Smart Meter Controls Whitepaper

Document Name:	compass_security_smart_meter_controls_whitepaper_v1.0.docx
Version:	v1.0, released on Hack In Paris 2014
Author(s):	Cyrill Brunschwiler, Compass Security AG
Date of Delivery:	June 19th, 2014
Classification:	PUBLIC

Executive Summary

Government requirements [1], [2], new business cases and consumer behavioural changes [3], [4] drive energy market players to improve the overall management of energy infrastructures.

While the energy infrastructure is steadily maintained and improved, some significant changes have been introduced to the power grids of late. Actually, the significance of the changes could be compared to the early days of the Internet where computers started to become largely interconnected. Naturally, questions arise whether a grid composed of so many interacting components can still meet today's requirements for reliability, availability and privacy.

Nations absolutely recognise the criticality of the energy infrastructure for their economic and political stability. Therefore, various initiatives to ensure reliability and availability of the energy infrastructures are being driven at nation as well as at nation union levels. In order to contribute to the evaluation of national cyber security risks, the author decided to conduct a security analysis in the fields of smart energy.

Utilities have started to introduce new field device technology - smart meters [5]. As the name implies, smart meters do support many more use cases than any old conventional electricity meter did. Not only does the new generation of meters support fine granular remote data reading, but it also facilitates remote load control or remote software updates. Hence, to build a secure advanced metering infrastructure (AMI), communication protocols must support bi-directional data transmission and protect meter data and control commands in transit.

To justify the scope of this whitepaper, a brief introduction into smart metering is provided. Moreover, relevant security standards and guidance are being referenced.

The paper aims to identify assets, threats and mitigating controls for smart metering using the OCTAVE Allegro risk assessment method [6]. The result is a collection of 43 controls which apply to any smart meter environment. Although the analysis is tailored to the analysis of the wireless M-Bus, the listed controls provide a good basis for metering companies, utilities or meter manufacturers to verify their meters protection level. During this analysis it has been recognised that legal aspects need to be clarified. Not only does the frequency of meter readings affect the consumer privacy, but also the records management at the metering company. Besides, it is not always clear who the owner of the consumption data is. This largely depends on local culture and law.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACC	Access Number
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMR	Advanced Meter Reading
ANSI	American National Standards Institute
BAN	Building Area Network
BCP	Business Continuity Management
BS	British Standard

BSI	British Standards Institution
BSI Germany	Federal Office for Information Security (BSI) in Germany
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CI	Control Information Field
CIA	Confidentiality, Integrity and Availability
CIRT	Computer Incident Response Team
COSEM	Companion Specification for Energy Metering
CPP	Critical Peak Pricing
D	Detective Control
DARPA	Defence Advanced Research Projects Agency
DER	Distributed Energy Resource
DFD	Data Flow Diagram
DG	Distributed Generation
DLMS	Device Language Message Specification
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DoS	Denial of Service
DSL	Digital Subscriber Line
DSO	Distribution System Operator
DSS	Digital Signature Standard
ECRYPT II	European Network of Excellence in Cryptology II
ENISA	European Network and Information Security Agency
EU	European Union
ETSI	European Telecommunications Standards Institute
FAN	Field Area Network
FIPS	Federal Information Processing Standards
FOC	Fibre Optic Cable
GPRS	General Packet Radio Service
GND	Common Ground
HLS	High Level Security
HVAC	Heating, Ventilation and Air Conditioning
EN	European Standard
Enc	Encryption Algorithm
EURELETRIC	Union of the Electricity Industry
EV	Electrical Vehicle
HAN	Home Area Network
HDLC	High-Level Data Link Control
HES	Head-end System
HHU	Hand-held Unit
IAN	Industrial Area Network
ICS	Industrial Control System
IV	Initialization Vector
IoT	Internet of Things
ISMS	Information Security Management Systems
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International organisation for Standardization
IT	Information technology
JAR	Jam and Replay Attack Technique
JTAG	Joint Test Action Group
KEK	Key Encryption Key
kV	Kilovolts
kWh	Kilowatt hour
LMS	Local metrological network
M2M	Machine to Machine
MAC	Message Authentication Code

MDM	Meter Data Management
MitM	Man-in-the-Middle
MK	Master Key
MPLS	Multi-protocol Label Switching
MW	Megawatts
N/A	Not applicable
NAN	Neighbourhood Area Network
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NRZ	No-return-to-zero line code
OBIS	Object Identification System
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OMS	Open Metering System
OTP	One-time Pad
P	Preventive Control
PDU	Protocol Data Unit
PHPDU	Physical Layer PDU
PLC	Power Line Carrier
PQ	Power Quality
prEN	European Draft Standard
PV	Photo Voltaic
RES	Renewable Energy Resources
RFC	Request for Comments
RNG	Random Number Generator
ROM	Read-only Memory
RTP	Real-time Pricing
RTT	Round Trip Time
RxD	Received Data
SCADA	Supervisory Control And Data Acquisition
SDL	Security Development Life cycle
SFR	Security Functional Requirement
SMCG	CEN/CENELEC/ETSI Smart Meter Co-ordination Group
SRD	Short Range Devices
TOE	Target of Evaluation
TMTO	Time-Memory Trade-Off
TSO	Transmission System Operator
US	United States of America
UML	Unified Modelling Language
VLAN	Virtual Local Area Network
WAN	Wide Area Network
Wh	Watt hour

1 Introduction

Government requirements on energy efficiency [1], [2], higher demands on energy availability and reliability as well as consumer demands and behavioural changes [3], [4] drive energy market players to improve the overall management of energy infrastructure. For that purpose, a large range of new technologies such as networks and sensors are being introduced. These, for example, allow for detailed energy consumption measurement at the consumer home or allow for management of peripheral energy generation. Thus, the technology allows for Smart Energy.

