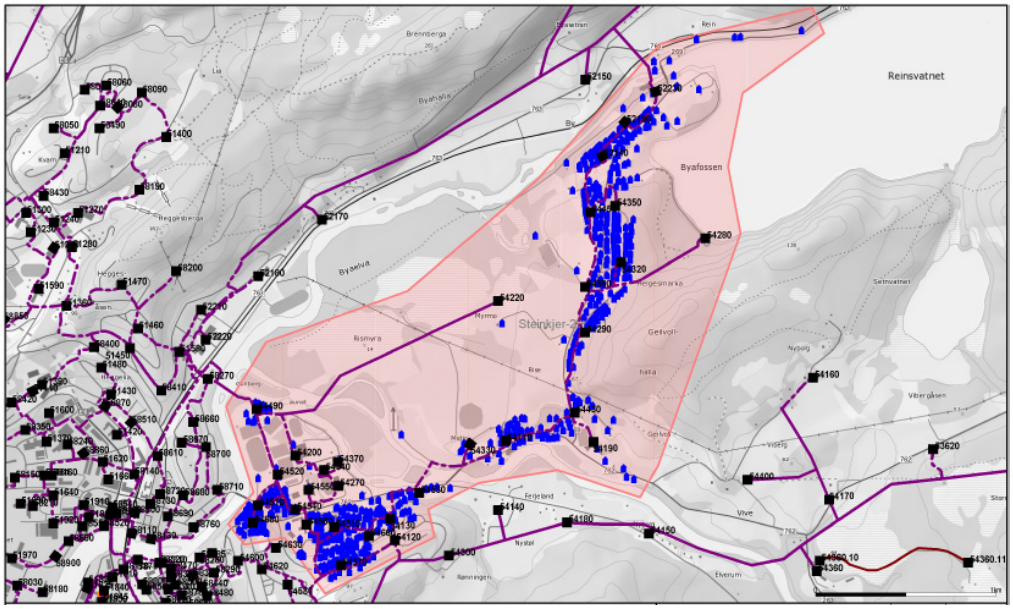
Security Threats in Demo Steinkjer

Report from the Telenor-SINTEF collaboration project on Smart Grids

Author(s)
Inger Anne Tøndel, SINTEF
Martin Gilje Jaatun, SINTEF
Maria Bartnes Line, SINTEF/NTNU



SINTEF ICT and Telenor
2012-09-12

Security Threats in Demo Steinkjer

Report from the Telenor-SINTEF collaboration project on Smart Grids

KEYWORDS:
Smart Grid
Smart Metering
Security
Risk
Threat
ICT

VERSION
1.0

DATE
2012-09-12

AUTHOR(S)
Inger Anne Tøndel, SINTEF
Martin Gilje Jaatun, SINTEF
Maria Bartnes Line, SINTEF/NTNU

CLIENT(S)
Telenor

CLIENT'S REF.

PROJECT NO.
90F32330

NUMBER OF PAGES
39

ABSTRACT
This report describes security threats associated with the deployment of an Advanced Metering Infrastructure (AMI) in the Demo Steinkjer demonstration project. The description is based on the first phase of the actual smart meter roll-out in Steinkjer, but is kept on a vendor-neutral level. This document should thus be relevant for all other Distribution System Operators choosing a similar configuration for their AMI.

The work described in this report has been performed by SINTEF with funding from Telenor, as a contribution to the Demo Steinkjer project organised under the auspices of the Norwegian Smart Grid Centre. Additional contributions have been received from NTNU, NTE and Aidon.

PREPARED BY
Inger Anne Tøndel

SIGNATURE
Inger Anne Tøndel

CHECKED BY
Gorm Johansen

SIGNATURE
Gorm Johansen

APPROVED BY
Erik Kampenhøy

SIGNATURE

REPORT NO. SINTEF A23351
ISBN 978-82-14-05301-2
CLASSIFICATION Unrestricted
CLASSIFICATION THIS PAGE Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION	
1.0	2012-09-12	First version	2

Table of contents

Abbreviations and terms

AMI	Advanced Metering Infrastructure
BSIMM	Building Security In Maturity Model
CC	Common Criteria
DDoS	Distributed Denial of Service (attack)
DFD	Data Flow Diagram
DoS	Denial of Service (attack)
DSO	Distribution System Operator (Norwegian: Nettselskap)
FAN	Field Area Network
GPRS	General Packet Radio Service (in GSM)
GSM	Global System for Mobile communications
HAN	Home Area Network
HES	Head End System
ID	Identity (or: IDentifier)
NIST	(US) National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
OTAP	Over The Air Provisioning
PLC	Power Line Communication
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges
USB	Universal Serial Bus
WAN	Wide Area Network

1 Introduction

The future power grid will be characterised by a high number of devices, a lot of interconnections and increased possibilities for real time control and supervision of the grid – it will be a Smart Grid. The introduction of internet technologies in the power grid however also results in a need to deal with cyber security threats.

Smart meters are a prerequisite, and from the point of view of the customers also the most visible component of a Smart Grid infrastructure. This document presents a high-level identification of information security threats against an Advanced Metering Infrastructure (AMI) as implemented in the Demo Steinkjer project, which subsequently can be used as basis for a full risk assessment. 30 threats are identified, and in addition five likely attack goals are explained.

This document does not contain detailed information on specific vendors' technology. Such information will be provided in a separate document with restricted distribution.

1.1 Scope

The focus of this document is on AMI, and primarily on the smart meter and its communication with the central system of the Distribution System Operator (DSO) (see Figure 1). The Home Area Network is out of scope. We also only consider threats that come from the meter side, and not threats that come from the DSO and its internal system. The primary focus is on malicious acts, as opposed to accidental errors.

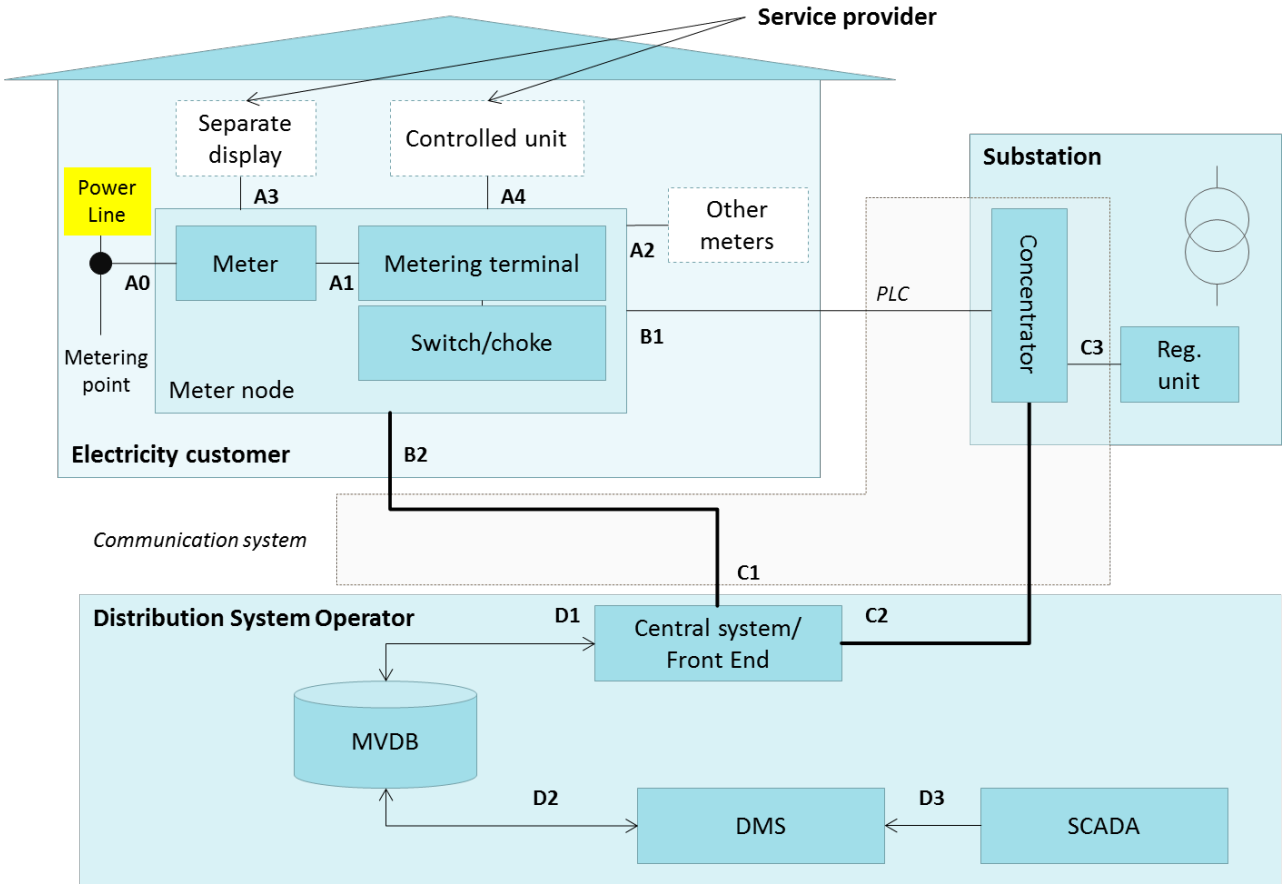


Figure 1: Advanced Metering Infrastructure

This report identifies threats towards AMI, but does not perform an assessment of the risk associated with the threats. Thus, the likelihood and consequences of the threats are not described. However, where relevant we describe important factors that influence the risk.

1.2 Intended audience

This report is intended for the Smart Grid community in Norway (and beyond).

1.3 Method

In this report, the risks related to the introduction of smart meters in Demo Steinkjer are addressed from two angles:

- *Threat overview and identification:* To ensure a high coverage of threats, we use a structured method to identify threats on the possible attack interfaces. The information flow of the AMI system is described using Data Flow Diagrams (DFDs) and the trust boundaries are identified. Then, for each trust boundary, the relevance of the STRIDE[1] threat categories is assessed. This method is based on the threat modelling approach of Microsoft [1].
- *Attacker goals and strategies:* The important assets of the system are identified in a brain storming session and by investigating the system [2]. Then attack goals are associated with these assets, and the possible ways to achieve the goals are detailed in attack trees [3].

To ensure that the relevant threats are covered, the work in this document takes into account already identified threats and risks in documents such as the risk assessment commissioned by NVE [4], the NIST Guidelines for Smart Grid Cyber Security [5] and the security profile for advanced metering infrastructure of the AMI-SEC Task Force [6].

1.4 Secure software engineering

If Smart Grid deployment is to gain trust among consumers, it is important to demonstrate that DSOs and vendors have taken every reasonable precaution to ensure security and privacy of installed systems. An important facet of this will be to demonstrate that the smart meters are developed according to accepted good practice for secure software engineering. This does not imply that units necessarily should be evaluated according to e.g. ISO/IEC 15408 (Common Criteria[2]), but rather that developers strive to follow industry guidelines such as BSIMM[3].

Note that secure software engineering is much more than ensuring that software security mechanisms perform as intended; even more importantly, it is about ensuring that "ordinary" software components are not designed with security flaws. Although the full details of how this can be approached is beyond the scope of this report, we encourage readers to consult e.g. McGraw and Chess [7] or the full BSIMM documentation.

[1] Spoofing of identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of Privileges

[2] http://www.commoncriteriaportal.org/

[3] http://www.bsimm.com

2 Background

Information security challenges of smart grid and AMI have been addressed by several actors. Below we introduce the resources that serve as important input to the threat assessment of Demo Steinkjer.

Line et al. [8] outline a number of challenges in smart grid security, including connectivity, new trust models, security management, software vulnerabilities and malware, and consumer privacy. These challenges are also reflected in the NISTIR 7628 report on Guidelines for Smart Grid Cyber Security [5], and this report also provides a lot of background material useful for future risk assessments. Of particular relevance are:

- Identification of important actors (organisations, buildings, individuals, systems, devices, etc.) and their interfaces
- A list of security requirements that are to some extent linked to the interfaces
- An overview of relevant vulnerabilities divided into vulnerability classes
- A list of potential security problems specific to the smart grid
- A set of key use cases for the smart grid, related to security objectives/requirements

The NISTIR 7628 vulnerabilities and security problems provide more information on several of the threats identified in the following sections. To facilitate use of the NISTIR report, we refer to individual sections of the NISTIR report, where relevant.

