	4
			Relative risk score:	24

In table 9 another possible threat to the meter reading message is described. This threat concerns the possible modification of metering values in the messages by a man-in-the-middle attack where communication between two systems is intercepted (Yang *et al*., 2012). Although modification of messages is more complex than simply intercepting, the motivation for meter readings modification might even be higher as it could lead to financial benefits. As integrity of communication messages is of highest importance in smart grid systems, then this is also reflected in the higher risk value of 30. Qin *et al*. (2012) describe an unidentifiable attack of compromising meter measurement data, where inaccurate meter readings lead to bad decisions regarding how much power needs to be generated.

Table 9 Meter Reading information asset modification risk

Information Asset Risk	**Threat**	Information asset	Meter Reading message
		Area of concern	An individual with suitable equipment could modify or inject the meter reading messages.
		(1) Actor	An individual (outsider)
		(2) Means	Man-in-the-middle (Yang *et al*., 2012), etc.
		(3) Motive	Consistently modify the meter reading values to lower values in order to reduce the electricity bill and/or decrease DSO revenue (McDaniel, 2009).

<table>
<tr><td rowspan="10"></td><td rowspan="3"></td><td>(4) Outcome</td><td colspan="6">□ <b>Disclosure</b> □ <b>Destruction</b>
☒ <b>Modification</b> □ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="6">Integrity of meter reading messages would be violated and customer’s actual consumption would be unknown to DSO.</td></tr>
<tr><td>(6) Probability</td><td colspan="2">☒ <b>High</b></td><td colspan="2">□ <b>Medium</b></td><td colspan="2">□ <b>Low</b></td></tr>
<tr><td colspan="3">(7) Consequences</td><td colspan="5">(8) Severity</td></tr>
<tr><td colspan="3" rowspan="6">The electricity consumption readings of customer(s) would be modified and this would impact customer invoices and the revenue of DSO. If reading value would be increased by the attacker, then afterwards indemnities may also have to be paid to customers. If such a scenario would happen, then it could result in a lawsuit filed against the DSO and would also damage the reputation of the DSO.</td><td colspan="2"><b>Impact area</b></td><td colspan="2"><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td colspan="2">Reputation</td><td colspan="2">Moderate</td><td>6</td></tr>
<tr><td colspan="2">Financial</td><td colspan="2">High</td><td>12</td></tr>
<tr><td colspan="2">Productivity</td><td colspan="2">Low</td><td>1</td></tr>
<tr><td colspan="2">Safety & Health</td><td colspan="2">Low</td><td>5</td></tr>
<tr><td colspan="2">Penalties</td><td colspan="2">High</td><td>6</td></tr>
<tr><td colspan="8"><b>Relative risk score:</b></td><td>30</td></tr>
</table>

C4 Security highlighted the risk of using public telecom infrastructure for smart grid communications, as then the DSO would be relying on an external party and there would be lack of certainty in who is able to access the communication equipment physically or remotely and how the third party is handling risks (C4 Security, 2012). Moreover, the telecom equipment could be accessible from the Internet for remote management and troubleshooting, opening another vector for attacking the network, for example, from the other side of the world via DDoS (Distributed Denial of Service) trying to corrupt the same target by sending multiple packets.

Another possibility is to send malformed packets, also called fuzzing, to either the meter or DC in order to crash the device (McLaughlin *et al.*, 2010). Additionally, C4 Security found fundamental smart meter security issues that are listed in the Open Web Application Security Project (OWASP) top 10 including: lack of authentication, authentication bypass, insecure protocol implementation and input validation errors. Hossain *et al.* (2012) describe wireless communication jamming in order to delay pricing updates from reaching the smart meters. The attacker can decide when to fill up power reserves and when to release the pricing updates based on real time power price. Once the demand is high, the attacker can benefit from selling the reserved energy and thus manipulating the power market by making market dynamics predictable to the attacker. Falsifying consumption data can also cause the control center to decide either to supply disconnected nodes and overloading the generators resulting in protection system disconnecting the generator, or to disconnect the lowest priority nodes, although the power supply is sufficient. The risk of meter reading interruption is analyzed further in table 10.

Table 10 Meter Reading information asset interruption risk

<table>
<tr><td rowspan="13"><b>Information Asset Risk</b></td><td rowspan="8"><b>Threat</b></td><td>Information asset</td><td colspan="4">Meter Reading message</td></tr>
<tr><td>Area of concern</td><td colspan="4">If any of the network components' interfaces have public IP address or attacker can access smart meter's communication module, then a DDoS attack could be launched.</td></tr>
<tr><td>(1) Actor</td><td colspan="4">An individual (outsider)</td></tr>
<tr><td>(2) Means</td><td colspan="4">Taking control over several network devices and creating "zombies" for DDoS (Sgouras <i>et al</i>., 2014) or crashing devices by fuzzing (McLaughlin <i>et al</i>., 2010)</td></tr>
<tr><td>(3) Motive</td><td colspan="4">Interrupt collecting of meter readings to damage the DSO or to abstain from paying for the electricity (McDaniel, 2009).</td></tr>
<tr><td>(4) Outcome</td><td colspan="4">□ <b>Disclosure</b> □ <b>Destruction</b>
□ <b>Modification</b> ☒ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="4">The communication in AMI network would be interrupted and the AMI functionalities would be unusable.</td></tr>
<tr><td>(6) Probability</td><td>☒ <b>High</b></td><td colspan="2">□ <b>Medium</b></td><td>□ <b>Low</b></td></tr>
<tr><td colspan="3">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="3" rowspan="5">The electricity consumption readings of customer(s) would not be able to reach the AMI HES. DSO would be unable to generate accurate invoices and customer support activities would be interrupted as well. In addition to meter reading messages, other type of messages would be affected as well. Also the reputation of</td><td><b>Impact area</b></td><td><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td>Reputation</td><td>Moderate</td><td>6</td></tr>
<tr><td>Financial</td><td>Moderate</td><td>8</td></tr>
<tr><td>Productivity</td><td>High</td><td>3</td></tr>
<tr><td>Safety & Health</td><td>Moderate</td><td>10</td></tr>
</table>

	the DSO would be impacted.	Penalties	Moderate	4
			Relative risk score:	31

5.7.2 End Device Control message

Another example information asset is the End Device Control (connect/disconnect, load control, demand reset and real-time pricing commands) message. As this message's asset profile is quite similar to meter reading information asset, then filling in the asset profile table will be skipped. The first threat is again disclosure of the End Device Control message to an unauthorized party, which could help the attacker to learn the structure of the message. The risk analysis is carried out in table 11.