While the energy infrastructure is steadily maintained and improved, some significant changes have been introduced to the power grids of late. Actually, the progress of these improvement projects heavily relies on regional politics and economics. To keep up with the requirements [7], major utilities already have started to introduce a new field device technology - smart meters [5]. As the name implies, smart meters do support much more use cases than any old conventional electromechanical electricity meter did previously. The new generation of meters not only supports fine granular remote data reading but also enables for remote load control or remote software updates. Hence, to build a secure advanced metering infrastructure (AMI), communication protocols must support bi-directional data transmission and protect meter data and control commands in transit. The need for exceptional reliability of the grid has therefore already lead to numerous publications in the fields of threat analysis [8], [9], [10] and analysis frameworks [11], [12] for AMI and the grid.

In order to justify the scope of this study, chapter 2 provides a brief introduction into smart metering. For a general introduction into the electrical grid and smart grids consult the Compass Security blog at http://blog.csnc.ch. Chapter 2 will very briefly discuss the approaches for metering and explain some basic terminology by means of architecture blue prints. It further introduces common threats towards industrial control systems (ICS) and specifically for the smart grid and points out issues for the AMI and smart meters. That part of the document is based on literature research.

Chapter 3 aims to identify relevant security controls for the smart metering communication. It does so by applying part of the OCTAVE Allegro risk assessment method [6] to the smart meter environment. In the course of the chapter, critical information assets, its security requirements and related threats will be identified. Finally, mitigating controls will be selected in order counter the identified risks. The mitigating controls could be used to analyse the metering communication in a structured way.

The document shall provide general controls for smart meter communication and will not conclude anything but will rather serve as a reference metering communication security benchmarking.

2 Metering Infrastructure

This chapter will focus on the advanced metering infrastructure - its benefits and issues. A short introduction into use cases and approaches will be provided. Further, terms will be introduced and the necessary components and its capabilities will be discussed in more detail. Some relevant standards and specifications will be outlined and referenced.

2.1 Purpose of Smart Meters

A smart meter has several advantages over a traditional mechanical meter. A smart meter does lots more [13], [14] than just providing detailed power consumption data to the operator. Primarily, a smart meter can significantly support the DSO to balance the network load and improve reliability.

A smart meter does not only lower manual reading cost but also enables to more efficiently estimate the load on the generators. It helps to more efficiently integrate DERs and helps to monitor the distribution network in order to identify PQ issues, misrouted energy flows or fire alerts in case a consumer outage is being detected. Beyond that, a meter could be used to push real-time pricing information to the consumer in order to allow appliances in the local network to optimise their power consumption according to the current rates. During an emergency, a meter could allow to disconnect consumers from the power grid. A meter could limit the consumption to a specified amount or could enforce pre-payment for defaulting customers.

Yet, at time of writing, the effective use cases implemented heavily differ from operator to operator. Whereby all of them support at least remote meter reading. However, a security analysis should take all potential use cases into consideration since it is likely that firmware and hardware is being enhanced to support additional use cases in the near future.

2.2 Approaches to Metering

2.2.1 Meter Reading vs. Metering Infrastructure

Typically, literature differs between advanced meter reading (AMR) and the advanced metering infrastructure (AMI) whereby AMR is to be seen as a subset of AMI [15].

AMR provides the metering company with usage data only. AMR does not allow for remote controlled action or advanced collection of power information. Thus, one-way communication from meter to the metering company is sufficient for that approach.

AMI will allow for remote initiated actions and therefore requires a two-way communication protocol. Though the border between the two approaches fades since remote initiated reading will also require for a two-way channel in AMR setups.

The remainder of the paper will focus to the AMI approach.

2.2.2 North American vs. European Implementations

The US as well as European countries have developed absolutely independent implementations of the AMI. Nevertheless, the key drivers and business needs are exactly the same. Comparing the two, the preferred communication protocols on either continent are not compatible with each other.

The National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA) respectively the European Committee for Standardization, the European Committee for Electrotechnical Standardization and the European Telecommunications Standards Institute (CEN/CENELEC/ETSI) mandated by the European Commission drive very similar projects to provide security guidance [16], [17] for smart grid and metering implementations. However, the guidance neither specifically requests for nor does it recommend the use of specific protocols.

If not otherwise stated the remainder of the paper refers to European implementations.

2.3 Architecture and Components

The AMI is typically structured into a bunch of networks and composed of a few major components. Figure 1 provides an overview of all components and most networks. It is made up of the Meter, the Collector and of the server systems at the DSO or metering company side.

The following sections will briefly introduce the major components and related networks of the AMI.

2.3.1 Head-end System

The head-end system (HES), also known as meter control system, is located within a metering company network. In most cases the metering company is the responsible DSO. The HES is directly communicating with the meters. Therefore, the HES is located in some demilitarised zone (DMZ) since services and functionality will be provided to the outside.

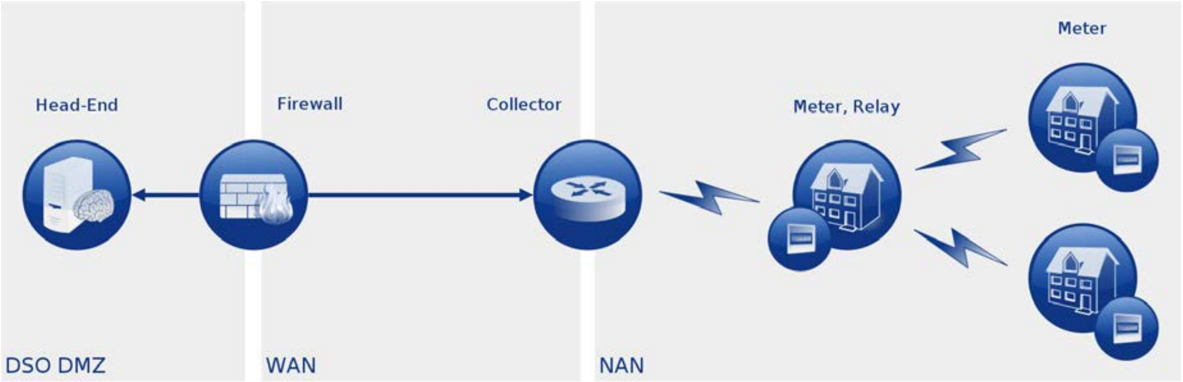


Figure 1: Advanced Metering Infrastructure Networks and Components

There is much more infrastructure at the DSO or metering company side. The collected data will be managed within a metering data management system (MDM) which also maps data to the relevant consumer. Depending on the automation level, the metering data will have influence on the DSO actions in order to balance the grid.