The components and interfaces that are part of AMI are covered in the NISTIR 7628 report. In addition, the AMI-SEC Task Force has published a security profile for AMI [6] defining the different components and a set of security requirements that are mapped to these components. A high level overview of the main cyber security issues of AMI has also been provided by Cleveland [9]. Relevant is also the security analysis of the Dutch smart metering systems performed by Keemink and Roos [10].

NVE has performed a risk analysis of AMI, which provides important background on the Norwegian context [4]. In the NVE risk analysis[4], a general AMI is described, and for each component there is a description of possible consequences of security breaches. A set of attack/unfortunate scenarios are presented, and they are assigned estimates for probability and consequences. The results are presented in a risk matrix, and a set of recommendations are provided at the end of the report. The high-risk incidents comprise one or more of the following:

- Unwanted power outage for several customers
- Software flaw
- Head End System at utility company fails or is used in the attack
- Internal personnel misuse knowledge and/or legitimate access

As the threat analysis of Demo Steinkjer only focuses on threats that come from the meter side, the two last incident types from the NVE analysis are not covered in this report. The main attention is also on malicious acts. The first incident type is studied in more detail, and several others are identified.

3 Demo Steinkjer in brief

Demo Steinkjer is a live lab offering infrastructure for testing new technology and new services. The first phase of the project is carried out in an area with 772 customers (see Figure 2).

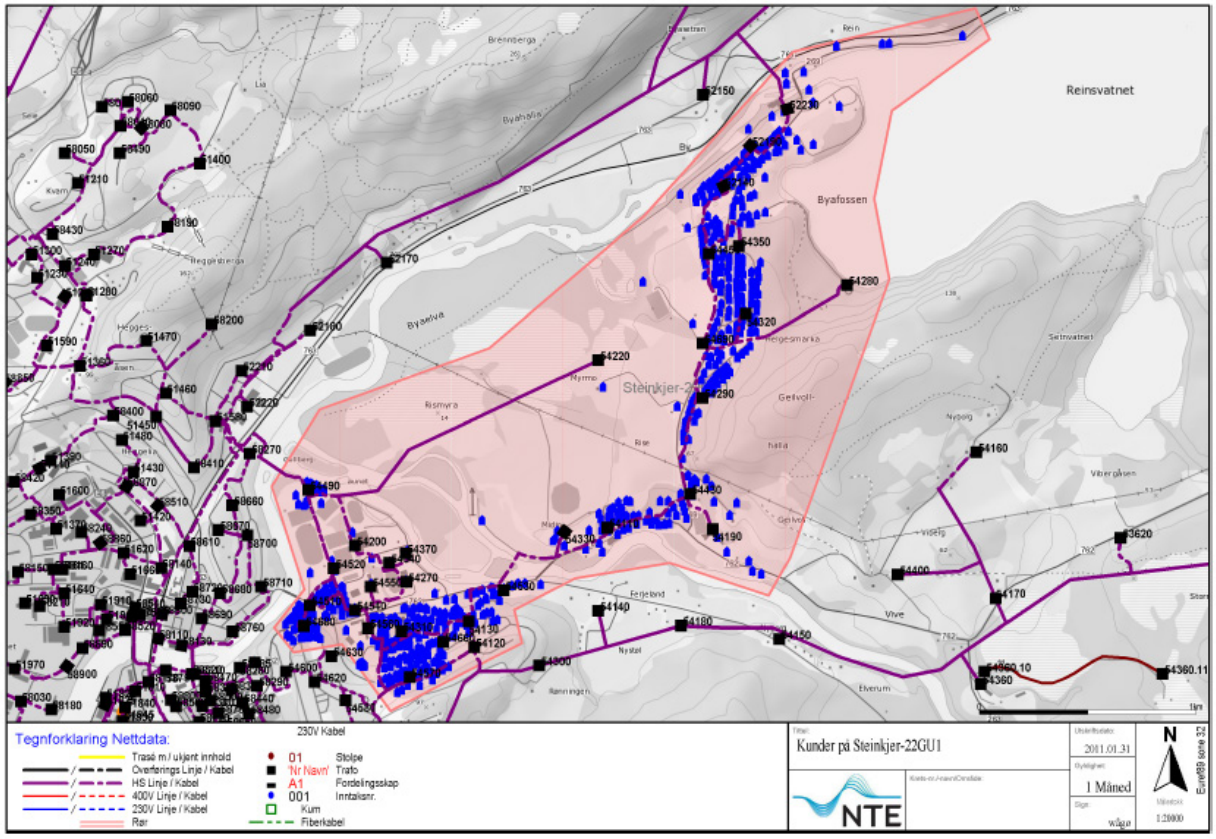


Figure 2: Deployment of Demo Steinkjer

In the first phase of the project, Demo Steinkjer is installing smart meters that are organised in a mesh network, as can be seen in Figure 3. The nodes of a mesh network communicate with the Head End System (HES) of the DSO via GPRS. In each mesh network, one node (the master node) will be responsible for communicating with the HES and the other nodes (the slave nodes) communicate with HES via that node. At the DSO, the data sent from the meters are made available to other systems, such as the distribution management system and systems for billing.

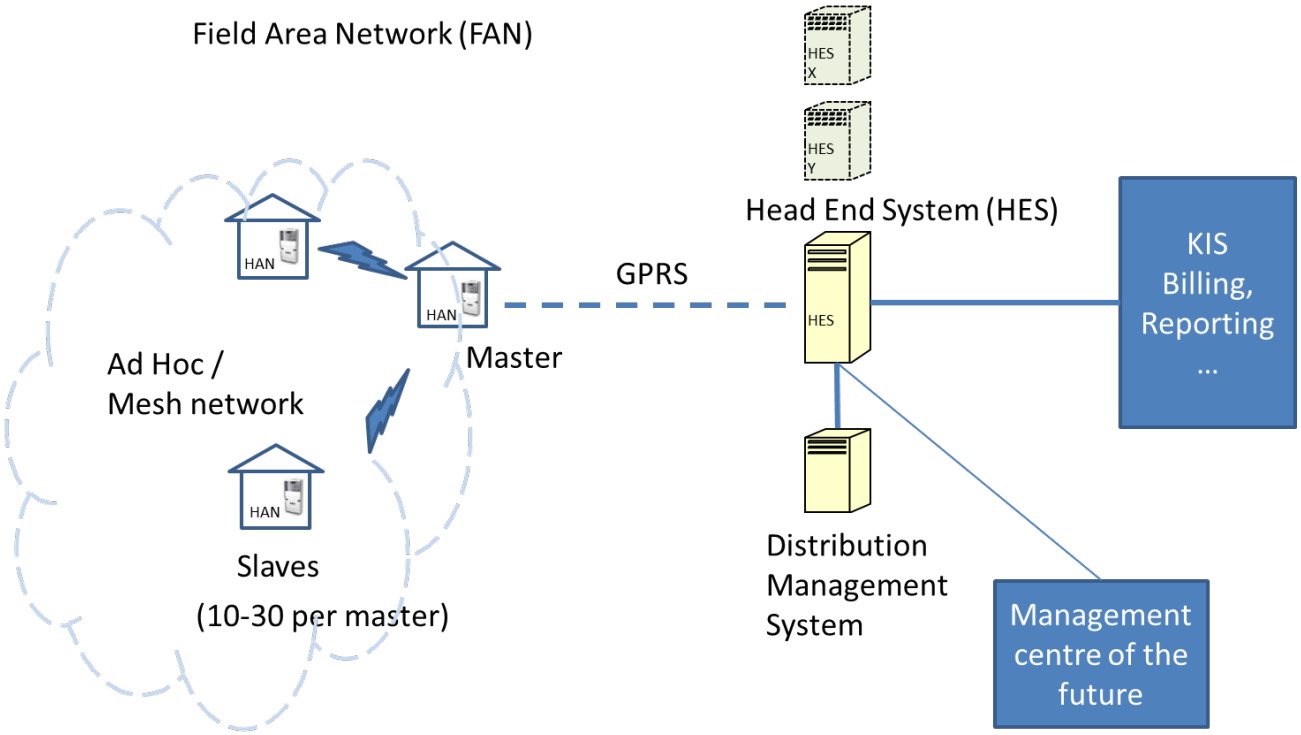


Figure 3: Demo Steinkjer conceptual layout

In general, a smart meter contains identity information that is used when reporting meter values. The meter performs analogue measurement of power consumption, and this is converted to a time-based value which is stored in internal memory, and accumulated and sent on to a Head End System at defined intervals. The smart meters used for Demo Steinkjer maintain an internal separation of duty as illustrated in Figure 4, where the metering application is responsible for performing the measurements, and the terminal is responsible for all processing and communication. This division also makes it possible for the smart meter manufacturer to impose separate restrictions on the two parts; e.g. some manufacturers only allow the terminal part to be changed via remote software update.

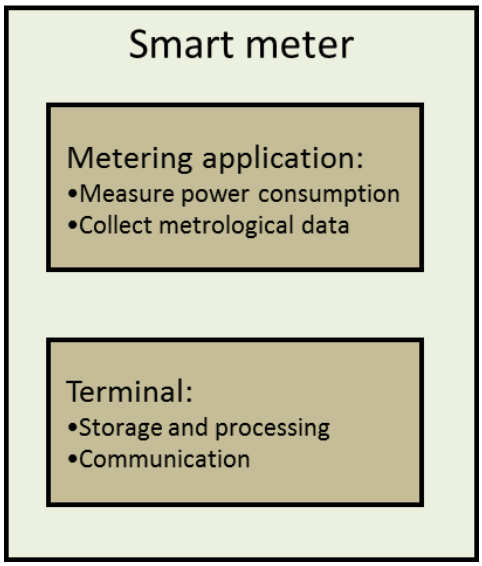


Figure 4: Internal separation of duty in smart meter

4 Threat overview and identification

Actors that want to attack a system need to have an interface to the system in order to be able to perform their deeds. In order to protect a system, it is important to have an overview of all the potential ways into the system, from an attacker's viewpoint. Thus, identification of a systems interfaces and an assessment of which threats are relevant at the interfaces, is useful in order to gain the necessary overview.

4.1 Data Flow Diagram of a master meter

Data Flow Diagrams (DFDs) provide an overview of the interfaces of a system, and how information flows on the interfaces. It is important to note that the DFD does not show any sequence in the data flow. The focus lies on where the different data is processed, stored and communicated, rather on how and when such processing, storage and communication occurs. A DFD of the master meter is shown in Figure 5. In the DFD, interactors[4] are represented as rectangles, processes as circles, data stores as horizontal lines and data flows as arrows.

As can be seen from the figure, a master meter has four main interfaces:

- An interface with HES (I1)
- An interface with other meters (slaves) (I2)
- An interface with third party equipment (e.g. displays) (I3)
- An interface towards maintenance personnel with physical access to the meter (I4)

In addition, meters have an internal interface between the metering application and the terminal. This interface is however not studied in any detail in this report, as it is not readily available for attackers. Slave meters have similar interfaces, except from the interface with HES.

A terminal has several important tasks:

- Report meter values at regular intervals
- Generate events
- Act on control messages (e.g. software updates, requests for readings, configuration updates, etc.)
- Respond to local maintenance
- Interact with third party equipment

Master terminals are also responsible for establishing and maintaining communication with HES. They also need to maintain the communication link with slave terminals in their mesh network, and forward messages to/from the slave nodes. Slave terminals can also take part in forwarding, if they are placed on route to the master node.

[4] "Interactors" is the term used in STRIDE for entities that interact.