Table 11 End Device Control information asset disclosure risk

Information Asset Risk	**Threat**	Information asset	Meter End Device Control (disconnect/connect) message		
		Area of concern	An individual with suitable equipment could snoop End Device Control messages while the messages are transmitted.		
		(1) Actor	An individual (outsider)		
		(2) Means	Intercepting communication channel by man-in-the-middle attack (Yang *et al*., 2012), etc.		
		(3) Motive	Learn the protocol being used between meter and HES in order to start generating similar messages for attack purposes.		
		(4) Outcome	☒ **Disclosure**	☐ **Destruction**	
			☐ **Modification**	☐ **Interruption**	
		(5) Security requirements	End Device Control messages would be disclosed to an unauthorized person and confidentiality of the messages would be violated.		
		(6) Probability	☒ **High**	☐ **Medium**	☐ **Low**
	(7) Consequences		(8) Severity		
	The attacker can learn the communication protocol being used between the smart meter and the utility back office, gaining		**Impact area**	**Value**	**Score**
			Reputation	Low	3

	knowledge for generating similar messages. This could ease an attack later on.	Financial	Low	4
		Productivity	Low	1
		Safety & Health	Low	5
		Penalties	Low	2
			Relative risk score:	15

Here is integrity again the most important security requirement, as it would be disastrous if the disconnect message would be sent to a wrong customer. Since disconnecting the electricity meter, either mistakenly or as a part of a cyber-attack, may lead even to loss of life, then this threat results in highest relative risk score of 37, as shown in table 12. Rice *et al*. (2013, 2014) describe *load-drop* attack tree which shows that an attacker using disconnect messages could create a situation where power supply far exceeds demand causing frequency increase at the generators leading to their shutdown, affecting quality and evoking disruption of the power delivered to customers.

Table 12 End Device Control message information asset modification risk

Information Asset Risk	**Threat**	Information asset	Meter End Device Control (disconnect/connect) message		
		Area of concern	An individual with suitable equipment could modify End Device Control messages.		
		(1) Actor	An individual (outsider)		
		(2) Means	Intercepting communication channel by man-in-the-middle attack (Yang *et al*., 2012), etc.		
		(3) Motive	Block a disconnect message to attacker's own meter or route the disconnect message to another customer (a neighbor, for example) or generate a bulk of disconnect messages.		
		(4) Outcome	☐ **Disclosure** ☒ **Modification**	☐ **Destruction** ☒ **Interruption**	
		(5) Security requirements	Integrity and confidentiality of End Device Control messages would be violated.		
		(6) Probability	☒ **High**	☐ **Medium**	☐ **Low**

	(7) Consequences	(8) Severity		
	The meter disconnect message of a customer would be modified and this would lead to unwanted and unexpected loss of power, which might be critical in hospitals. After recovering from wrong disconnecting, indemnities may have to be paid to customers. Power generation plants may also suffer from sudden drop in the load on the system. If such a scenario would happen, then it could result in a lawsuit filed against the DSO and reputation of the DSO could be damaged.	**Impact area**	**Value**	**Score**
		Reputation	Moderate	6
		Financial	Moderate	8
		Productivity	Moderate	2
		Safety & Health	High	15
		Penalties	High	6
			Relative risk score:	37

5.7.3 End Device Event message

Since End Device Event messages include outage and voltage threshold detection, tamper detection and meter health data, then there might be special interest in sabotaging messages of this type. The sabotaging could be in the form of modifying or blocking the End Device Event from reaching the HES server in order to hide theft attempts from the utility. The risk of End Device Event disclosure and modification is analyzed in table 13.

Table 13 End Device Event information asset disclosure and modification risk

Information Asset Risk	**Threat**	Information asset	End Device Event message
		Area of concern	An individual with suitable equipment could modify End Device Control messages.
		(1) Actor	An individual (outsider)
		(2) Means	DDoS attack, intercepting communication channel by man-in-the-middle attack (Yang *et al*., 2012), etc.
		(3) Motive	Block a tamper detection message from meter to HES in order to hide the fact of opening the meter cover.
		(4) Outcome	☒ **Disclosure** ☐ **Destruction** ☒ **Modification** ☒ **Interruption**

		(5) Security requirements	Integrity of End Device Event messages would be violated and HES may make an incorrect assumption that the meter has not been tampered.		
		(6) Probability	☒ **High**	☐ **Medium**	☐ **Low**
	(7) Consequences		(8) Severity		
	The tampering alarm message of meter(s) would be modified or blocked and this would complicate detection of electricity fraud. If meter is tampered in order to lower meter readings then DSO may lose some of the revenue and utilizing resources would be needed to locate the source of loss of electricity.		**Impact area**	**Value**	**Score**
			Reputation	Low	3
			Financial	Moderate	8
			Productivity	Moderate	2
			Safety & Health	Low	5
			Penalties	Low	2
				Relative risk score:	20

5.7.4 Master Data Management and Data Linkage message

These messages are used, among other things, to provide configuration and pricing structure information to the meters (Goodrich, 2011). Attackers might be motivated to learn the structure of these configuration messages and also the configuration values used by the utility. As a next step, attackers may modify these messages, for example, to change communication module parameters in order to route or interrupt the traffic in a desired way. The risk of data linkage message disclosure and modification is specified in table 14.

Table 14 Master Data Management information asset disclosure and modification risk

Information Asset Risk	**Threat**	Information asset	Data Linkage message
		Area of concern	Attackers might be interested in intercepting and modifying devices' configuration messages.
		(1) Actor	An individual (outsider)
		(2) Means	Intercepting communication channel by man-in-the-middle attack (Yang *et al.*, 2012), etc.