Exposing the HES to consumers enables some significant threats to the DSO. For example, an adversary getting hold of the HES could read all consumer data. Moreover, one could control meters or could manipulate usage data or generate alerts in order to disturb the DSO operations or at least trigger the computer incident response team (CIRT) and maybe force the DSO to backup to some business continuity plan (BCP) while analysing and recovering the HES.

2.3.2 Collector

The collector, also known as concentrator or gateway, serves as communication node for the HES. Depending on the infrastructure the collector could be a meter itself. Its primary function is to interface between the HES and the meters and/or other collectors within its neighbourhood – the neighbourhood area network (NAN).

Not only the head-end but also the collector exposes threats. The collector is physically exposed to adversaries, has a trust binding to the HES and the NAN side and is thus privileged to communicate with either end. Adversaries might exploit the fact in order to attack the HES. Additionally, on the NAN side, adversaries might impersonate the collector to setup a man-in-the-middle scenario or to invoke arbitrary commands at the meters.

2.3.3 Meter

The meter is installed at consumer premises. When integrated with a collector, it directly communicates to the HES. As a meter it either communicates with the collector or may serve as a relay in order to route packets between nearby meters and the collector. Some meters provide an interface for appliances. With retail consumer that network is known as the home area network (HAN). Meters do also provide local diagnostic ports for manual readout, installation and maintenance tasks as shown in figure 2.

From an adversaries perspective the meter is the entry point to building automation, DER and usage data. But the meter is also a relevant part of the smart grid and under no circumstances should its manipulation allow critical influence or affect the availability of the grid or parts of it.

2.4 Communication

The infrastructure consist of several networks of which all could rely on absolutely different media and a multitude of protocols. In total, three networks are commonly described when referring to the AMI. The WAN, NAN and HAN.

2.4.1 Wide Area Network

The WAN connects a meter or collector to the HES. The WAN is sometimes also referred to as the backhaul network. Communication on the WAN link is mostly Internet protocol (IP) based and commonly relies on standard information technology (IT) media and technology stacks such as fibre optic cables (FOC), digital subscriber line (DSL), general packet radio service (GPRS), multi-protocol label switching (MPLS), PLC or some sort of private network. A brief overview on PLC for WAN side communication is provided in [18]

2.4.2 Neighbourhood Area Network

The NAN connects meters and collectors. Typical NAN devices are electricity, gas, water or heat meters. Organisations sometimes refer to the NAN as local metrological network (LMS) [19], field area network (FAN) [14] or the metering LAN [20].

Although standards such as the IEEE 802.15.4 [21], [22] based ZigBee profiles are gaining momentum, the industry and regulators seam to struggle on a common standard. Utilities among the European Union (EU) nations seem to prefer the meter bus standard for NAN communication [19] although the ENISA does not list [14] the meter bus as a NAN protocol.

2.4.3 Home Area Network

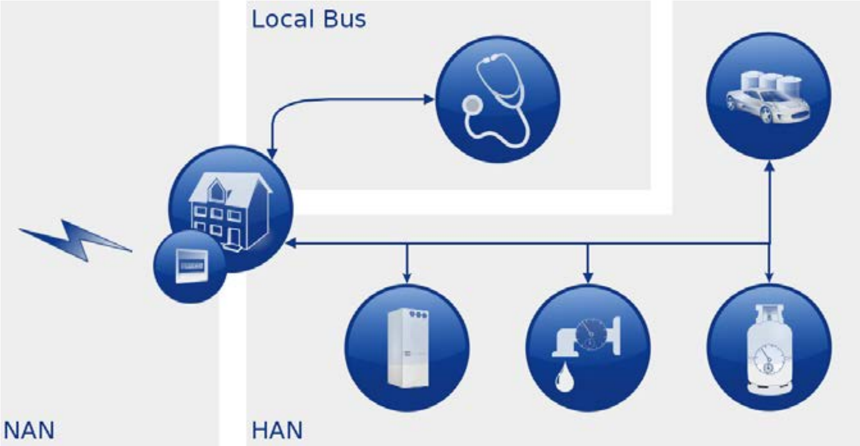


Figure 2: Home Area Network and Local Bus Blueprint

Depending on the consumer type the HAN could also be named as building area network (BAN) or industrial area network (IAN). Whatever its name is, the purpose of the HAN is to integrate additional gas, water or heat meters. The HAN allows for intelligent building automation and also allows the integration of DERs with the smart grid. To optimise consumption during peak hours a utility might for example decide not to entirely turn off but to throttle large heating, ventilation, and air conditioning (HVAC) appliances to balance the grid. For that purpose, consumers will be required to grant utilities or a third-party supplier access to their appliances. However, intelligent control does not necessarily require the intervention of an external part. Therefore, an intelligent HVAC might decide to throttle automatically based on the real-time pricing information provided by the utility.

Meters in the US largely focus on ZigBee for HAN communication [23]. Profiles for home automation and smart energy are specified in [24], [25]. The open metering system (OMS) group is pushing a specification that relies on M-Bus. In addition, the wireless M-Bus stack has been chosen as a foundation for WiMBex [26] and the KNX [27] wireless version. KNX is very popular in home automation among Europe. Unfortunately, KNX does not provide any security measures. Though there are studies which propose security enhancements to KNX [28].