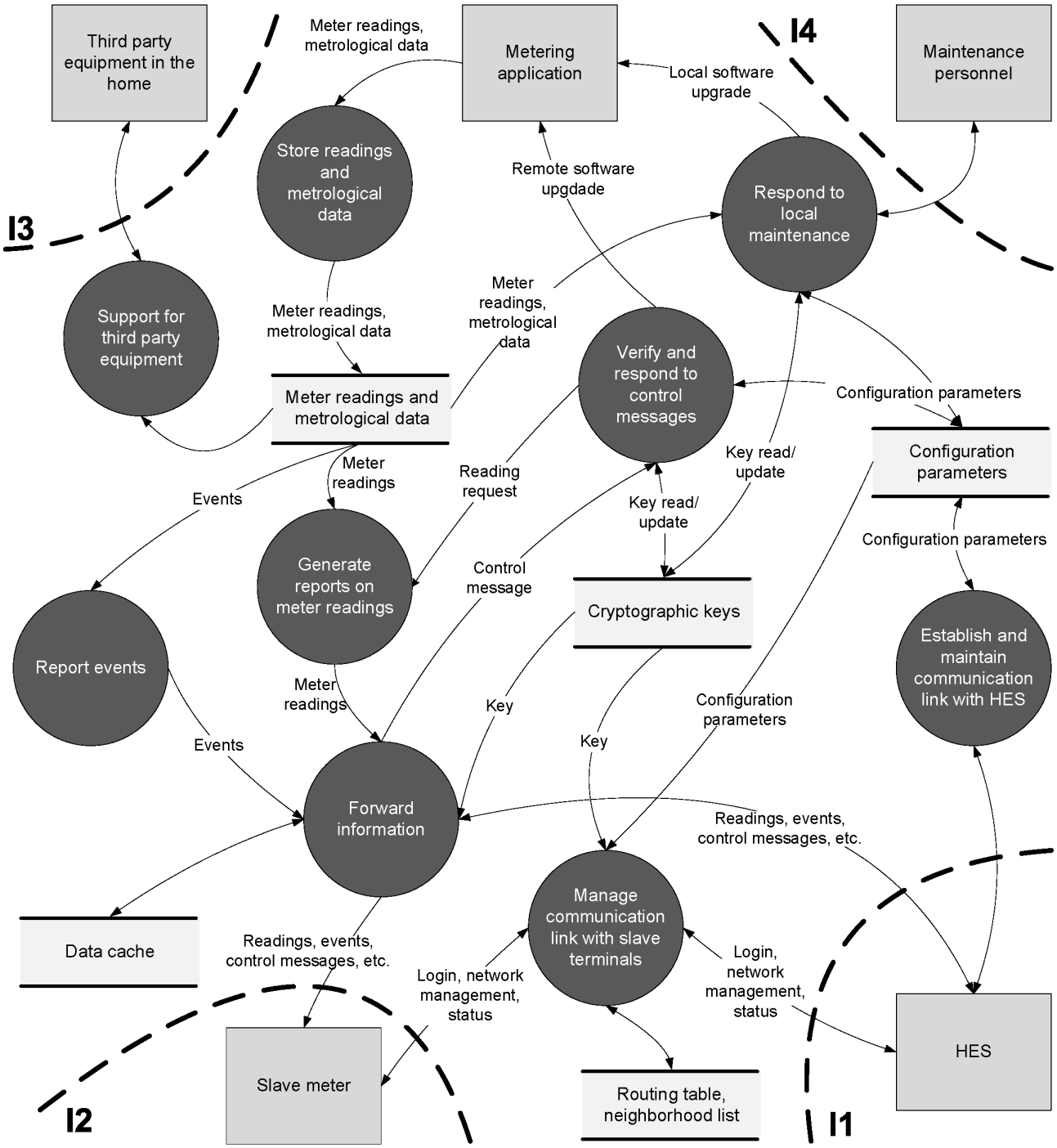


Figure 5: Overview of data flow related to a master meter

Master meters can be designed and implemented in several ways. It is not the aim of the DFD in Figure 5 to explain the internal design of a master meter. The focus lies on how information flows between the meter and other components, and also on typical processes you will find in meters.

To explain the type of information that can be deduced from the DFD, we look more closely at one of the meter tasks, as listed above: To report meter values at regular intervals. The typical actions necessary in order to generate such reports, and their representation in the DFD, is explained in Table 1 below.

Sequential actions assumed	Representation in the DFD
Metering application measures meter readings	Happens in the *Metering application* – not further detailed in the DFD
Meter reading is stored by the terminal	*Meter readings* from the *Metering application* is handled by the process *Store readings and metrological data*, that stores the *Meter readings* in an internal data store (named *Meter readings and metrological data* in the DFD)
Stored meter readings are used as a basis for creating a meter reading report	The process *Generate reports on meter readings* takes recent *Meter readings* from the internal data store, and generates a report based on those
The meter reading report is sent to HES, potentially protected by cryptographic means	The process *Generate reports on meter readings* sends the *Meter readings* to the process *Forward information* that is responsible for all message communication. This process can access the internal data storage named *Cryptographic keys* in the figure if encryption or signing of the message is to be performed before sending the *Readings* on towards the *HES*

Table 1 Reporting of meter values, as represented in the DFD

In the use of DFDs in this report, the attention lies on the communication on the interfaces identified. On these interfaces, the data travels from one trust zone to another (e.g. from one meter to another meter, or from a master meter to the HES), thereby exposing the data for attack.

In the subsections below, we explain the main communication on the interfaces I1-I4, and assess the relevance of the STRIDE threats for each interface. We also provide input on what aspects should be taken into account when assessing the degree to which a specific meter is vulnerable towards the threats. First, however, we provide a brief introduction to the STRIDE threat categorisation.

4.2 The STRIDE threat categories

STRIDE [11] has been given its name based on the first letter in the six threat categories that is covered: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges. In the following we briefly explain these threat categories.

Spoofing is defined by Swidersky and Snyder [11] as something that *"[a]llows an adversary to pose as another user, component, or other system that has an identity in the system being modelled."* Spoofing can be performed in order to be better positioned to perform further attacks, or may be an attack goal in itself (e.g. if wanting to report meter values as someone else)

Tampering refers to *"[t]he modification of data within the system to achieve a malicious goal."* [11] Tampering attacks the data integrity, a quality that is essential for AMI, e.g. for the purpose of billing [5].

Repudiation threats allow adversaries *"to deny performing some malicious activity because the system does not have sufficient evidence to prove otherwise"* [11]. Cleveland [9] points at accountability or non-repudiation as critical for AMI and its financial transaction, metrology information and responses to control commands.

Information disclosure results in *"[t]he exposure of protected data to a user that is not otherwise allowed access to that data."* [11] For power systems, data confidentiality is generally considered less important than data availability and integrity. However, AMIs communicate a lot of different data that should not be exposed, including private consumption data, encryption keys and certain control messages or software updates.

A *Denial of Service* (DoS) attack *"[o]ccurs when an adversary can prevent legitimate users from using the normal functionality of the system"*. [11] NISTIR 7628 [5] states that *"[a]vailability of meter data is not critical since alternate means for retrieving metering data can still be used."* AMIs, however, process a variety of data, and the dependence on e.g. timely alarms and control messages should be assessed.

Elevation of privileges occurs *"when an adversary uses illegitimate means to assume a trust level with different privileges than he currently has"*. [11]

4.3 I1: Master meter – HES

All meters will support two-way communication with HES. For slave meters this communication happens via other meters, while master meters have direct communication links with HES. As shown in Figure 5, different types of data are communicated on this link:

- Information needed to establish and maintain a communication link with HES
- Readings and events from meters
- Control messages, including software updates, configuration changes, meter reading requests and updated keys
- Any messages needed in order to allow master and slave meters to "login" to the HES. This may imply registering the presence of meters, authenticating meters towards the HES and getting access to necessary network keys. Messages may also be needed in order for the HES to maintain the status of the meters (e.g. to verify that the meters are still responding).

According to the AMI-SEC security profile for AMI [6], other types of data such as pricing data, prepayment information, meter read requests, and turn on/off commands are also communicated on this interface.

4.3.1 Spoofing

On I1 it is relevant to consider the risks related to spoofing of meter identities, as well as spoofing of the identity of the HES. This leads to two main threats[5]:

[5] These types of threats are also addressed by one of the cyber security problems listed in NISTIR 7628, namely "Authenticating Meters to/from AMI Head Ends" (7.2.5).

T1 Fake HES: Attacker is able to trick a master meter into believing that the meter is communicating with the HES, when in fact the meter is communicating with an attacker. This may lead to consequences of the following types:
  - Fake control commands to meter systems [10], including false circuit breaking and false software upgrades
  - Attacker gets access to all communication from the meters, including personal data

T2 Fake meter ID: A meter is able to change its identity, and potentially take the identity of another meter. As a result, meters can e.g. report meter values for other meters.

When considering whether a system is vulnerable to these threats it is important to consider:

- The mechanisms used to authenticate meters[6]
- The mechanisms used to authenticate the HES
- Who is in charge of initiating and establishing the communication link between master meter and the HES

4.3.2 Tampering

On I1, tampering of data can happen in three places: at the master node, at the HES or on the communication link between master and the HES. In this document we do not consider the security of the HES, and thus tampering at the HES is considered out of scope. When it comes to tampering at the master node this will be addressed in the analysis of the other interfaces (e.g. T16 Tampering before forwarding message, and T30 Local meter compromise (users physically tampering with their meter)). On the communication interface there is the following threat:

T3 Tamper with communication between HES and master meter: An attacker is able to tamper with data that is sent on the link between the master meter and the HES. This can result in errors in meter reading reports, wrong configuration settings, unauthorized changes of software, or erroneous or missing alarms. It can also open up for attacks on the HES or the master node (exploits). Attackers may modify messages or insert new messages.

When considering whether a system is vulnerable to this threat it is important to consider:

- The security of the communication infrastructure and protocols[7]
- The strength of the integrity protection (if present)[8]
- The strength of encryption (if present)

4.3.3 Repudiation

Cleveland [9] points at accountability or non-repudiation as critical for AMI systems and its financial transaction, metrology information and responses to control commands. As the security of the HES is out of scope for this study, we focus on the repudiation threats related to the meters:

T4 Meter denies having received a message: Some of the messages that can be sent to a meter are not necessarily beneficial to a customer/attacker (e.g. circuit breaking commands, or software updates

[6] See NISTIR 7628 and the vulnerability "Weaknesses in Authentication Process or Authentication Keys" (6.5.1.4)
[7] See e.g. the following cyber security problems described in NISTIR 7628: "Outsourced WAN links" (7.2.15), "Secure End-to-End Meter to Head End Communication" (7.2.10) and "Insecure Protocols" (7.2.24)
[8] See NISTIR 7628 and the vulnerability "Inadequate Integrity Checking" (6.5.1.1)

that set aside achievements made by an attacker). If there is no way to prove that a message has been received and should have been acted upon, it is difficult to be sure what caused the lack of response to a message.

T5 Meter denies sending of message: Due to errors or the malicious intent of an attacker, messages sent by a meter may cause harm to the HES or may contain erroneous alarms or meter reports. If there is no way to prove who is the sender of a given message, it is difficult to know the cause of any problems and if someone should be held responsible.

When considering whether a system is vulnerable to these threats it is important to consider:

- Integrity protection of messages
- The ability to prove the origin of a message, e.g. by the use of cryptographic techniques
- The ability to be sure messages have been received (the amount of responses required and if the integrity and authenticity of these responses are ensured)

4.3.4 Information disclosure

Information disclosure can happen on the communication links or at the two end points. As the security of HES is considered out of scope in this study, there are two threats to consider:

T6 Eavesdrop on communication between master and HES: Information sent on this communication link includes personal data such as meter readings, and also potentially confidential data such as software upgrades, configuration settings and alarms.

T7 Meter leaks configuration information: Compromised meters may leak sensitive information received from HES, including details on the software, configuration settings, encryption keys, etc.

When considering whether a system is vulnerable to the eavesdropping threat it is important to consider:

- The security of the communication infrastructure and protocols[9]
- The strength of any encryption used on the communication link

When considering to what extent meters can leak information it is important to consider:

- The ability to compromise the meter (covered by the threats T13 Remote access to meter and T30 Local meter compromise)
- Protection of essential parameters such as encryption key

4.3.5 Denial of service

In the below list of threats we mainly consider the unavailability of individual system components, such as a meter or HES. In addition it is important to consider the effects of having several meters unavailable simultaneously and at critical situations [9]. As the security of HES is out of scope, we do not consider threats where HES is the source of the availability problems, e.g. situations where HES locks out meters. The main threats concerning denial of service are:

T8 Denial of service attack on HES: The HES becomes unavailable due to an attack. The attack may be of two types:

- A distributed denial of service (DDoS) attack where a large number of meters together sends a large number of requests to the HES, rendering the HES unavailable for legitimate requests

[9] See e.g. the following cyber security problems described in NISTIR 7628: "Outsourced WAN links" (7.2.15), "Secure end-to-end meter to head end communication" (7.2.10) and "Insecure protocols" (7.2.24)

- Attackers/malware exploit vulnerabilities in HES in a way that makes the HES unavailable

T9 Meter errors/attacks make meter unable to communicate with HES: Errors on the meter side, or erroneous software or configuration updates make meter unavailable and/or unable to communicate with the HES. One example of such an update would be if the key used to communicate with the HES is erroneously updated.