<table>
<tr><td rowspan="11"></td><td rowspan="4"></td><td>(3) Motive</td><td colspan="3">Modify meter’s communication module parameters in order to change routing in a desired way or modify pricing structure.</td></tr>
<tr><td>(4) Outcome</td><td colspan="3">☒ <b>Disclosure</b> ☐ <b>Destruction</b>
☒ <b>Modification</b> ☒ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="3">Messages would be disclosed to and integrity would be violated by an unauthorized party.</td></tr>
<tr><td>(6) Probability</td><td>☒ <b>High</b></td><td>☐ <b>Medium</b></td><td>☐ <b>Low</b></td></tr>
<tr><td colspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="2" rowspan="6">Attacker may achieve cheaper pricing if pricing structure change is accomplished. If configuration of lots of meters or DCs is changed as desired by attackers, then considerable amount of resources might be needed on DSO side to restore correct configuration once the attack is discovered. Normal communication of various types of messages might be affected as well, causing failing SLAs.</td><td><b>Impact area</b></td><td><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td>Reputation</td><td>Moderate</td><td>6</td></tr>
<tr><td>Financial</td><td>Moderate</td><td>8</td></tr>
<tr><td>Productivity</td><td>High</td><td>3</td></tr>
<tr><td>Safety & Health</td><td>Low</td><td>5</td></tr>
<tr><td>Penalties</td><td>Low</td><td>2</td></tr>
<tr><td colspan="5"><b>Relative risk score:</b></td><td>24</td></tr>
</table>

5.7.5 Payment Metering Service message

This type of message concerns prepayment meters installed at customer’s premises, usually in hotels or student dorms, where customers are changing frequently. Although not so widely used as typical residential meters, there still might be motivation to change the tariff of the prepayment meters in favor of the customer. The risk of payment metering service message disclosure and modification is analyzed in table 15.

Table 15 Payment Metering Service information asset modification risk

Information Asset Risk	**Threat**	Information asset	Payment Metering Service message
		Area of concern	An attacker may modify or generate payment metering service message to consume electricity for free.
		(1) Actor	An individual (outsider)

		(2) Means	Intercepting communication channel by man-in-the-middle attack (Yang *et al.*, 2012), etc.		
		(3) Motive	An attacker might want to modify the tariff information included in prepayment metering service message.		
		(4) Outcome	☒ **Disclosure** ☒ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security requirements	The message would be disclosed and integrity violated by an unauthorized party.		
		(6) Probability	☒ **High**	☐ **Medium**	☐ **Low**
	(7) Consequences		(8) Severity		
	The attacker changes the tariff of the prepayment meter to his/her favor. The utility would be affected financially due to the lower tariff. If the attacker manages to lower the tariff of his/her meter and increase the tariff of another meter at the same time, then there might be a health risk for the other customer, as the other meter may start to switch off appliances.		**Impact area**	**Value**	**Score**
			Reputation	Low	3
			Financial	Low	4
			Productivity	Low	1
			Safety & Health	Moderate	10
			Penalties	Low	2
				Relative risk score:	20

5.7.6 Meter configuration

McLaughlin *et al*. (2009) describe how it was possible to extract meter plain text password by optical port snooping in order to gain access to meter's administrative interface. As meters typically contain limited hardware resources, including memory, then size of the software is also kept to a minimum, therefore cutting back on input validation and error handling (IOActive, 2010). Inadequate input validation could enable buffer overflows, where program overwrites adjacent memory. In brute force attacks a large amount of login credentials could be submitted in an automated way until successful login. In addition, any interface accessible to the outside world may be a means of an attack, especially program/debug connections (Grand, 2011). The risk of meter configuration loss of confidentiality and integrity is analyzed in table 16.

Table 16 Meter configuration information asset disclosure and modification risk

<table>
<tr><td rowspan="12"><b>Information Asset Risk</b></td><td rowspan="9"><b>Threat</b></td><td>Information asset</td><td colspan="3">Meter configuration</td></tr>
<tr><td>Area of concern</td><td colspan="3">An attacker could try to read configuration parameters from the meter memory.</td></tr>
<tr><td>(1) Actor</td><td colspan="3">An individual (outsider)</td></tr>
<tr><td>(2) Means</td><td colspan="3">Man-in-the-middle attack, Brute force login, Buffer overflow, etc.</td></tr>
<tr><td>(3) Motive</td><td colspan="3">Learn the enabled interfaces of meter, configuration and reveal plaintext passwords or password hashes.</td></tr>
<tr><td rowspan="2">(4) Outcome</td><td colspan="2">☒ <b>Disclosure</b></td><td>☐ <b>Destruction</b></td></tr>
<tr><td colspan="2">☒ <b>Modification</b></td><td>☒ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="3">Meters’ configuration and passwords’ confidentiality and integrity would be violated.</td></tr>
<tr><td>(6) Probability</td><td>☒ <b>High</b></td><td>☐ <b>Medium</b></td><td>☐ <b>Low</b></td></tr>
<tr><td colspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="2" rowspan="2">An attacker could extract passwords, IP addresses to other system components, etc. from meter. The attacker might change the configuration in order to achieve desired routing of messages or break some of the functionalities.</td><td><b>Impact area</b></td><td><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td>Reputation
Financial
Productivity
Safety & Health
Penalties</td><td>Moderate
Moderate
High
Moderate
Low</td><td>6
8
3
10
2</td></tr>
<tr><td colspan="5"><b>Relative risk score:</b></td><td>29</td></tr>
</table>

5.7.7 DC configuration

Although data concentrators are typically enclosed in locked substations where usual substation physical security requirements apply, the possibility of an outsider breaking into the facility or a disgruntled employee using his/her privileged access might attempt to tamper the DC. As DC is handling the communication and storing information of all the meters connected to it, then it could be considered as a more important information asset container than an individual meter, which results in a higher relative risk score for the DC. The risk of DC configuration confidentiality and integrity breach is described in table 17.