2.4.4 Local Bus

Common interfaces for diagnostic purposes are provided as two or three-wire serial lines, current loop or as an optical interface [29], [30].

2.4.5 Network Protocols

Good overviews on common protocols for WAN, NAN, HAN and the Local Bus are provided in [31], [32].

3 Smart Meter Threats and Controls

3.1 Overview

The goal of this chapter is it to capture controls. It will identify smart meter assets, requirements, threats and related security controls. Section 3.1.1 - 3.1.3 will provide an introduction to the chosen approach and justify the scope of the analysis. Section 3.2 will then focus on the smart meter threat analysis and section 3.3 covers the selection of appropriate controls.

3.1.1 Business Rationale

The European commission has mandated [33], [34] CEN/CENELECT/ETSI to provide an overview on current standards for smart grids and smart meters. The first release of these reports [35], [36] identify objectives for all domains of the grid and specifically for smart meters. Some of these distribution (WAN) and consumer side (NAN, HAN) objectives serve as reference to model requirements and identify assets and threats. The objectives out of [35], [36] which matter for this work can be summarised as follows:

1. Remain flexible for new business cases
2. Ensure system control
3. Ensure and monitor quality of service
4. Support demand side management and distributed energy resources
5. Ensure high accuracy of individual data
6. Provide interfaces for consumer energy management systems
7. Provide real time information to consumers

Smart meters are regarded as crucial key components in order to achieve the listed smart grid objectives. Thus, it is evident that smart meter implementations and specifications follow the core principles of information security, referred to as the extended CIA triad, to face current and future cyber security threats. ISO 27000 [37], a well established information security standard, defines the core principle of information security as listed:

"Confidentiality: *Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.*
Integrity: *Property of protecting the accuracy and completeness of assets.*
Availability: *Property of being accessible and usable upon demand by an authorized entity.*
Authenticity: *Property that an entity is what it claims to be.*
Non-repudiation: *Ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event." [37]*

Metering assets are threatened by a multitude of threat actors. The majority of threats need to be realised deliberately and will of course need some badly motivated actor being involved. Moreover, the limited physical protection exposes the devices to environmental threats such as flooding or storms. The threats towards traditional electricity meters were essentially of physical nature [38]. Examples are: various forms of electrical current miss-routing, demolishing the circuitry, influence with electromagnetic fields or to manipulate the real-time clock. Smart meters will of course inherit all physical threats but will additionally be threatened by information security issues due to the various available interfaces and communication links. Besides, smart meters will inherit threats as they may share the communication media with third parties and may rely on telecommunication networks which are not exclusively bound to smart meter communication.

Literature [39] does not only differ between intentionally and accidentally realised threats but also between active and passive threats. Whereby listening to conversations is passive and modifying contents is an active task.

Threats include potential theft, damage and manipulation of smart meter installations. Furthermore, loss of smart meter hardware or disclosure, corruption and modification of data are to be considered. Finally, actions that could cause service interruption will prevent business and therefore pose significant threats as well.

Section 3.3.1 and 3.3.2 will focus on the identification of appropriate controls that support the grid to meet the required business rationale. For that purpose one out of many risk assessment approaches has been selected.

3.1.2 Analysis Approach

The approach and terminology on how to identify controls is in most parts followed the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro [6] methodology. OCTAVE Allegro is an asset centric and lean risk assessment successor of the OCTAVE method. The method was chosen since it supports straight-forward qualitative risk assessment and structured threat analysis. Figure 3 is based on [40] and groups the methodology steps into four major phases.

3.1.2.1 OCTAVE Allegro Phases

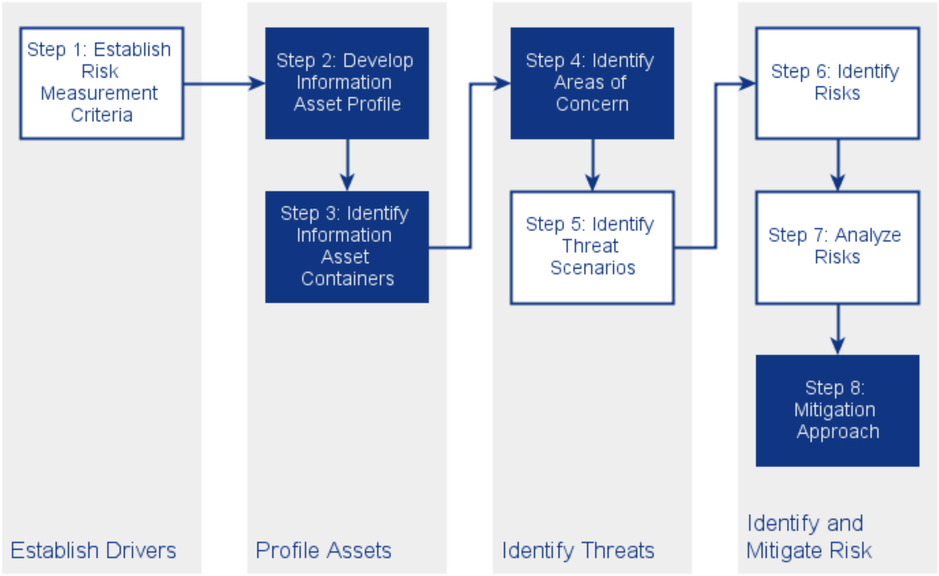

Step 1: Establish Risk Measurement Criteria
Step 2: Develop Information Asset Profile
Step 3: Identify Information Asset Containers
Step 4: Identify Areas of Concern
Step 5: Identify Threat Scenarios
Step 6: Identify Risks
Step 7: Analyze Risks
Step 8: Mitigation Approach
Establish Drivers
Profile Assets
Identify Threats
Identify and Mitigate Risk

Figure 3: OCTAVE Allegro steps and phases

Phase "Establish Drivers" aims to justify and prioritise the measurement criteria for risk for a specific organisation.