T10 Communication failure on the link between HES and master meter: The communication link between the HES and the master meter may be unavailable or have insufficient available bandwidth. As an example, wireless links may be subject to intentional or unintentional interference and congestion[10]. If GPRS is used, this would include vulnerability of the GPRS communication, and also limited GPRS access due to (too) many master nodes per GSM/GPRS cell (i.e., per base station).

T11 Meter refuses to communicate with HES: Compromised master meters may refuse to set up communication link with the HES.

In addition to the above, the sending of a fake circuit break command could be considered a special case of denial of service (denial of power). This threat is however considered covered by threats T1 Fake HES, T3 Tamper with communication between HES and master meter, and T12 Remote access to HES.

When considering whether a system is vulnerable to these threats it is important to consider:

- The capacity of the communication lines
- The capacity of HES, and its abilities to withstand DDoS attacks[11]
- The software quality (both HES and meters), including the likelihood that there are critical security vulnerabilities in the software[12]
- Authenticity and integrity protection of software and configuration updates
- The ability to compromise the meter (covered by the threats T13 Remote access to meter and T30 Local meter compromise)

4.3.6 Elevation of privileges

On this interface, there are two systems that could be compromised, the HES and the meter, as represented by the following threats:

T12 Remote access to HES: Attackers/malware exploit vulnerabilities in HES in order to get access to and control HES. As a consequence, attackers have the same rights in the systems as those controlling HES.

T13 Remote access to meter: Attackers/malware exploit vulnerabilities in meters in order to get access to and control meter. As a result the meter is compromised and the data it holds (personal data as well as software, configuration settings and keys) are disclosed.

When considering whether a system is vulnerable to these threats it is important to consider:

- The software quality (both HES and meters), including the likelihood that there are critical security vulnerabilities in the software[13]

---

[10] See the security problem "Outsourced WAN links" (7.2.15) in NISTIR 7628.
[11] See NISTIR 7628 and the vulnerability "Insufficient Redundancy" (6.5.1.5)
[12] More details included on the section on Elevation of privileges below
[13] In NISTIR 7628, the section on software development vulnerabilities (6.3.1) provides an overview of important categories of software vulnerabilities relevant for a smart grid environment. Also relevant is the vulnerability "Unneeded Services Running" (6.4.3.2).

- The security mechanisms controlling software updates[14]
- The presence of malware protection software[15]
- The patching regime[16]
- The ability to detect software and configuration changes in a meter[17]

4.4 I2: Meter – Meter

For slave meters the communication with HES is achieved via a master meter (and potentially also other slave meters). As a result, the data communication on the link between meters is quite similar to the data communicated with HES, except from the data related to management of the communication link. As shown in Figure 5, the data communicated on this link include:

- Readings and events from meters
- Control messages (including software updates, configuration changes, meter reading requests and updated keys)
- Login management and messages needed to maintain status
- Data needed for network management

4.4.1 Spoofing

In the mesh network, the identities considered are mainly those of meters, and the main spoofing threat is:

T14 Fake master meter, or fake route to the master meter: A compromised slave meter, or some other IT equipment, claims to be a master meter, and tricks slave meters to send their communication via this fake master instead of the real master. Alternatively, a slave meter/attacker falsely claims to have the shortest route to the master, and thus tricks nodes into sending their messages via this fake slave node. Consequences of such an attack depend on the security measures in place, with denial of service and information disclosure as potential consequences.

In addition, the threat **T2 Fake Meter ID** applies.

When considering whether a system is vulnerable to these threats it is important to consider:

- The mechanisms used to authenticate meters[18].
- The protection mechanisms in the routing protocols, including any spoofing detection functionality of master meters[19]

4.4.2 Tampering

Tampering of data can happen while the data is sent on the communication link, or the data can be tampered with by nodes on route to HES. The main threats are:

---

[14] See the security challenge "Insecure Firmware Updates" (7.2.16) in NISTIR 7628
[15] See NISTIR 7628 and the vulnerability "Inadequate Malware Protection" (6.4.2.1)
[16] See NISTIR 7628 and the vulnerability "Lack of Prompt Security Patches from Software Vendors" (6.4.3.1)
[17] See NISTIR 7628 and the description of the security problem "Remote Attestation of Meters" (7.2.12)
[18] See NISTIR 7628 and the vulnerabilities "Weaknesses in Authentication Process or Authentication Keys" (6.5.1.4) and "Inappropriate Protocol Selection" (6.5.1.3)
[19] To what extent master nodes will detect if another node uses the master's identity.

T15 Tamper with communication in mesh network: An attacker is able to tamper with data that is sent on the wireless link of the mesh network. This can result in errors in meter reading reports, wrong configuration settings, unauthorised changes of software, or erroneous or missing alarms. It can also open up for attacks on the HES or the meter nodes (exploits). Attackers may modify messages or insert new messages.

T16 Tampering before forwarding message: Compromised meters, or some other IT equipment that claims to be a meter, tamper with messages before they are passed on towards their intended recipient (HES/meter node). This can result in errors in meter reading reports, wrong configuration settings, unauthorised changes of software or erroneous or missing alarms. It can also open up for attacks on HES or the meter nodes (exploits). Attackers may modify messages or insert new messages.

When considering whether a system is vulnerable to these threats it is important to consider:

- The security of the mesh network and its routing protocols[20]
- The strength of the integrity protection (if present)[21]
- The strength of encryption (if present)[22]

4.4.3 Repudiation

The repudiation threats in the mesh network are similar to that described above for the communication interface between meters and HES (**T4 Meter denies having received a message**, and **T5 Meter denies sending of message**), and the same considerations apply for considering whether a system is vulnerable to these threats.

4.4.4 Information disclosure

Information disclosure can happen on the communication links or at the meter nodes, the main threats being:

T17 Eavesdrop communication in the mesh network: Information sent on this communication link includes personal data such as meter readings, and also potentially confidential data such as software upgrades, configuration settings and alarms.

T18 Leaking of forwarded messages: Compromised meters, or some other IT equipment that claims to be a meter, leaks information from messages that are sent via them on route to their final destination.

In addition, the threat **T7 Meter leaks configuration information** also applies here.

When considering whether a system is vulnerable to these threats it is important to consider:

- The security of the mesh network and its routing protocols[23], including the ease of adding new slaves on route to the master
- The strength of any encryption used on the communication link

[20] See the security problem of "Protection of Routing Protocols in AMI Layer 2/3 Networks", section 7.2.13 in NISTIR 7628.
[21] See NISTIR 7628 and the vulnerability "Inadequate Integrity Checking" (6.5.1.1)
[22] Section 7.2.10 in NISRIT 7628 states the importance of end-to-end protection of meter to head end communication.
[23] See the security problem of "Protection of Routing Protocols in AMI Layer 2/3 Networks", section 7.2.13 in NISTIR 7628.

- The ability to compromise the meter (covered by the threats T13 Remote access to meter and T30 Local meter compromise)

4.4.5 Denial of service

The main threats concerning denial of service in the mesh network are:

T19 Denial of service attack on meter: A meter (slave or master) becomes unavailable due to an attack. The attack may be of two types:
  - A distributed denial of service (DDoS) attack where a large number of nodes together send a large number of requests to the meter under attack, rendering the meter unavailable for legitimate requests
  - Attackers/malware exploit vulnerabilities in a meter in a way that makes the meter unavailable

T20 Disrupt communication in mesh network: Attackers may disrupt the general ability to communicate in the mesh network in a number of ways, depending on the communication technology and protocols used. Mechanisms include jamming, dropping of packets, injection of false keys, etc. As a consequence, nodes in the mesh network are unable to communicate.

T21 Node lockout: Attackers may limit the ability of individual meters to communicate with other meters and with HES. Mechanisms include not forwarding messages from individual nodes, falsely rejecting login attempts from a node (message tampering), etc.

In addition to the above, the sending of a fake circuit break command could be considered a special case of denial of service (denial of power). On the mesh network, this threat is however considered covered by threats T15 Tamper with communications in mesh network and T16 Tampering before forwarding message.

When considering whether a system is vulnerable to these threats it is important to consider:

- The capacity of the communication lines and the general vulnerability of the communication technology and protocols
- The processing capacity of meter nodes, and their abilities to withstand DDoS attacks
- The software quality, including the likelihood that there are critical security vulnerabilities in the meter software[24]
- Authenticity and integrity protection of software and configuration updates
- The ability to compromise the meter (covered by the threats T13 Remote access to meter and T30 Local meter compromise) and the ease of adding new slaves on route to the master

4.4.6 Elevation of privileges

The mesh network consists of master and slave meters, all of which are at risk of compromise. This is covered by threat **T13 Remote access to meter**, and the same considerations apply for considering whether a system is vulnerable to these threats.

4.5 I3: Meter – 3rd party equipment

Figure 5 does not specify what data is exchanged between a meter and any third party equipment that may be connected to the meter. In the Dutch study [10] it is stated that this interface is read only. In the EU smart

[24] More details included on the section on Elevation of privileges below

grid task force work group 2 report [12] the data exchanged on this interface is summarised as meter reads, pricing info and tariff info. The AMI-SEC security profile [6] for AMI envisions that communication between a meter and a display will include various notifications, pricing data, consumption data and prepayment information. The communication will be initiated by the meter, and displays will mainly send confirmations in return. For other types of 3rd party equipment, such as load control devices, the information sent may be different, but the meter will still be the initiator of most of the communication.

In the following we assume that third party equipment will be allowed to request meter reads, and also that meter reads may be sent to third party equipment in a periodic fashion.

The security of the third party equipment itself and the means of communication towards these are considered out of scope for this study.

4.5.1 Spoofing

Spoofing of identity is not considered relevant, as we assume the meter is not considering the identity of the third party equipment, and as we are not aware of any benefits associated with modifying the meter ID towards third party equipment.

4.5.2 Tampering

As the third party equipment and the communication link towards this equipment is considered out of scope, we are left with tampering of data from third party equipment on the meter side. As we assume that no data, except for requests, are to be exchanged, tampering is not a threat.

4.5.3 Repudiation

It is possible to imagine scenarios where an erroneous message from a meter causes harm of third party equipment, and that the meter denies sending the message. This threat is however considered out of scope for this study.

4.5.4 Information disclosure

As the third party equipment and the communication link towards this equipment are considered out of scope, we are left with information disclosure on the meter side. A possible threat is:

T22 Meter leaks information about third party equipment: Compromised meters leak information on which third party equipment is connected to the meter.

The relevance of this threat depends on the types of equipment that can be connected to the meter, e.g. if it is possible to deduce from the information whether there are expensive equipment in the household.

When considering whether a system is vulnerable to this threat it is important to consider:

- What information about third party equipment is available to the meter
- The ability to compromise the meter (covered by the threats T13 Remote access to meter and T30 Local meter compromise)
- The ability for the meter to pass on any of this information

4.5.5 Denial of service

It should be considered to what extent third party equipment can pose a threat to the availability of the meter, as represented by the following threat:

T23 Meter unavailability caused by third party equipment: The meter becomes unavailable due to errors/attacks from third party equipment. This may happen in two ways:

- A high number of requests from third party equipment make the meter unable to perform other tasks
- Malicious requests from third party equipment exploit vulnerabilities in a meter in a way that makes the meter unavailable

When considering whether a system is vulnerable to this threat it is important to consider:

- The processing capacity of meter nodes
- The software quality, including the likelihood that there are critical security vulnerabilities in the meter software[25]

4.5.6 Elevation of privileges

Third party equipment represents a possible attack path for meters, if they are able to send requests to meters. It is possible to imagine scenarios where third party equipment is online and is compromised remotely, and that the attacker then tries to attack the meter via the third party equipment. It is also possible to imagine that the customer associated with the meter uses the interface towards third party equipment to attack the meter. These two threats are covered by threats **T13 Remote access to meter** and **T30 Local meter compromise**. The same considerations apply for assessing whether a meter is vulnerable to these threats.