Table 17 DC configuration information asset disclosure and modification risk

<table>
<tr><td rowspan="15">**Information Asset Risk**</td><td rowspan="8">**Threat**</td><td>Information asset</td><td colspan="3">DC configuration</td></tr>
<tr><td>Area of concern</td><td colspan="3">An attacker or disgruntled employee may try to extract contents of DC memory.</td></tr>
<tr><td>(1) Actor</td><td colspan="3">An individual (outsider)</td></tr>
<tr><td>(2) Means</td><td colspan="3">Man-in-the-middle, Brute force login, Buffer overflow, etc.</td></tr>
<tr><td>(3) Motive</td><td colspan="3">Gaining privileged access to a DC might me more prestigious than an individual meter, as all of the meters communicating with the DC might be affected and information about multiple meters may be retrieved at the same time.</td></tr>
<tr><td>(4) Outcome</td><td colspan="3">☒ **Disclosure**
☐ **Destruction**
☒ **Modification**
☒ **Interruption**</td></tr>
<tr><td>(5) Security requirements</td><td colspan="3">The confidentiality and integrity of DC configuration would be breached.</td></tr>
<tr><td>(6) Probability</td><td>☒ **High**</td><td>☐ **Medium**</td><td>☐ **Low**</td></tr>
<tr><td colspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="2" rowspan="6">An attacker could be able to extract passwords and IP addresses to other systems. Configuration might be modified in a way that would change the AMI routing logic or break some of the functionalities of the DC. If an attacker manages to trigger configuration changes on all of the meters connected to the DC, then correcting the configuration on the field would require utility’s resources.</td><td>**Impact area**</td><td>**Value**</td><td>**Score**</td></tr>
<tr><td>Reputation</td><td>Moderate</td><td>6</td></tr>
<tr><td>Financial</td><td>High</td><td>12</td></tr>
<tr><td>Productivity</td><td>High</td><td>3</td></tr>
<tr><td>Safety & Health</td><td>Moderate</td><td>10</td></tr>
<tr><td>Penalties</td><td>Low</td><td>2</td></tr>
<tr><td colspan="5">**Relative risk score:**</td><td>33</td></tr>
</table>

5.7.8 Historical readings in meter memory

The measured reading values in meter’s memory could be accessed by logging into the administrative interface of the smart meter or by requesting historical readings via communication interface or by tampering the meter and dumping the memory contents (McLaughlin *et al.*, 2009). If program input validation is insufficient, then an attacker could inject a system command which might be executed by the application, providing a pseudo system shell. Based on a set of meter reading values over a period of time, conclusions could be made on the energy consumption patterns of the customer connected to the meter (IOActive, 2010). The risk of disclosure of historical readings in meter memory is analyzed in table 18.

Table 18 Historical readings in meter memory information asset disclosure risk

<table>
<tr><td rowspan="13"><b>Information Asset Risk</b></td><td rowspan="8"><b>Threat</b></td><td>Information asset</td><td colspan="3">Historical readings in meter memory</td></tr>
<tr><td>Area of concern</td><td colspan="3">An attacker could try extracting historical readings from meter memory.</td></tr>
<tr><td>(1) Actor</td><td colspan="3">An individual (outsider)</td></tr>
<tr><td>(2) Means</td><td colspan="3">Brute force login, buffer overflow, command injection, etc.</td></tr>
<tr><td>(3) Motive</td><td colspan="3">Extract historical meter readings in order to plot a customer’s energy consumption patterns.</td></tr>
<tr><td>(4) Outcome</td><td colspan="3">☒ <b>Disclosure</b> ☐ <b>Destruction</b>
☐ <b>Modification</b> ☐ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="3">The confidentiality of an individual’s meter readings would be breached.</td></tr>
<tr><td>(6) Probability</td><td>☒ <b>High</b></td><td>☐ <b>Medium</b></td><td>☐ <b>Low</b></td></tr>
<tr><td colspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="2" rowspan="4">The attacker would be able to make assumptions on an individual’s lifestyle based on extracted historical meter readings. Further harmful actions could then be planned based on the assumptions.</td><td><b>Impact area</b></td><td><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td>Reputation</td><td>Low</td><td>3</td></tr>
<tr><td>Financial</td><td>Low</td><td>4</td></tr>
<tr><td>Productivity</td><td>Low</td><td>1</td></tr>
</table>

		Safety & Health	Moderate	10
		Penalties	Low	2
			Relative risk score:	20

5.7.9 Historical readings in DC memory

PLC meter readings cached in DC memory could be read by sending a request from the WAN side of the DC for specific historical readings, by gaining physical access to the DC and dumping the memory contents or logging into the DC administrative interface using a sniffed or brute forced password. Since DC stores data for the meters that are communicating with it, then motivation for attackers is most likely higher than extracting readings from an individual meter. The risk of extracting historical readings from DC memory is described in table 19.

Table 19 Historical readings in DC memory information asset disclosure risk

<table>
<tr><td rowspan="11"><b>Information Asset Risk</b></td><td rowspan="8"><b>Threat</b></td><td>Information asset</td><td colspan="3">Historical readings in DC memory</td></tr>
<tr><td>Area of concern</td><td colspan="3">An attacker may try to extract historical readings from DC memory.</td></tr>
<tr><td>(1) Actor</td><td colspan="3">An individual (outsider)</td></tr>
<tr><td>(2) Means</td><td colspan="3">Brute force login, buffer overflow, command injection, etc.</td></tr>
<tr><td>(3) Motive</td><td colspan="3">Gaining access to readings of multiple meters connected to the DC and learning the energy consumption patterns of several customers.</td></tr>
<tr><td>(4) Outcome</td><td colspan="3">☒ <b>Disclosure</b> ☐ <b>Destruction</b>
☐ <b>Modification</b> ☐ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="3">Confidentiality of customers’ historical meter readings would be violated.</td></tr>
<tr><td>(6) Probability</td><td>☒ <b>High</b></td><td>☐ <b>Medium</b></td><td>☐ <b>Low</b></td></tr>
<tr><td colspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="2" rowspan="2">The attacker would be able to make assumptions on multiple customers’ lifestyles based on extracted historical</td><td><b>Impact area</b></td><td><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td>Reputation</td><td>Moderate</td><td>6</td></tr>
</table>

	meter readings. Further harmful actions could then be planned based on the assumptions.	Financial	Low	4
		Productivity	Low	1
		Safety & Health	Moderate	10
		Penalties	Low	2
			Relative risk score:	23

5.7.10 Alarms/events in meter memory

Attackers or thieves may be interested in deleting End Device Event records from the meter memory before they are sent out towards HES, to hide their malicious actions. This could be achieved by knowing the meter's administrative interface password (McLaughlin *et al.*, 2009). The primary motive might be to remove the cover of the unit and intercept or modify other information assets in the meter. The risk of disclosure and modification of events in meter memory is analyzed in table 20.