Phase "Profile Assets" is designed to identify and document logical, technical, physical and people assets.

Phase "Identify Threats" focuses on the identification of threats against the identified assets.

Phase "Identify and Mitigate Risk" supports the valuation of the risks posed against the critical information assets. Finally, after this step, the mitigation strategy for each of the identified risks is defined.

3.1.2.2 OCTAVE Allegro Steps

This section goes through all of the OCTAVE Allegros steps to provide an introduction into the methodology. Moreover, each step will be accompanied by a fictitious example related to AMI. Additionally, it will be justified why dark coloured steps in figure 3 will be considered for the threat analysis and why light coloured steps are being omitted in order to reach the goals of this study.

Step 1 advises to identify all areas that impact an organisation. The methodology requires for a minimum set of areas which includes safety, health, productivity, reputation, financial and fines. For each of the impact areas, a set of criteria to measure low, medium and high impact must be developed. Table 1 provides an example for loss of revenue in case of data privacy violation. Finally, the major areas will be ranked and assigned values in order to allow for risk scoring. In case five areas have been identified and "legal penalties" is considered the top risk area, then the area would be assigned a five. An example is provided in table 6.

Impact Area	Low	Medium	High
Legal penalty, data privacy violation	Less than 5% cost of typical yearly revenue.	5% to 10% cost of typical yearly revenue.	More than 10% cost of typical yearly revenue.

Table 1: OCTAVE Allegro Step 1: Establish Risk Measurement Criteria. Impact Area Example

Step one of the methodology is being omitted in this study since the project work does not aim to evaluate an organisation's risk.

Step 2 provides guidance in identifying critical information assets for the organisation. The methodology also provides a set of questions and asks for example for the value of assets or the dependency on assets for the day-to-day business of the organisation. Each identified information asset will be attributed additional cornerstone such as the security requirements to make up a whole information asset profile. An example for key material in a smart meter is provided in table 2. Moreover, each profile's most important security requirement is being identified to support the later valuation of the potential impacts. OCTAVE Allegro does not provide much guidance and structure on how to identify security requirements. A way to model such requirements is by means of misuse cases [41]. The approach described lends it from the unified modelling language (UML) such as used in common software engineering processes where success and fail scenarios of interaction with data and processes is being modelled. Some brief thoughts on potential use cases for the metering environment are provided in appendix 6.1. Though, the modelling of misuse cases rather focuses on the abuse of such scenarios by malicious actors (misusers). In this study, step two of the OCTAVE Allegro methodology is entirely being followed.

Information Asset	Rationale for Selection	Description	Owner	Confidentiality	Integrity	Availability
Key material	Leakage will allow access to meter device.	Refers to all secrets stored in the meter device.	Device manufacturer and meter mgmt. personnel	**Key material must be kept secret.**	Only the utility shall be granted to update and revert key material.	Key material must be available for meter mgmt. personnel.

Table 2: OCTAVE Allegro Step 2: Develop Information Asset Profile. Critical Information Asset Example

Step 3 collects information asset containers in the form of an information asset risk environment map. Information asset containers, as the name implies, can hold, process or somehow get in touch with information assets. The methodology classifies containers as technical, physical and people. Table 3 provides examples for each of the types. Correspondingly, containers are being attributed whether they are of type internal which means under control of the organisation or whether the container is external.

Container	Description	Owner	Type	Class
Meter	Holds various assets. E.g. key material	Metering company	Internal	Technical
Monthly paper invoice	Consumption data on monthly invoice	Utility, Consumer	External	Physical
Service technician	Knows the initial secret of meters	Service company	External	People

Table 3: OCTAVE Allegro Step 3: Identify Information Asset Containers. Container Examples

For the analysis of an organisation the type column can be attributed with minimal effort. However, for an abstract analysis such as of the wireless metering protocol or of a component such as the smart meter, some assumptions must be made. For the later application of step three, it is assumed that the organisation is the metering company.

Area of Concern	Actor	Means	Motive	Outcome
Inadequate link encryption could allow to access metering values.	Investigative Journalists	Put a tap on the link	gain information on energy use monitor consumption behaviour	Disclosure

Table 4: OCTAVE Allegro Step 4: Identify Areas of Concern. Area of Concern Example

Step 4's goal is to identify major areas of concern. Thereby the method foresees to consider all containers and to identify issues that could affect assets within the container. The compiled list of "areas of concern" is then expanded with the according actor, the means to realise the threat, the motive of the actor and the potential outcome. Whereby an outcome is always one out of disclosure, modification, interruption or destruction. The method documentation further lists loss next to destruction. An example, implicitly referencing the affected information asset, is provided in table 4. This step does not aim to identify a complete list of threats but helps to capture the major concerns in short time. The study will make use of this step to capture area of concerns for the smart meter and wireless metering analysis.