4.6 I4: Meter – Local maintenance

Figure 5 does not specify what data is exchanged between a meter and any equipment used for local maintenance. In the AMI-SEC security profile for AMI [6], it is envisioned that field tools will send requests to meters for data and logs, in addition to commands, configuration data and test requests. Credentials for the field person may also be communicated. Meters will in turn send stored meter data and logs, confirmations and test results.

Meters that support the ANSI C12.18 or similar standards for optical communication can be read or written to using a hand-held device. The ANSI C12.18 standard supports configuring passwords to authenticate various read and write requests, but details on how to handle password management of devices in an enterprise setting are not part of the standard. Recent publicity around a "hacking tool" for smart meters [13] may be interpreted as an indication that some meters (or meter configurations) are vulnerable to attack, but there are to our knowledge currently no specific reports that confirm such vulnerabilities.

While considering threats towards the local maintenance interface in particular, we also include threats that come from attackers with physical access to the equipment (independent of the functionality that allows local maintenance).

[25] More details included on the section on Elevation of privileges, below

4.6.1 Spoofing

Regarding identities we do not consider the spoofing of meter identity towards local maintenance personnel, as this personnel will know where they are physically located and thus would know the real ID of the meter. Then we are left with threats related to the identity of the maintenance personnel:

T24 Attacker is authenticated as maintenance personnel: An attacker with physical access (e.g. a dishonest customer) is able to pose as maintenance personnel, and thus gets access to all functionality intended for maintenance personnel. Such functionality is likely to include software updates, configuration updates, and access to potentially sensitive data such as configuration settings, software and encryption keys.

When considering whether a system is vulnerable to this threat it is important to consider:

- The authentication scheme and the strength of the authentication mechanism used to authenticate maintenance personnel to meters[26]
- The functionality available to maintenance personnel, and also the additional checks required (e.g. integrity of software updates)

4.6.2 Tampering

Tampering can happen on the meter side or on the maintenance personnel side, as follows:

T25 Local maintenance alters meter data or software: Dishonest maintenance personnel or attackers posing as maintenance personnel modify meter values, configuration settings, software, or encryption keys.

T26 Meter reports wrong data to local maintenance: A compromised meter reports wrong data (e.g. meter values, configuration settings or test results) to maintenance personnel.

In this study we do not consider physical tampering with the metering software in order to change the power consumption measurements.

When considering whether a system is vulnerable to threat T25 it is important to consider:

- The system's vulnerability towards threat T24 Attacker is authenticated as maintenance personnel, and also the access rights of maintenance personnel
- The system's ability to detect such changes

When considering whether a system is vulnerable to threat T26 it is important to consider:

- The ability to compromise the meter (covered by the threats T13 Remote access to meter and T30 Local meter compromise)

4.6.3 Repudiation

The repudiation threat related to maintenance can be described as follows.

T27 Maintenance dispute: Meter falsely denies that maintenance has taken place and/or maintenance personnel deny maintenance or some of the actions taken during maintenance. The lack of ability to verify what has happened during maintenance can result in limited possibilities to identify the source of any meter problems.

[26] See NISTIR 7628 and the description of the security problem "Authenticating and Authorizing Maintenance Personnel to Meters" (7.2.3)

When considering whether a system is vulnerable to this threat it is important to consider:

- Any logging functionality in the meter or in the maintenance equipment, and the protection of the log itself

4.6.4 Information disclosure

The main threat to information disclosure on this interface comes from attackers that have physical access to the equipment. This physical access can be gained by spoofing the identity of maintenance personnel or by otherwise compromising the meter. This is covered by the threats T24 Attacker is authenticated as maintenance personnel, and T30 Local meter compromise. The threat related to the meter leaking information is covered by threat T7 Meter leaks configuration information.

4.6.5 Denial of service

The threats towards denial of service on the physical and maintenance interface are:

T28 Physical disabling of meter communication: Attackers with physical access to the meter can physically destroy the meter or disable its communication abilities (e.g. by disconnecting cables or by building a Faraday cage).

T29 Meter unavailability due to local maintenance: The meter becomes unavailable due to errors/attacks from local maintenance equipment. This may happen in two ways:

- A high number of local maintenance requests make the meter unable to perform other tasks
- Malicious local maintenance requests exploit vulnerabilities in a meter in a way that makes the meter unavailable

When considering whether a system is vulnerable to this threat it is important to consider:

- The capacity of meter nodes
- The software quality, including the likelihood that there are critical security vulnerabilities in the meter software[27]

4.6.6 Elevation of privileges

Attackers with physical access to the meter can try to compromise the meter in various ways[28]. Note that it is also possible to consider that compromised meters try to compromise any equipment used to perform local maintenance, e.g. in order to gain control of even more meters. This is however considered out of scope for this study. The main threat related to elevation of privileges on this interface thus is:

T30 Local meter compromise: A local attacker compromises the meter and thus gets access to the data and functionality of the meter. The attacker may:

- Physically connect to the maintenance port (or any other port) of the meter, and send requests/install software that exploits vulnerabilities in the meter
- Physically break open the meter

When considering whether a system is vulnerable to these threats it is important to consider:

[27] More details included on the section on Elevation of privileges below

[28] The vulnerability related to physical access to equipment is described in Section 6.5.1.6 of NISTIR 7628

- The software quality (both HES and meters), including the likelihood that there are critical security vulnerabilities in the software[29]
- The security mechanisms controlling software updates[30]
- The presence of malware protection software[31]
- The patching regime[32]
- The ability to detect software and configuration changes in the meter[33]
- The presence of any physical tampering detection mechanisms

4.7 Other interfaces

Some vendors may have a direct channel to the meters for firmware upgrades, support etc. This capability varies between manufacturers, in some cases only the terminal part of a smart meter may be upgraded via remote or over-the-air-provisioning (OTAP); the metrology part then cannot be upgraded without replacing the meter.

As this interface is very vendor specific, we exclude any details in this report.

[29] In NISTIR 7628, the section on software development vulnerabilities (6.3.1) provides an overview of important categories of software vulnerabilities relevant for a smart grid environment. Also relevant is the vulnerability "Unneeded Services Running" (6.4.3.2).
[30] See the security challenge "Insecure Firmware Updates" (7.2.16) in NISTIR 7628
[31] See NISTIR 7628 and the vulnerability "Inadequate Malware Protection" (6.4.2.1)
[32] See NISTIR 7628 and the vulnerability "Lack of Prompt Security Patches from Software Vendors" (6.4.3.1)
[33] See NISTIR 7628 and the description of the security problem "Remote Attestation of Meters" (7.2.12)

5 Attacker goals and strategies

5.1 Assets and threats

An asset is anything of value that needs protection; assets can comprise information, processes, physical devices and even intangible concepts such as reputation.

Table 2 shows the assets and threats revealed in the brainstorming session performed February 13, 2012. Participants in the brainstorming session were to write down potential assets related to smart metering in Demo Steinkjer on Post-it® notes, and the resulting assets and the potential threats towards the assets were discussed in the group. The list of assets and threats were then evaluated for completeness after the session.

As can be seen from the table, different types of assets were identified. In the following we do an assessment of the importance of an asset from an attacker's perspective, as a motivation for the attack trees described in the next subsection.

Among the identified assets, two have the potential to be key goals of attackers:

- A5 HES:
  - Using the meters to attack the HES and systems beyond HES
- A4 Meter values:
  - Getting access to consumption values/patterns of individual users
  - Modifying power consumption data in order to influence electricity bills

For the assets A1, A2, A3, A6 and A7, access to or control of the asset is not usually a mean in itself, but rather an important step on the way to achieve some other attack goal:

- Knowledge of the grid topology and configuration (A1) can be useful when planning attacks on the grid
- Spoofing of identities (A2) is a necessary step in many types of attacks
- Modification of control messages (A3) can be used as a mean to make the receiver of the message take some action to the advantage of the attacker. Such messages can also reveal important details about the system – that can be used further to perform attacks.
- Tariffs in meters (A6) are not sensitive, but unauthorised modification may have consequences for power stability.
- Access to meters (A7) is attractive due to the possibilities it brings when it comes to accessing information in the meter and using the meter in further attacks.

Based on the listed threats towards assets A2, A3, A6 and A7, important attack goals involving the compromise of these assets include:

- Causing instability in power delivery: E.g. by manipulation of tariffs (A6), by injecting false alarms (A3), or by sending fake circuit break messages (A3)
- Limiting the DSO's ability to control meters: E.g. by jamming or taking control of meters (A7) or by compromising the keys (A2)

Regarding A1, the configuration and topology of the grid cannot be directly deduced based on knowledge of the configuration and communication of the smart meters. Thus the main threats towards this asset do not come from the introduction of smart meters. It is therefore not considered further in this report.

ID	Asset	Description	Threats
A1	The configuration/topology of the grid	Information on the grid configuration /topology can be useful for performing further attacks	Social engineering
A2	The identities of meters	The identity of a meter is tied to the authentication performed and the encryption keys. For a DSO it is important to be able to correctly identify meters and know which meter is associated with a given message.	Compromised or broken keys (brute force or otherwise) Unauthorised change of meter identity
A3	Control messages	Include messages such as alarms, management events and system status.	Injection of false control messages, including alarms Attacker gets access to choke function for several subscribers Buffer overflow attack by crafting oversize control message Attacker assumes remote control of smart meter
A4	Meter values	Can reveal consumption values/patterns Covers both values stored in meter and communication between household and Distribution Service Organisation	Delete metering data Modification of communication GPRS eavesdropping General eavesdropping
A5	HES	Meters could be used in order to attack the HES	FAN access used to break into central systems (HES and beyond) Unauthorised modification of HES
A6	Tariffs in meter	Incorrect tariff information may cause consumers to change their consumption pattern	Large-scale tariff manipulation may cause instability in the power grid
A7	Meter (the actual box)	All threats to a slave meter also apply to the master meter, but a successful attack on a master meter has a greater impact. Master meter is additionally vulnerable to GPRS-based attacks. Attacks can also originate with the subscriber that controls the premises where meter is located.	Manipulating power measurement (physically) Manipulating measurement values Manipulating messages from meter Physical break-in USB autorun Break-in via Ethernet-port Report consumption/Status as other subscriber Jamming

Table 2: Assets and threats from brainstorming session

5.2 Attack trees

The asset identification process revealed the following attack goals, which have been further described by attack trees:

- Unauthorised access to power consumption data
- Manipulation of power consumption values (influencing electricity bills)
- Attackers cause instability in power delivery
- Attackers are able to limit the DSO's ability to control meters
- The meters are used to attack the HES

In the subsections below, attack trees are used to describe how attackers may go about achieving the above attack goals. The notation used for attack trees are explained in Figure 6. The main attack goal described in the tree is found at the top of the tree. Then the branches show how attackers may go about achieving the top goal. In the trees, all attack goals have been given a unique ID in order to be able to refer to attack paths described in other trees.