Table 20 Alarms/events in meter memory information asset disclosure and modification risk

Information Asset Risk	**Threat**	Information asset	Alarms/events in meter memory
		Area of concern	An attacker may attempt to tamper the meter memory right before an alarm is generated from the meter towards the HES in order to prevent sending out the alarm.
		(1) Actor	An individual (outsider)
		(2) Means	Brute force login, buffer overflow, etc.
		(3) Motive	Hiding fraud/case opening event from the utility.
		(4) Outcome	☒ **Disclosure** ☐ **Destruction** ☒ **Modification** ☐ **Interruption**
		(5) Security requirements	The confidentiality and integrity of metering unit events would be violated.
		(6) Probability	☒ **High** ☐ **Medium** ☐ **Low**

	(7) Consequences	(8) Severity		
	The attacker could prevent the alarms from being sent out from the meter. This could ease carrying out successive malicious activities without notifying the utility. If attacker would succeed in modifying the tariff of metering messages, then the utility might endure financial loss.	**Impact area**	**Value**	**Score**
		Reputation	Moderate	6
		Financial	Moderate	8
		Productivity	Moderate	2
		Safety & Health	Low	5
		Penalties	Low	2
			Relative risk score:	23

5.7.11 Meter firmware

There have been examples of reverse engineering smart meters' firmware (Lawson, 2010) and even spreading a worm among thousands of smart meters (Davis, 2009). Reverse engineering the firmware of a meter can give an attacker an idea about the logic and functionalities used in the application code, which could have publicly known vulnerabilities that could be exploited. If the manufacturer of the meter publishes firmware on their web page, then attackers might get access to the firmware. The risk of meter firmware disclosure and modification is described in table 21.

Table 21 Meter firmware information asset disclosure and modification risk

Information Asset Risk	**Threat**	Information asset	Meter firmware
		Area of concern	If an attacker is able to extract and reverse engineer the firmware of the meter then implemented logic and open source functions might be revealed in the program code.
		(1) Actor	An individual (outsider)
		(2) Means	Manufacturer website, etc.
		(3) Motive	Learn the logic and functions of the device and create an impersonating device with additional malicious logic or forge a user's identity (Grand, 2011).
		(4) Outcome	☒ **Disclosure** □ **Destruction** ☒ **Modification** □ **Interruption**

		(5) Security requirements	The confidentiality and integrity of the meter's firmware would be breached.		
		(6) Probability	☒ **High**	☐ **Medium**	☐ **Low**
	(7) Consequences		(8) Severity		
	In reconnaissance phase the attacker could discover the versions of binaries and functions used by the meter in order to plan successive exploits. Unit could be disassembled, modified, recompiled or reprogrammed (Grand, 2011). An impersonating device might be created, imitating the behavior of the original device, but with altered logic.		**Impact area**	**Value**	**Score**
			Reputation	Moderate	6
			Financial	High	12
			Productivity	High	3
			Safety & Health	Low	5
			Penalties	Low	2
				Relative risk score:	28

5.7.12 DC firmware

Similarly to meters, attackers could also want to learn the program code of the DC. The motivation for hacking a DC might even be higher, since DC might be communicating with hundreds of smart meters. As DCs are typically installed inside substations, then physical access might be more difficult to outsiders, but not for disgruntled employees. Therefore the probability of an attack is lower from the physical perspective, but on the other hand motivation might be higher. The risk of DC firmware disclosure is further analyzed in table 22.

Table 22 DC firmware information asset disclosure modification risk

Information Asset Risk	**Threat**	Information asset	DC firmware
		Area of concern	An attacker might be able to reverse engineer DC firmware and learn the logic of the program code.
		(1) Actor	An individual (outsider), disgruntled employee
		(2) Means	Manufacturer website, etc.
		(3) Motive	Since DC aggregates data from several meters then the motivation to exploit a DC is higher than a single meter. DC could be reprogrammed and additional logic added.

		(4) Outcome	☒ **Disclosure** ☒ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security requirements	Confidentiality of DC firmware would be breached.		
		(6) Probability	☐ **High**	☒ **Medium**	☐ **Low**
	(7) Consequences		(8) Severity		
	DC could be disassembled, modified, recompiled or reprogrammed (Grand, 2011). An impersonating DC might be set up which acts similarly to the original DC.		**Impact area**	**Value**	**Score**
			Reputation	Moderate	6
			Financial	High	12
			Productivity	Moderate	2
			Safety & Health	Low	5
			Penalties	Low	2
				Relative risk score:	27

5.7.13 Meter encryption key

In order to be able to intercept and understand the encrypted communication between the meter and the HES system, the attacker might be motivated to extract the cryptographic keys from the meter. This would allow the attacker to analyze the traffic despite of encryption and impersonate the meter, sending modified metering data to the utility. The side-channel attacks, specifically timing attacks, monitor the data flow into and out of the CPU or memory running the cryptographic algorithm. By measuring the time fluctuations in how long it takes to execute cryptographic operations, it might be possible to determine the secret key (Grand, 2011). The risk of extracting the meter's encryption keys is analyzed in table 23.

Table 23 Meter encryption key information asset disclosure risk

Information Asset Risk	**Threat**	Information asset	Meter encryption key
		Area of concern	An attacker might be able to extract the private cryptographic key from the meter and act as a legitimate device to the DC or HES.

(1) Actor	An individual (outsider)		
(2) Means	Side-Channel attack (Grand, 2011), etc.		
(3) Motive	Be able to decrypt the communication from the DC or HES and view metering data or configuration changes, for example.		
(4) Outcome	☒ **Disclosure** □ **Modification**	□ **Destruction** □ **Interruption**	
(5) Security requirements	The private cryptographic key of the meter would be disclosed to an unauthorized party.		
(6) Probability	☒ **High**	□ **Medium**	□ **Low**

(7) Consequences	(8) Severity		
	Impact area	**Value**	**Score**
An attacker could create an impersonating device that would be able to legitimately authenticate and send encrypted messages to the DC or HES. The attacker would then be able to forge meter readings.	Reputation	Moderate	6
	Financial	Moderate	8
	Productivity	High	3
	Safety & Health	Low	5
	Penalties	Low	2
		Relative risk score:	24

5.7.14 DC encryption key

As in the case of firmware, DC might be a more tempting target for the attacker as it is communicating with lots of meters and the HES. By extracting the cryptographic keys from the DC, the attacker would be able to read all the readings of the connected meters and act as a legitimate DC unit. As several attack methods require physical access to the device, then the probability of an attack is slightly lower than in the case of a meter. The risk of extracting DC encryption keys is analyzed in table 24.