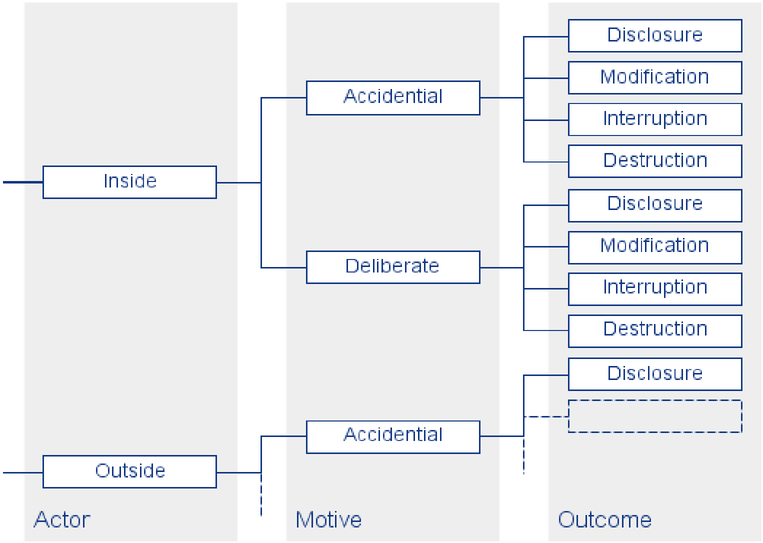


Figure 4: OCTAVE Allegro "Human Actors Using Technical Means" Tree

Step 5: ensures structured identification of all potential threats. Threat trees ensure robust consideration of threats. The step relies on four trees in total. Two considering human actors with either technical or physical means and two considering technical and other problems. Part of the *"Human Actors Using Technical Means"* tree originating of the methodology documentation [6] is shown in figure 4. With each information asset, each branch of the four trees will be traversed to ensure thorough coverage and identification of threats. The guidance provides worksheets and questionnaires to simplify the activity. The result of the walk through will be a comprehensive list of threat entries as shown in table 4. Optionally, each resulting list entry can be assigned the probability of the realisation of the concerned threat scenarios with either low, medium or high likelihood.

This study does not need thorough coverage of threat scenarios to answer major security questions regarding most wireless metering protocols. On that account, step five will not be considered unless the previous step "Identify Areas of Concern" does not provide sufficient material or the analysis significantly lacks coverage.

Step 6: consists of a single activity and aims to identify the impact if a certain threat scenario becoming realised. Following that, each threat scenario will be attributed a consequence. Thus, table 4 has been expanded with an additional column to describe the consequence for the scenario. Part of table 4 and the newly added column is shown in table 5.

Area of Concern	Actor	)ut- ome	Consequence
Inadequate link encryption could allow to access metering values.	Investigative Journalists	)isclo- ure	Disclosure of private information leads to legal penalty. The legal department estimates the total case at £ 500'000.

Table 5: OCTAVE Allegro Step 6: Identify Risks. Risk Example

This step is not considered in the remainder of the project since the OCTAVE Allegro approach has been chosen to identify the major threats and appropriate mitigating controls rather than evaluating an organisational risk.

Step 7: focuses on creation of a relative risk scores for each identified threat scenario. The impact on each impact area as well as the impact area importance will be reflected in the total risk score. The score should help to decide on what mitigation approach to choose in the ultimate step of the methodology. Assumed the impact area ranking in table 6 and threat scenario listed in table 5 the risk score for that specific scenario calculates as shown in table 6. Basically, for each impact area the impact will be measured according to the criteria defined in step 1. An example of such criteria is provided in table 1. High impact will be assigned a value of three and low impact accordingly a value of one. The impact area ranking is then multiplied with the threat scenario impact value whereby the results of that calculation contributes to the total risk score.

Impact Area	Rank	Impact	Value	Score
Fines/Legal Penalties	5	High	3	15
Reputation	4	High	3	12
Safety and Health	3	Low	2	6
Productivity	2	Low	2	4
Financial	1	Medium	1	1
Total Risk Score				**38**

Table 6: OCTAVE Allegro Step 7: Analyse Risk. Example Risk Score Calculation

Step 8: the ultimate step in the OCTAVE Allegro qualitative risk assessment method deals with the mitigation approach of identified risks. In general risks can be accepted, mitigated, transferred, avoided or being further monitored (deferred) whereas mitigation aims to avoid or limit the risk. However, the efforts for avoidance and limitation should never outweigh a potential impact.

Though numbers have been assigned as risk scores, their specific value only provides indication to whether a risk should to be mitigated or not. One might also take the likelihood of occurrence and some organisation specifics into account. It is suggested to divide the risks into four pools, pool one to pool four, whereby each pool groups threats for a range of the total risk score. The four pools are then approached as follows:

Pool 1: Mitigate
Pool 2: Mitigate or Defer
Pool 3: Defer or Accept
Pool 4: Accept

Depending on whether probabilities have been assigned in step 5 of the methodology it is suggested to either form a list of all risks and then split it into four pools or create a matrix which reflects the four pools and takes the probability into account. Finally, a mitigation strategy should be formulated for all risks that need to be mitigated. The mitigation strategy should list the information asset container to which the controls will be applied. Plus, the chosen strategy should consider and outline potential residual risks. An example of such a mitigation strategy is provided in table 7.

Container	Control	Residual Risk
WAN link	Implement encryption to avoid disclosure of metering values	Weak encryption, issues with the key schedule or derivation or wrong implementation could lead to disclosure

Table 7: OCTAVE Allegro Step 8: Select Mitigation Approach. Mitigation Strategy Example

OCTAVE Allegro is a lean risk assessment method and does not provide guidance in selecting security controls as with extensive information security management standards such as ISO 27000 [37]. However, ISO 27002 [42] and NIST SP 800-53 [43] provide a comprehensive list of controls to choose from, if needed.

Since the analysis does not pose a full organisational risk assessment, the steps involving measurement definition, identification and mitigation approach selection have not been completed.

Specifically, the OCTAVE Allegro methodology is being followed for:

Step 2: Develop Information Asset Profile
Step 3: Identify Information Asset Containers
Step 4: Identify Areas of Concern

Mitigating controls will be proposed for all of the identified and relevant areas of concern (step 4). The selection of the controls will be completed under aid of the common criteria standards [44] to ensure adequate coverage. The next section commences with a definition of the scope that will be of relevance for the remainder of the document and during completion of the threat analysis and selection of mitigating controls in section 3.3.