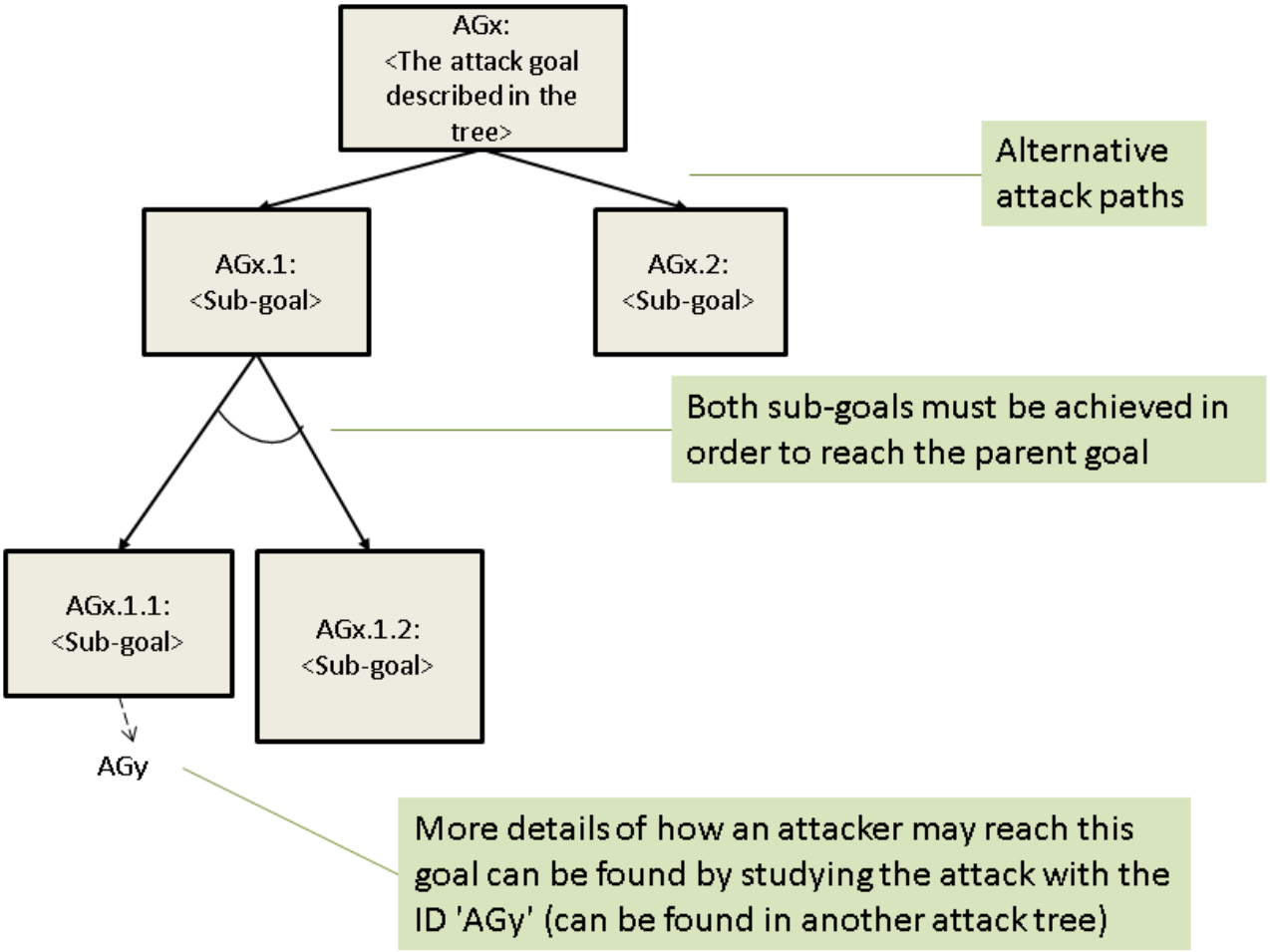


Figure 6: Attack tree notation

In the explanations of the attack trees, we refer to threats identified in the previous section, where relevant.

5.2.1 Unauthorised access to power consumption data

Power consumption is often considered personal, as it can reveal details about the daily life of individuals, or a limited number of people. Thus, protecting this type of data is important from a privacy perspective. The attack tree in Figure 7 describes how attackers may gain access to power consumption data, either by getting access to the values stored in meters or by picking up the values as they are sent to the HES.

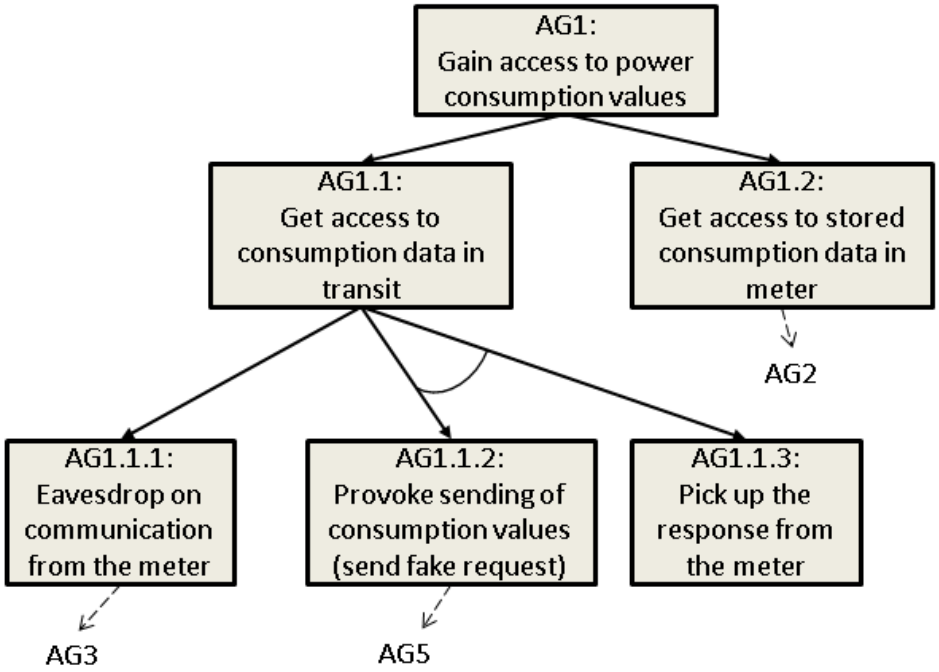


Figure 7: Attack tree - Gain access to power consumption values (AG1)

Access to stored meter values implies gaining access to the meter. The possible ways in which attackers may compromise a meter is described in the attack tree in Figure 7. If the attacker has physical access to the meter it is possible to perform a local attack, e.g. by tampering with the physical meter (T30). For most attackers, however, a remote meter compromise is an easier option (T13). Such a compromise may be achieved if an attacker is able to trick the meter into installing malicious software (through the software update feature), by using an exploit, or by gaining access to the vendor interface (if present). Central in these types of attacks is the ability to send malicious messages to meters. This is covered by the attack tree of Figure 11, but before going more into detail about how such modification may take place, we describe how attackers may gain access to consumption data as it is communicated on the network.

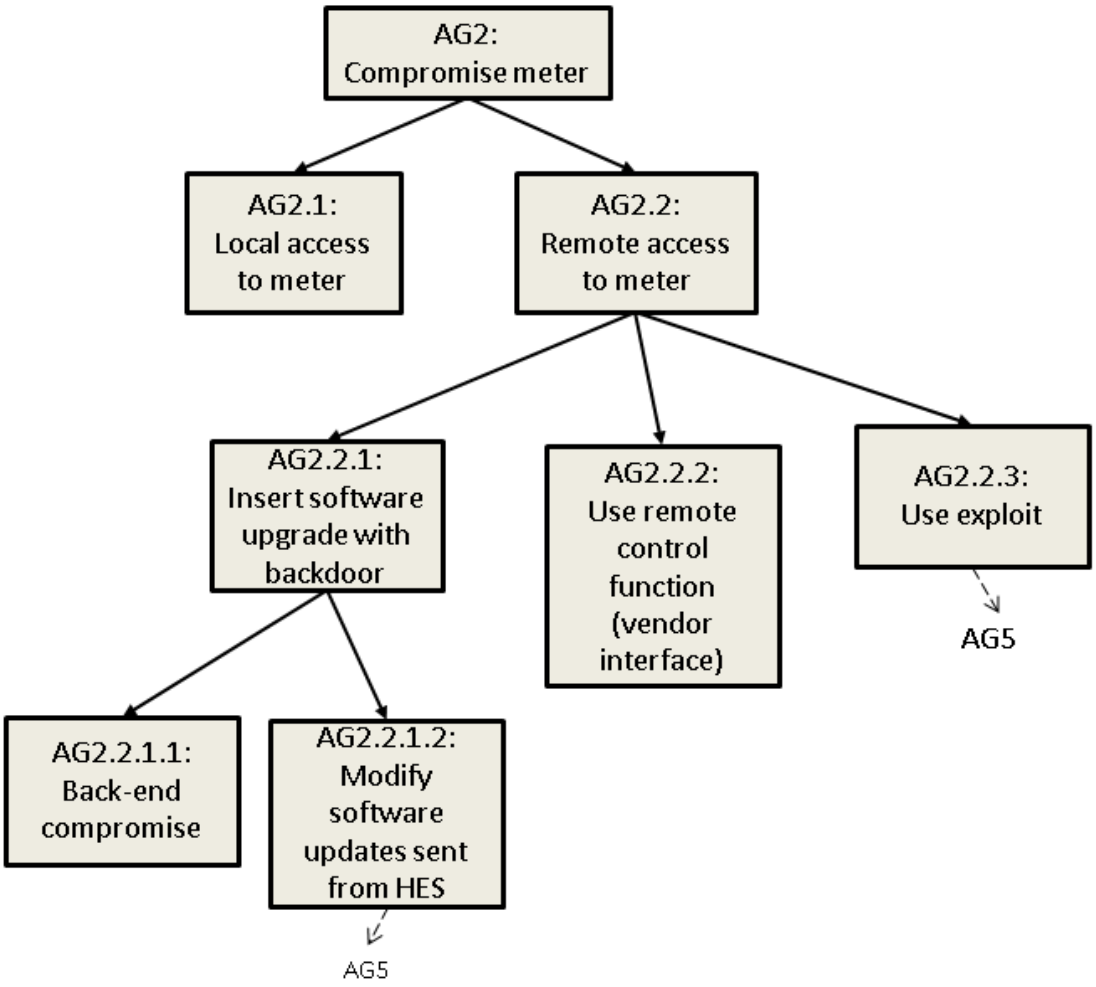


Figure 8: Attack tree – Compromise meter (AG2)

Attackers may gain access to consumption data by eavesdropping on the network traffic, and study the relevant messages. This is explained in more detail in the attack tree of Figure 9. Attackers may get access to communicated messages either by listening in on the communication channel (the GPRS link (T6) or the wireless link used in the mesh network (T17)) or by posing as a man in the middle (T1, T14). If information is encrypted, attackers will also need to be able to decrypt messages in order to get access to the actual consumption values. If attackers need access to encryption keys, these need to be retrieved from the holders of the key (it being meters or the HES), or cracked (e.g. by using brute force techniques) (see the attack tree in Figure 10).

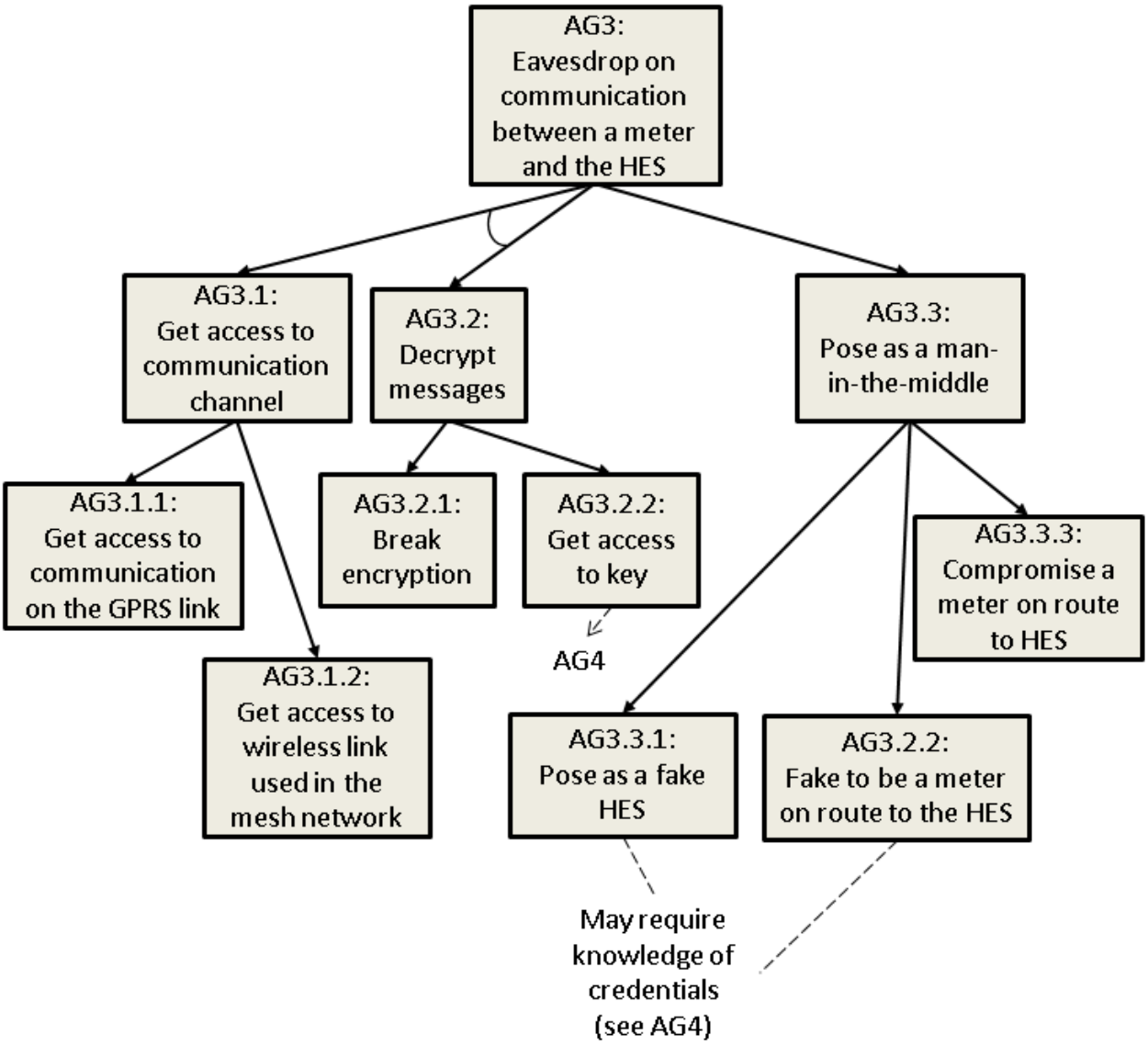


Figure 9: Attack tree – Eavesdrop on communication between a meter and the HES (AG3)

For attackers that are not that patient, it is also possible to send messages to the meter in order to provoke the meter into sending meter readings (e.g. by sending read requests). In order to do this, attackers must be able to modify the communication towards the meter (see the attack tree in Figure 11), either by inserting a message or picking up and modifying an existing message (T3, T15, T16). If the communication is cryptographically protected, this may require knowledge of the key.