Table 24 DC encryption key information asset modification risk

<table>
<tr><td rowspan="15"><b>Information Asset Risk</b></td><td rowspan="8"><b>Threat</b></td><td>Information asset</td><td colspan="3">DC encryption key</td></tr>
<tr><td>Area of concern</td><td colspan="3">An attacker could extract the private key of the DC and be able to act as a legitimate DC, while executing altered logic.</td></tr>
<tr><td>(1) Actor</td><td colspan="3">An individual (outsider)</td></tr>
<tr><td>(2) Means</td><td colspan="3">Side-Channel attack (Grand, 2011), etc.</td></tr>
<tr><td>(3) Motive</td><td colspan="3">By possessing the DC private key the attacker could read the traffic from the meters as well as from the HES.</td></tr>
<tr><td>(4) Outcome</td><td colspan="3">☒ <b>Disclosure</b> ☐ <b>Destruction</b>
☐ <b>Modification</b> ☐ <b>Interruption</b></td></tr>
<tr><td>(5) Security requirements</td><td colspan="3">Confidentiality of the DC encryption key would be violated and disclosed to an unauthorized party.</td></tr>
<tr><td>(6) Probability</td><td>☐ <b>High</b></td><td>☒ <b>Medium</b></td><td>☐ <b>Low</b></td></tr>
<tr><td colspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td colspan="2" rowspan="6">Attacker would be able to decrypt the traffic between meters and the HES, including meter readings and End Device Control messages, possibly leading to arbitrary meter disconnects. Attacker might also be able to act as a legitimate DC to the other communication devices.</td><td><b>Impact area</b></td><td><b>Value</b></td><td><b>Score</b></td></tr>
<tr><td>Reputation</td><td>Moderate</td><td>6</td></tr>
<tr><td>Financial</td><td>High</td><td>12</td></tr>
<tr><td>Productivity</td><td>High</td><td>3</td></tr>
<tr><td>Safety & Health</td><td>Moderate</td><td>10</td></tr>
<tr><td>Penalties</td><td>Moderate</td><td>4</td></tr>
<tr><td colspan="5"><b>Relative risk score:</b></td><td>35</td></tr>
</table>

5.8 Selecting mitigation approach

Organizations determine which of the identified risks require mitigation and develop a mitigation strategy for those risks. This is accomplished by first prioritizing risks based on their relative risk scores. Relative risk scores and probability combinations are divided into different pools in table 25. In turn, each pool has a mitigation approach in table 26, which is taken as input for developing mitigation plans. When risks have been prioritized, mitigation strategies can be established that consider the value of the asset and its security requirements, surrounding containers, and the organization's distinct operating environment (Caralli *et al*., 2007).

Table 25 Relative risk matrix

Probability	Risk score		
	30 to 45	16 to 29	0 to 15
High	Pool 1	Pool 2	Pool 2
Medium	Pool 2	Pool 2	Pool 3
Low	Pool 3	Pool 3	Pool 4

Table 26 Mitigation approaches per pool

Pool	Mitigation approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Considering the probabilities and relative risk scores from tables 8 – 24 the identified risks have been divided into pools in table 27. Risks that require mitigation are visible under pool 1, while less critical risks which could either be mitigated or deferred are outlined in pool 2. Although pool 3 and pool 4 are left empty in this analysis, other less critical risks surely exists, which were not addressed in this assessment.

Table 27 Risk prioritization and mitigation strategy

Risk	Probability	Relative risk score
Pool 1 – Mitigate		
End Device Control modification	High	37
DC configuration disclosure	High	33
Meter Reading interruption	High	31
Meter Reading modification	High	30
Pool 2 – Mitigate or defer		
DC encryption key disclosure	Medium	35
Meter configuration disclosure	High	29
Meter firmware disclosure	High	28
DC firmware disclosure	Medium	27
Meter Reading disclosure	High	24
Data Linkage modification	High	24
Meter encryption key disclosure	High	24
Historical reading in DC disclosure	High	23
Meter alarms modification	High	23
End Device Event modification	High	20
Meter historical readings disclosure	High	20
Payment Metering Service modification	High	20
End Device Control disclosure	High	15
Pool 3 – Defer or accept		
Pool 4 - Accept		

6 Conclusion

Based on the risk analysis in section 5 and the resulting risk prioritization in table 27, it can be concluded that the first risk mitigation efforts should be targeted at preventing malicious generation or modification of End Device Control messages, which could be used to power off smart meters in a large area of a country and could lead to loss of life. It is followed by threats to the Meter Reading information asset, where communication could be interrupted by a DDoS attack or messages disclosed and modified, leading to violation of individuals' privacy or shutting power off by the operations center. Researchers have been able to deploy fast spreading viruses on smart meters, which re-enforces the indisputable need for regular ICT risk assessments in the smart grid solutions.

The chosen OCTAVE Allegro method has proven to be the most suitable for implementation in conditions of limited preparation time, practical skills and financial resources, as it did not involve overwhelming manuals and forms to be filled in or complex cost calculations. If the same method is used in the future research, then the selection and prioritization of risk measurement criteria might be different, resulting in relative risk scores distinct from this analysis. However, the method's focus on information assets, their containers and various areas of concern can help organizations and researchers achieve meaningful results in an efficient manner. In addition, the demonstration of the methodology hopefully contributes to demystification of the complexity of conducting risk assessments and encourages organizations to establish regular and formal method based risk assessments, which do not have to be costly or cumbersome in order to provide valuable output.