3.1.3 Relevant Scope

Since this is a conceptual analysis and not an analysis of an organisation some of the attributes do not fit. Following that, the section aims to clarify the scope of the threat analysis. It is assumed that all analysis is being conducted as if it were done for a metering company that runs the entire AMI. However, a full AMI analysis would for example need to consider the flow of billing relevant information from the smart meter over collectors and the head-end system to the utilities billing system and by post back to the consumer. It would also require to take all facilities and networks being crossed into account. Additionally, people on site and remote workers that manage IT system would need to be modelled also.

Since this chapter shall support the identification of security controls for the metering protocol standards analysis, the scope is being restricted to the directly related information asset containers. Thus, or the remainder of the threat analysis section it shall be considered at maximum the information asset containers shown in figure 5. A list of relevant information asset containers is provided in table 11.

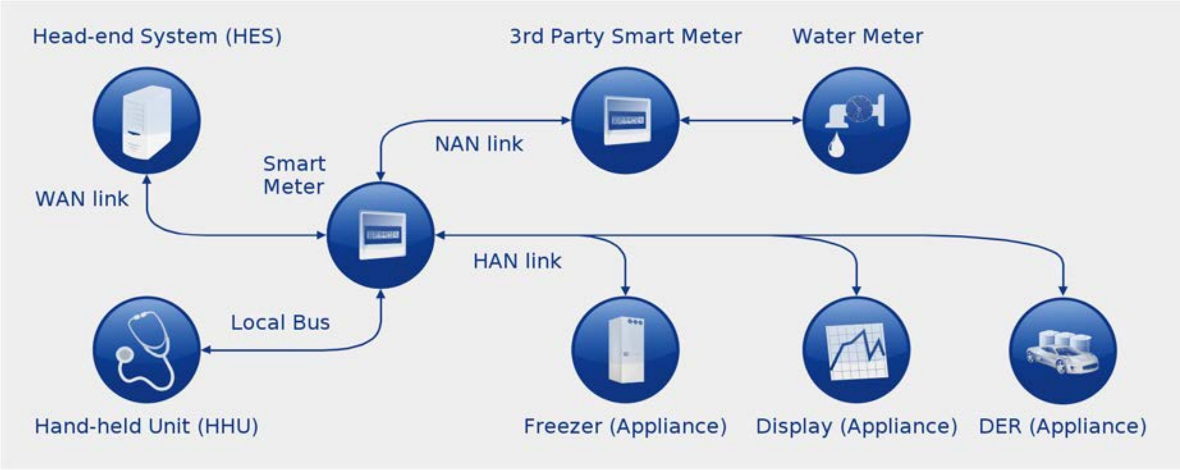


Figure 5: Information Asset Containers Scope Definition

The assumed metering company runs components such as the HES, concentrators and smart meters whereas the metering company must not necessarily be the DSO or utility, although this is often the case. The metering company also integrates with 3rd party meters and the DSO or utility can access the smart meters features such as load limiting and remote disconnect on behalf of the metering company. For the WAN side, the identification of containers will stop at the HES.

The NAN side analysis will not go any further than to the third-party meter which is run by an independent company. For the HAN side, arbitrary appliances will be considered. These are assumed to support display of pricing information, allow for load control or pose some form of DER. The appliances may additionally connect to an external service provider portal. However, the analysis will be limited to the appliances.

3.2 Threat Analysis

3.2.1 Develop information asset profile

A meter must support different use cases to meet the business needs. However, the supported use cases mainly depend on the "smartness" of a meter. For example, a simple gas meter without remote controlled valve will maybe just need to send metrological values. The majority of these devices need local bus connectivity to be provisioned and will send bursts of meter information on pre-configured intervals. Consequently, there is no need to evaluate complex threat scenarios for such devices.

The subsequent sections will identify assets that should be considered in order to answer the questioning whether a wireless metering standard would provide adequate security to rely on for an AMI.

3.2.1.1 Collection of Information Assets

Assets do pose some form of value to its owners. An asset may be a certain piece of information or a physical element. The chosen method [6] distinguishes between information assets and technical assets. The collection of information assets listed in table 8 have been identified from common smart grid use cases and the summarised business objectives in section 3.1.1. Information assets referenced in table 8 which do pose huge value or which will be required to run essential business processes are considered critical and have been marked accordingly.

Note, the majority of the identified assets refer to electricity metering. However, some of the assets do also apply to heat, gas and water meters.

ID	Asset Name	Critical	Asset Type
A01	WAN	yes	Technology
A02	NAN	yes	Technology
A03	HAN	yes	Technology
A04	Local Bus	yes	Technology
A05	Hardware (controller, networking, enclosure)	yes	Technology
A06	Firmware and Software	yes	Technology
A07	Calibration data	yes	Information
A08	Identification	yes	Information
A09	Key material	yes	Information
A10	Meter values (consumption, monitoring, profiles, timing information)	yes	Information
A11	Alerts	yes	Information
A12	Audit records	yes	Information
A13	PQ measurements	yes	Information
A14	Application logs	no	Information
A15	Error logs	no	Information
A16	Pricing Information	yes	Information
A17	Prepayment Information	yes	Information
A18	Load limit configuration	yes	Information
A19	Remote disconnect configuration	yes	Information

A20	Information on DER status and availability	yes	Information
A21	Firmware	yes	Information

Table 8: Collection of Information Assets

The collection of information assets is not to be considered as an exhaustive list. A thorough analysis of a complete AMI would for sure result in a much longer list. However, the list reflects relevant assets which need to be handled by one or the other meter implementation. If not in current installations then probably in the near future. Whatsoever, the approximately twenty assets are considered sufficient in order to identify the major controls for smart meters.

3.2.1.2 Description and Assignment of Owners

In the course of the analysis, critical information assets are being carried on and will be attributed additional detail. Therefore, table 9 has been limited to the "critical" marked information assets and has been expanded with a short description of each asset, a reasoning why the asset was selected and with information to the relevant asset owners. Note, the ownership of some assets might not entirely apply to a specific real-world case since it heavily depends on contracts between parties and predominant local law.