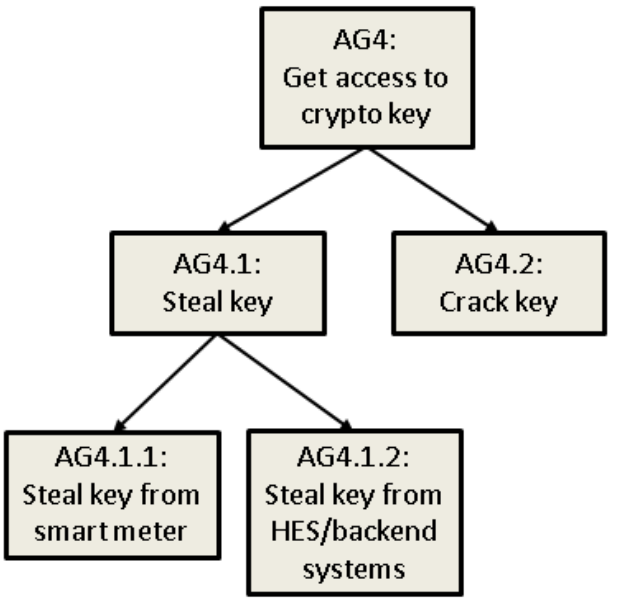


Figure 10: Attack tree – Get access to crypto key (AG4)

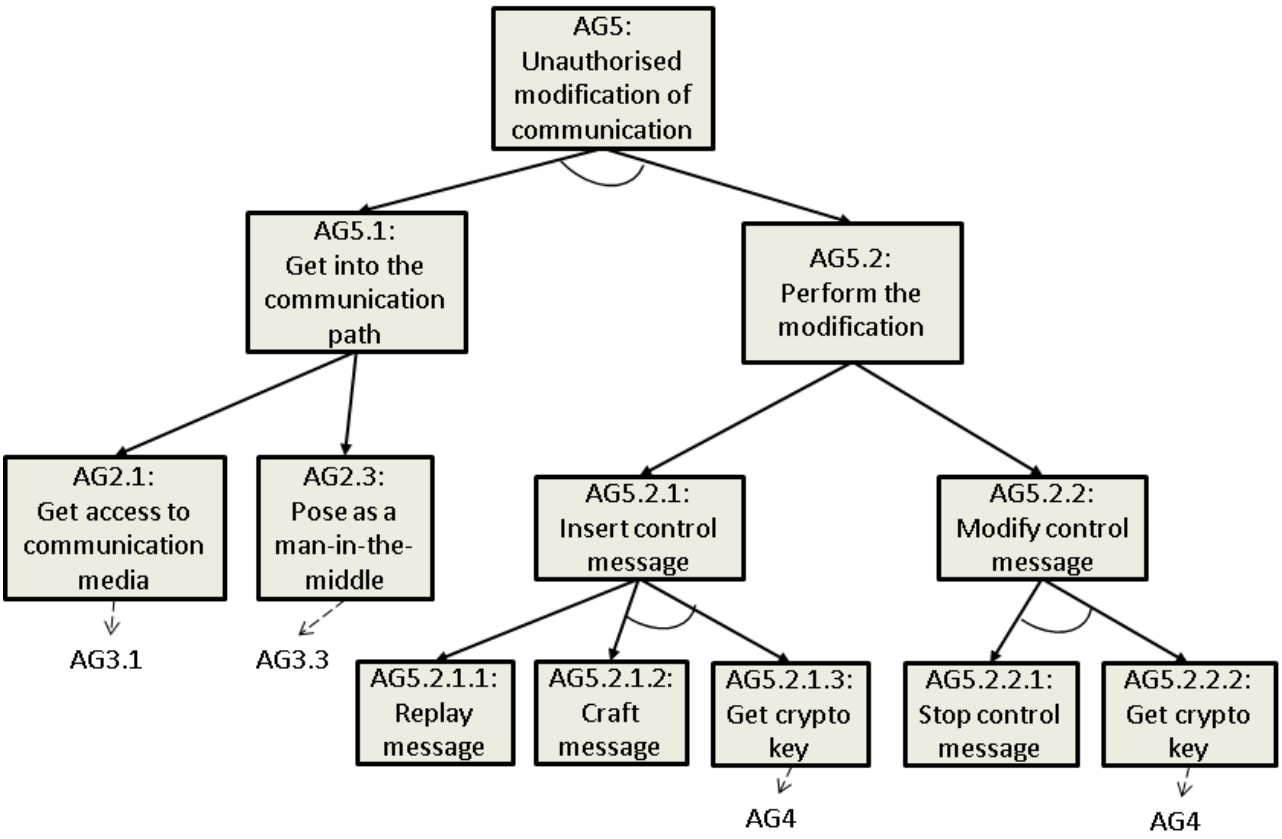


Figure 11: Attack tree – Unauthorised modification of communication (AG5)

5.2.2 Manipulation of power consumption values (influencing electricity bills)

Power consumption values reported to the HES directly impact the power consumption bill received at some later stage. Thus, manipulation of reported meter values is a potentially attractive attack goal. House owners may wish to change their own consumption values. Attackers may also want to change consumption values of other customers, e.g. to hide manipulation of own values.

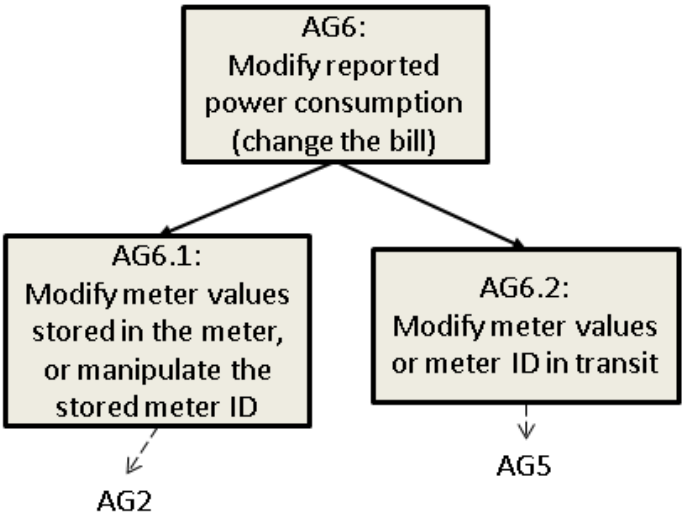


Figure 12: Attack tree – Modify reported power consumption (change the bill) (AG6)

As shown in the attack tree of Figure 12, power consumption values may be modified while stored in the meter (local tampering (T30) or remote access(T13)), or while sent on the network (T3, T15, T16). It is also possible to manipulate the meter ID associated with the meter value (T2) in order to report the consumption as another customer. However, this may be more easily detected by the HES, as it will not receive meter readings from the meter at the expected time.

5.2.3 Attackers cause instability in power delivery

Reliability in power delivery is essential in our modern society. Thus, it is important to investigate whether the introduction of AMI may pose challenges to power reliability. The attack tree in Figure 13 shows three main ways in which attackers may use meters in order to cause instability of power delivery.

Meters come with the functionality necessary in order to turn off power remotely. If attackers are able to send fake circuit breaker messages that are accepted by the meters, they can effectively turn off the power at any customer they can reach from their position in the network. However, instable power delivery can also happen in more subtle ways. In the future, we may have smart homes and smart devices that automatically adjust the power consumption based on the current tariff. Attackers may be able to manipulate the tariffs sent to meters, so that the meters e.g. falsely believe the price has dropped at a time when the distribution network is performing close to its limits. This may result in several appliances turning on at the same time, potentially causing instability of the distribution grid [14].

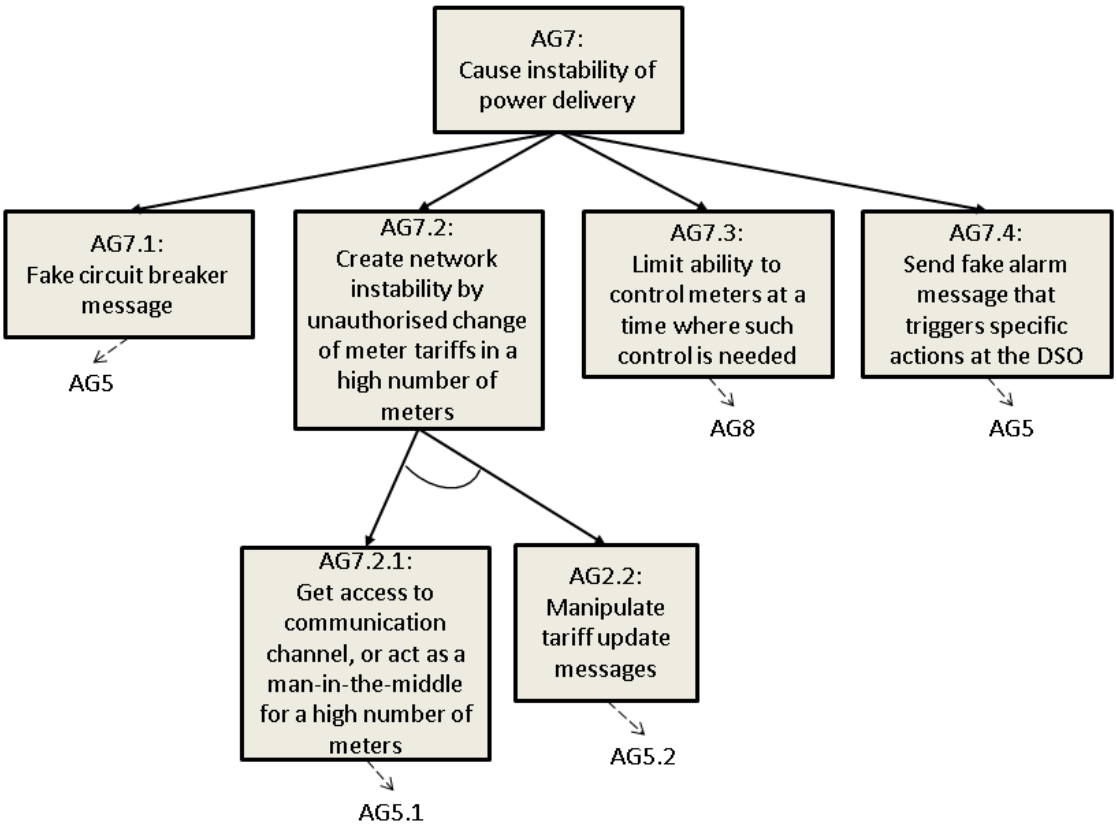


Figure 13: Attack tree – Cause instability of power delivery (AG7)

Meters can also play an important role in the ability to control power delivery in case there is a problem. The circuit breaker functionality can be used to shut down power at critical times, in order to maintain power delivery to prioritised customers. This however relies on the meters being available at such points in time. In case of an attack on the infrastructure, the consequences may increase if the meters are also attacked, and are not available for control purposes. This is further addressed in the subsection below.