References

Bompard, E., Huang, T., Wu, Y., Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. – Electrical Power and Energy Systems 50 (2013), p. 50–64 (Online) ScienceDirect (20.04.2014)

BSI, Bundesamt für Sicherheit in der Informationstechnik. (2013). IT-Grundschutz An Overview. – Revision April 2013. (Online) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-Grundschutz_Guide_for_Managers.pdf?__blob=publicationFile (15.02.2014)

C4 Security. (2012). The Dark Side of the Smart Grid – Smart Meter (in)Security. (Online) http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf (14.04.2014)

Caralli R., Stevens J., Young L., Wilson W. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. – *Software Engineering Institute Technical Report,* CMU/SEI-2007-TR-012 (Online) http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf (8.03.2014)

CESG. National Technical Authority for Information Assurance. (2009). HMG IA Standard No. 1. Technical Risk Assessment. – Issue No. 3.51 (Online) http://www.cesg.gov.uk/publications/documents/is1_risk_assessment.pdf (9.03.2014)

Davis, M. (2009). SmartGrid Device Security. Adventures in a new medium. - Black Hat USA 2009 (Online) http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf (20.04.2014)

ENISA ad hoc working group on risk assessment and risk management. (2006). Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs) – *Deliverable 2, Final version, Version 1.0* (Online) https://www.enisa.europa.eu/activities/risk-management/files/deliverables/information-packages-for-small-and-medium-sized-enterprises-smes (17.02.2014)

ENISA Technical Department of Section Risk Management. (2006). Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. (Online) http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools (10.02.2014)

ENISA. (2012). Smart Grid Security. – Annex I. General Concepts and Dependencies with ICT [Deliverable – 2012-04-19] (Online) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid (15.02.2014)

ENISA. (2012). Smart Grid Security. Recommendations for Europe and Member States. – *Deliverable – 2012-07-01* (Online) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations (14.02.2014)

ENISA. [WWW] Inventory of Risk Management / Risk Assessment Methods. http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods (10.02.2014)

EU Smart Grid Task Force. (2013). Expert Group 3 - First Year Report: Options on handling Smart Grids Data. (Online) http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group3_first_year_report.pdf (16.02.2014)

European Commission. (2011). A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the SMART METER. – FULL REPORT (Online) http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_10_smart_meter_funtionalities_report_full.pdf (05.03.2014)

European Commission. (2011). Communication on Critical Information Infrastructure Protection. Achievements and next steps: towards global cyber-security. - COM(2011) 163 final (Online) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF (03.03.2014)

European Commission. (2011). Energy Efficiency Plan. – COM(2011) 109 final (Online) http://eur-lex.europa.eu/resource.html?uri=cellar:441bc7d6-d4c6-49f9-a108-f8707552c4c0.0002.03/DOC_1&format=PDF (04.03.2014)

European Commission. (2011). Smart Grids: from innovation to deployment. – COM(2011) 202 final (Online) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0202&qid=1397551864837&from=EN (04.03.2014)

European Parliament. (2009). Directive 2009/72/EC of the European Parliament and of the Council concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. (Online) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0072&qid=1397552555914&from=EN (17.02.2014)

Falliere, N., Murchu, L. O., Chien, E. Symantec. 2011. W32.Stuxnet Dossier. – Version 1.4 (Online)
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (18.02.2014)

Fang, X., Misra, S., Xue, G., Yang, D. (2012). Smart Grid – The New and Improved Power Grid: A Survey. – IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 4, FOURTH QUARTER 2012, 944 - 980 (Online) IEEE Xplore (12.03.2014)

Goodrich, M. SISCO. (2011). 61968 – 9 Meter Reading and Control. - CIM University, Prague, Czech Republic (Online) http://cimug.ucaiug.org/Meetings/Prague2011/Shared%20Documents/CIM%20University/03-61968-9%20Meter%20Reading%20and%20Control.pdf (06.04.2014)

Hossain, E., Han, Z., Poor, H. V. (2012). Smart Grid Communications and Networking. Cambridge : Cambridge University Press.

Huczala, M., Lukl, T., Misurec, J. (2006). Capturing Energy Meter Data over Secured Power Line. - Communication Technology, 2006. ICCT '06. International Conference on 27-30 Nov. 2006, 1-4 (Online) IEEE Xplore (13.03.2014)

IEEE Standards Coordinating Committee 21. (2011). IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. – IEEE Std 2030-2011 (Online) IEEE Xplore (20.03.2014)

IOActive. (2010). Securing the Smart Grid. (Online) http://www.ioactive.com/pdfs/InfosecurityEurope10SmartGrid.pdf (23.04.2014)

Jackson, J. (2009). Are Smart Grids a Smart Investment? Hourly Load Analysis of 800,000 Utility Customers at 200 of the Largest US Utilities. (Online) http://www.hks.harvard.edu/hepg/Papers/2009/sganal.pdf (14.02.2014)

Kuzlu, M., Pipattanasomporn, M., Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. - Computer Networks. Volume 67, 4 July 2014, Pages 74–88 (Online) ScienceDirect (19.04.2014)

Landis+Gyr. (2012). [WWW] http://www.landisgyr.com/landisgyr-to-bring-630000-smart-meters-to-estonia/ (03.03.2014)

Landis+Gyr. (2012). Introducing the power of PLC. (Online) http://www.landisgyr.com/webfoo/wp-content/uploads/2012/11/LG_White_Paper_PLC.pdf (15.02.2014)

Landoll, D. J. (2005). The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. Boca Raton : Auerbach Publications.

Lawson, N. (2010). Reverse-engineering a smart meter. [WWW] http://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/ (20.04.2014)

Lehtla, T. (2013). Tarkvõrgud ja elektrivarustuse tulevikuvisioone. – TTÜ elektrotehnika instituut (Online) http://www.ttu.ee/public/t/Taiendusoppijale/Energeetika_tulevikuvisioone_22.veebr_2013.ppt (24.04.2014)

Luan, W., Sharp, D., Lancashire, S. (2010). Smart grid communication network capacity planning for power utilities. - Transmission and Distribution Conference and Exposition, 2010 IEEE PES, p. 1-4 (Online) IEEE Xplore (16.04.2014)

McDaniel, P., McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. - Security & Privacy, IEEE (Volume:7 , Issue: 3), p. 75-77 (Online) IEEE Xplore (18.04.2014)

McLaughlin, S., Podkuiko, D., McDaniel, P. (2009). Energy theft in the advanced metering infrastructure. - CRITIS'09 Proceedings of the 4th international conference on Critical information infrastructures security, p. 176-187 (Online) http://www.patrickmcdaniel.org/pubs/critis09.pdf (17.04.2014)

McLaughlin, S., Podkuiko, D., Miadzvezhanka, S., Delozier, A., McDaniel, P. (2010) Multi-vendor Penetration Testing in the Advanced Metering Infrastructure. – Proceedings of the 26th Annual Computer Security Applications Conference, p. 107-116 (Online) http://www.patrickmcdaniel.org/pubs/acsac10b.pdf (17.04.2014)

Meng W., Ma R., Chen H. H. (2014). Smart Grid Neighborhood Area Networks: A Survey. – Network, IEEE (Volume:28, Issue: 1), 24-32. (Online) IEEE Xplore (27.02.2014)

Meng, H., Chen, S., Guan, Y. L., Law, C. L., So, P. L., Gunawan, E., Lie, T. T. (2004). Modeling of Transfer Characteristics for the Broadband Power Line Communication Channel. - IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 19, NO. 3, JULY 2004, 1057 - 1064 (Online) IEEE Xplore (18.02.2014)

Mullenmaster, B., Goodrich, M., Wilhoit, F. (2011). Outage Notification Use Case. - Use case #5.4 (Online) http://smartgrid.epri.com/UseCases/Outage%20Notification_ph2add.pdf (22.04.2014)

NIST. (2010). NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid. – The Smart Grid Interoperability Panel – Cyber Security Working Group. (Online) http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf (18.04.2014)

NIST. (2012). Guide for Conducting Risk Assessments. – Special Publication 800-30 Revision 1 (Online) http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (22.02.2014)

OPEN meter Consortium. (2009). D1.1 Report on the identification and specification of functional, technical, economical and general requirements of advanced multi-metering infrastructure, including security requirements. – Version 1.0 (Online) http://openmeter.com/files/deliverables/Open%20Meter_D1%201_Requirements_v1.0_20090701.pdf (23.03.2014)

Pauzet, O. (2010). Cellular Communications and the Future of Smart Metering. – Sierra Wireless Inc. (Online) http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/energy20cellular20communications20and20the20future20of20smart20metering.pdf (23.04.2014)

Platinum Squared. RiskSafe Assessment and IS1&2. [WWW] http://risksafe.co.uk/IS1 (02.04.2014)

Platinum Squared. RiskSafe. [WWW] http://www.risksafe.co.uk/Cramm (01.04.2014)

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., Tan, J. (2008). Evidence Theory based Decision Fusion for Masquerade Detection in IEC61850 Automated Substations. - Information and Automation for Sustainability, 2008. ICIAFS 2008. 4th International Conference, p. 194-199 (Online) IEEE Xplore (21.04.2014)

Qin, Z., Li, Q., Chuah, M. (2012). Unidentifiable Attacks in Electric Power Systems. - Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference, p. 193-202 (Online) IEEE Xplore (20.04.2014)

Rice, E. B., AlMajali, A. (2014). Mitigating The Risk Of Cyber Attack On Smart Grid Systems. - Procedia Computer Science 28 (2014), p. 575-582 (Online) ScienceDirect (20.04.2014)

Rice, E., AlMajali, A., Viswanathan, A., Tan, K., Neuman, C. (2013). A Systems Approach to Analysing Cyber-Physical Threats in the Smart Grid. – Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference, p. 456-461 (Online) IEEE Xplore (21.04.2014)

Salam, A. S., Mahmud, S.A., Khan, G.M., Al-Raweshidy, H.S. (2012). M2M communication in Smart Grids: Implementation scenarios and performance analysis. – *WCNC 2012 Workshop on*

Internet of Things Enabling Technologies, Embracing Machine-to-Machine Communications and Beyond, 142 - 147 (Online) IEEE Xplore (12.03.2014)

Sgouras, K. I., Birda, A. D., Labridis, D. P. (2014). Cyber Attack Impact on Critical Smart Grid Infrastructures. - In proceeding of: 5th Innovative Smart Grid Technologies Conference (ISGT North America 2014) (18.04.2014)

Simmins, J., Sarfi, R. (2011). Remote Meter Firmware Upgrade. - Use case #5.8 (Online) http://smartgrid.epri.com/UseCases/Remote%20Meter%20Firmware%20Update_ph2add.pdf (22.04.2014)

Simmins, J., Tao, M. (2011). In-Field Programming of Smart Meter and Meter Firmware Upgrade. - Use case #5.10 (Online) http://smartgrid.epri.com/UseCases/In%20Field%20Meter%20Program-Firm%20Upgrdadd.pdf (22.04.2014)

Souryal, M.R., Golmie, N. (2012). Analysis of advanced metering over a Wide Area Cellular Network. - Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on 17-20 Oct. 2011, 102 – 107 (Online) IEEE Xplore (17.03.2014)

Spoonamore, S., Krutz, R. L. (2009). Smart Grid and Cyber Challenges. National Security Risks and Concerns of Smart Grid. (Online) http://www.whitehouse.gov/files/documents/cyber/Spoonamore-Krutz%20-%20Smart%20Grid%20CyberSecurity%20Risks%20and%20Concerns.pdf (22.04.2014)

ST. (2013). General purpose ST7540 power line modem module based on ST7540 PLM and STM32 microcontroller. - UM1619 User manual. DocID024383 Rev 1 (Online) http://www.st.com/st-web-ui/static/active/en/resource/technical/document/user_manual/DM00079951.pdf (03.04.2014)

Texas Instruments. (2014). Smart Grid Solutions Guide 2014. (Online) http://www.ti.com/lit/sl/slym071n/slym071n.pdf (19.04.2014)

Wang, W., Xu, Y., Khanna, M. (2011). A survey on the communication architectures in smart grid. – Computer Networks 55, 3604–3629 (Online) http://www.ece.ncsu.edu/netwis/papers/11wxk-comnet.pdf (17.03.2014)

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Im, Eul Gyu, Yao, Z.Q., Pranggono, B., Wang, H.F. (2012). Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems. - Sustainable Power Generation and Supply (SUPERGEN 2012), International Conference, p. 1-8. (Online) IEEE Xplore (24.03.2014)

Yazar, Z. (2002). A Qualitative Risk Analysis and Management Tool - CRAMM. – SANS Institute InfoSec Reading Room, GSEC, Version 1.3 (Online) http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83?show=qualitative-risk-analysis-management-tool-cramm-83&cat=auditing (01.04.2014)