Another attack scenario is that attackers send fake alarm messages to the HES, in order to trigger the DSO to take actions in order to deal with the alarm. If the attack goals it to cause instability in power delivery, attackers would aim at provoking the DSO to take actions that will result in disruption of power delivery for certain customers or in certain areas.

5.2.4 Attackers are able to limit the DSO's ability to control meters

Problems in meter management can be achieved in several ways, as shown in the attack tree in Figure 14. If the security mechanisms opens up for lockout of meters (e.g. due to use of wrong credentials), then attackers may provoke meter lockouts (T21). Similarly, if attackers are able to damage the keys used for authentication and communication (e.g. by sending a fake key update message), communication with the meter will be hampered. Meters can also be put out of action by sending fake shutdown messages.

Communication problems can also cause meter unavailability. Attackers may attack the network channel (T10, T20) or act as a man-in-the-middle and drop the packets. Attackers may also perform general denial of service attacks on a meter or a group of meters (T19).

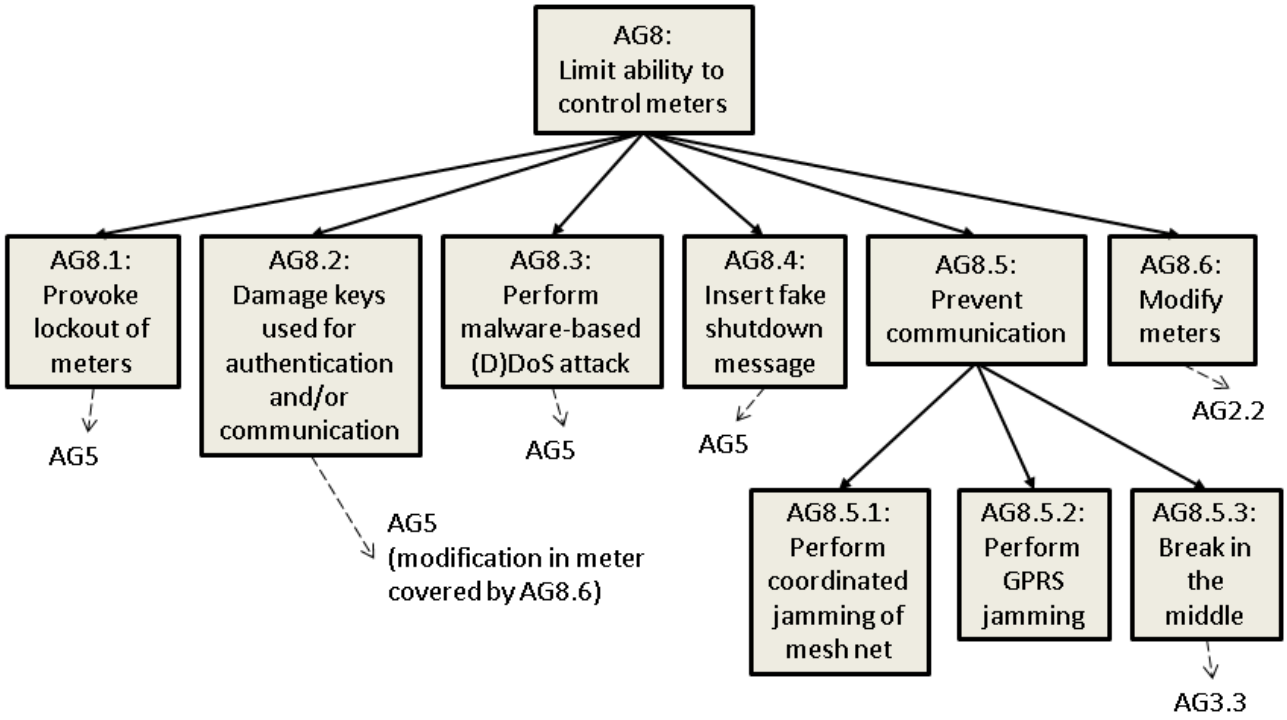


Figure 14: Attack tree – Limit ability to control meters (AG8)

The ability to control meters may also be reduced if attackers are able to compromise the meter and change its functionality (T9, T11).

5.2.5 The meters are used to attack the HES

The HES and other systems of the DSO become more exposed to attacks due to the new communication channel that comes as a result of the introduction of AMI. It is therefore important to assess whether meters can be used in order to attack the HES. The attack tree in Figure 15 shows two main strategies that can be used in order to attack the HES from the meter-side.

The potentially high number of meters makes it possible to use the meters to perform distributed denial-of-service attacks on the HES (T8). To do this, attackers need to gain control of a high number of meters, and coordinate these in order to overload the HES with requests. The HES may also be attacked by using exploits that take advantage of vulnerability in the HES software. To do this, attackers need to be able to send unauthorised messages to the HES.

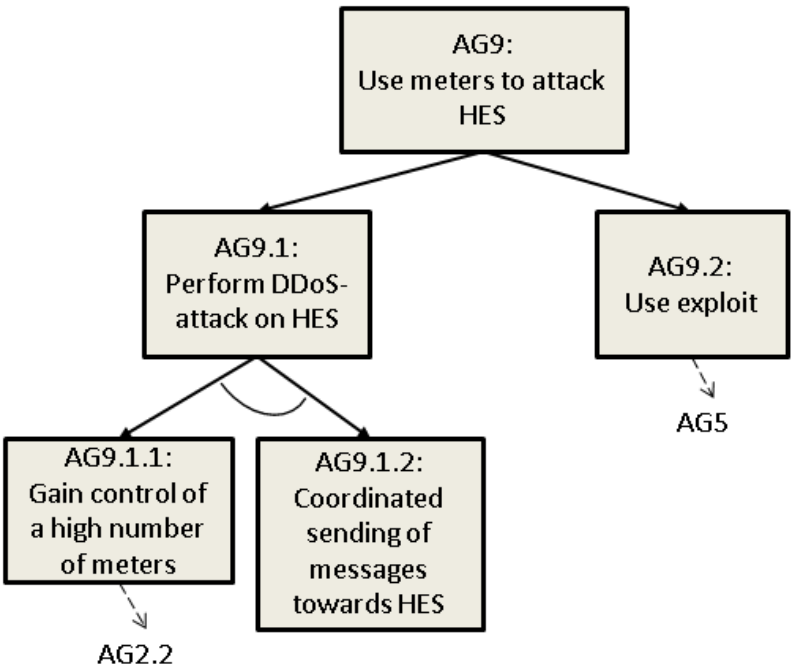


Figure 15: Attack tree – Use meters to attack HES (AG9)

6 Privacy

Some threats to end-users' privacy are covered in the above presented threats and attack trees, but we have not aimed to cover all privacy issues related to AMI in this threat assessment. However we would like to include some general remarks on the issue. Preserving privacy is an essential challenge that must be properly addressed in order for the AMI deployment to be a success.

When smart meters are deployed, the utility companies will automatically receive measurements collected much more frequently than today; usually several times a day. For billing purposes, hourly readings are needed, but for grid management purposes the DSOs can make use of per-minute readings or even per-second readings. These are huge amounts of data related to each household. Usage data must be kept confidential as they can tell a lot about the lifestyle and habits of the specific household. In its most simple form it will clearly show when someone is at home and when the house is empty, which is interesting information for someone planning robberies. More detailed readings can reveal information on which activities take place inside the house, as many household appliances have unique signatures that can be read from fine-grained metering data [15].

There is no doubt that usage data must be protected from unauthorized inspections, and there must be clear rules and guidelines in place describing what this data may be used for and who should have access. This is already the case for other similar large-scale collections of personal information, like money transactions, phone calls and broadband usage.

It should be carefully considered whether users would be interested in controlling their own privacy. The majority of end-users will probably not be able to understand their privacy exposures and even less able to understand how to mitigate them. The services provided must therefore be privacy-preserving and trusted by default; the principle of privacy-by-design should be followed at all times during development and in operation; such that the customers do not have to be concerned about their own privacy.

For further information, please refer to the guidelines by the Norwegian Data Inspectorate [16] .

7 Concluding remarks

This report has provided an overview of potential threats towards AMI solutions. Identification of threats is an important step in understanding the risks of a system, and evaluating whether a system is adequately protected. When threats have been identified, it is however necessary to assess the system's level of vulnerability towards the threat, and also the potential consequences of a breach. Due to the open nature of this report, full risk analysis details cannot be included, as this would violate confidentiality agreements with vendors and DSOs. Such details are being documented in a separate report which will have a much more restricted distribution. In this document, you thus only find input that can be used in performing such an assessment, in particular:

- Indications of which factors should be considered when evaluating a systems vulnerability towards the identified threats in section 4 (*Threat overview and identification*).
- Identification of relevant attacker goals in section 5 *(Attacker goals and strategies*).

This report only identifies threats, but do not prioritise them and also do not suggest how to mitigate them. Thus, this document should not be considered in isolation, but rather be viewed as important input to the work on information security that already takes place at the vendors and DSOs. It will also be used as a basis for the work on risk analysis that is taking place in the DeVID project. The aim of this report has been to better understand the threats facing AMI systems. Understanding is the first step, but needs to be followed by wise decisions and actions.

8 Acknowledgements

The work presented in this report has been made possible due to the support from Telenor and the collaboration with NTE and Aidon. Expertise from the Demo Steinkjer project has participated in workshops where assets and threats have been identified and discussed, and have contributed with comments to the technical content of the report. Aidon has contributed with input on how smart meter solutions may be realized. Thanks also to the Norwegian Smartgrid Centre for their support of the Demo Steinkjer project.

Figure 1 is based on a figure created by Hanne Sæle, SINTEF Energy.

A References

[1] A. Shostack, "Experiences Threat Modeling at Microsoft," presented at the Modeling Security Workshop, Toulouse, 2008.

[2] M. G. Jaatun and I. A. Tøndel, "Covering Your Assets in Software Engineering," presented at the Second International Workshop on Secure Software Engineering (SecSE - ARES 2008), Barcelona, Catalonia, 2008.

[3] B. Schneier, "Attack Trees - Modeling security threats," *Dr. Dobb's Journal,* 2001.

[4] M. B. Line*, et al.*, "Risikovurdering av AMS," SINTEF ICT, Trondheim SINTEF A22318, February 2012.

[5] P. Liu*, et al.*, "Automated planning for incident response based on CBR," 2010, pp. 403-406.

[6] L. Bass*, et al.*, "SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE," EnerNex CorporationJune 22 2010.

[7] G. McGraw and B. Chess. (2008, Software [In]security: A Software Security Framework: Working Towards a Realistic Maturity Model. *informIT*. Available: http://www.informit.com/articles/article.aspx?p=1271382

[8] M. B. Line*, et al.*, "Cyber Security Challenges in Smart Grids," presented at the IEEE ISGT, Manchester, UK, 2011.

[9] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1-5.

[10] S. Keemink and B. Roos, "Security analysis of Dutch smart metering systems," Universiteit van Amsterdam2008.

[11] F. Swiderski and W. Snyder, *Threat Modeling*: Microsoft Professional, 2004.

[12] "TASK FORCE SMART GRIDS - EXPERT GROUP 2: REGULATORY RECOMMENDATIONS FOR DATA SAFETY, DATA HANDLING AND DATA PROTECTION," FEBRUARY 16 2011.

[13] D. Fisher. (2012, Termineter Security Framework for Smart Meters Released *Threatpost*. Available: http://threatpost.com/en_us/blogs/termineter-security-framework-smart-meters-released-072012

[14] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," *Smart Grid, IEEE Transactions on,* vol. 2, pp. 667-674, 2011.

[15] M. A. Lisovich*, et al.* (2010) Inferring Personal Information from Demand-Response Systems. *IEEE Security & Privacy*. 11-20.

[16] "Guide for processing of personal data in connection with automatic metering systems within the energy sector," Norwegian Data Inspectorate2010.

Technology for a better society

www.sintef.no