Ref.	Rationale for Selection	Description	Owner
A07	Manipulation of the calibration data would result in intolerable measurement errors. Besides, the measurement precision is subject to regulatory requirements. Wrong calibration will result in wrong billing.	This information asset contains information that help to adjust the accuracy of the metering module and is stored in the meter.	Meter calibration personnel at an approved calibration facility
A08	Manipulation of the identification leads to inconsistent mapping in the meter mgmt. or billing system. The identification is considered personal data as this identification can be mapped to a specific consumer.	This information asset contains the unique identification information of a meter. This could be a serial number or device address	a) Device manufacturer b) Meter mgmt. personnel at the MDM site c) Utility accounts receivable department
A09	Leakage of key material could allow access to smart meters or could allow to forge signatures.	This information asset refers to all secrets, public key pairs or certificates stored in the meter	a) Device manufacturer b) Meter mgmt. personnel at the MDM site c) Meter service personnel
A10	Leakage and manipulation of meter values would raise privacy issues, wrong assumptions for load profiling and financial loss to consumer or utility due to wrong bills.	This information asset stores various consumption information	a) Meter mgmt. personnel at the MDM site b) Utility accounts receivable department
A11	Alerts would indicate issues with a meter or grid segment. Tampering with alerts would lead to wrong assumption for incident response. Unfortunately, incidents cannot be detected if alerts cannot be received.	Alerts indicate critical events such as power drops, sabotage or hardware issues.	a) Meter mgmt. personnel at the MDM site b) Meter service personnel

A12	Tampering with audit records would significantly complicate the analysis and reconstruction of incidents and most likely violate compliance requirements.	Audit records contain information which need to serve as chain of custody for critical operations and should support to answer the five Ws questions	Meter mgmt. personnel at the MDM site
A13	Manipulation of PQ measurements might lead to wrong control activity at the DSO side	PQ measurements contain detailed information that help to assure supply quality	a) Meter mgmt. personnel at the MDM site b) DSO processes information to ensure power quality"
A16	Manipulation of the pricing information would cause the consumer to base its consumption behaviour on wrong data. Leakage of the pricing information would reveal custom pricing plans.	Pricing information does hold information that supports the consumer or intelligent HAN devices to evaluate the correct consumption strategy.	a) Utility sales department
A17	Manipulation of prepayment information could allow defaulting consumer to obtain free energy.	Prepayment information is composed of all values needed to ensure energy is paid before delivered an the correct amount is being served.	a) Utility accounts receivable department b) Meter service personnel
A18	Malfunction of the load limiter based on configuration errors could lead to service disruption at the consumer side.	Load limiting configuration does for example include the value of the actual load limit.	a) Meter mgmt. personnel b) Meter service personnel c) Utility accounts receivable department
A19	Malfunction of remote disconnect functionality based on wrong configuration parameters may cause serious damage or loss at the consumer side or with utility service personnel.	Remote disconnect configuration includes all register to switch power supply.	a) Meter mgmt. personnel b) Meter service personnel c) DSO load management department d) Utility accounts receivable department
A20	Inadequate information prevents the integration of DER into the grid or could result in wrong estimates on storage and generation and cause instabilities.	DER information includes the capacity and capabilities in terms of storage and generation of a DER connected to a meter.	DSO load management department
A21	Manipulation of firmware would lead to control over the meter and over meter data. Loss of firmware would lead to disclosure of intellectual property.	The firmware contains the logic on how to store, manage, process and transmit with surrounding devices, tailored to the metering company needs.	Device manufacturer

Table 9: Critical Information Asset Profiles (Rationale, Description, Owners)

By now, the list of critical information assets contains a reasoning and description for each asset as well as the associated owner for each of the assets.

3.2.1.3 Identification of Security Requirements

Activities seven and eight in OCTAVE Allegro's identification of the critical information assets, advises to record the security requirements for each of the assets. Table 10 lists the security requirements for core information security principles such as confidentiality, integrity and availability for each asset. Security requirements that do not fall in either of the three categories are listed in column "Other". The most important requirement of each asset is printed in bold letters.

Ref.	Confidentiality	Integrity	Availability	Other
A07	Certified calibration personnel shall have access to the calibration data.	**Certified calibration personnel shall have permission to alter the value**	Calibration data must be available for calibration personnel only.	
A08	**Device manufacturer will need read access to the ID until the device is shipped.** **MDM personnel and accounts receivable will need access to the ID to map the device geographically and to map it to the consumer**	Manufacturer will need to write the ID on manufacturing. Later on, the ID does not need to be changed again.	ID must be available permanently for MDM personnel. For the utility accounts receivable department the ID must be available on regular billing schedules.	The ID allows a mapping to the consumer and is therefore considered personal data and must comply with according regulations.
A09	**Manufacturer will need to generate and maybe ship the initial key material with the device. Nobody, except the meter shall be granted access to key material**	a) Manufacturer sets initial keys and secrets b) Utility shall be granted to update keys and secrets c) Utility shall be granted to revert to initial key material	Key material must be available for MDM personnel and service technicians.	
A10	Only authorised parties are granted access to to metering values	**Meter values shall be protected of unauthorised manipulation**	Meter values might remain unavailable for remote reading for longer time in case the meter keeps a history	Consumer should not be able to deny having sent (non-repudiation of origin) a certain meter value.
A11	MDM personnel and service personnel will need to receive alerts to maintain the meter integrity and the grid stability.	Everyone is denied modification of alerts.	**Alerts need to be available to MDM and service personnel on presence.**	
A12	Audit records will need to be read by authorised personnel to react on is-	**Everyone is denied modification of audit records. Security functions will**	Audit records shall retain until they have been read	

	sues with power supply or to react on issues with the meter itself.	**need to append audit records to the log.**	and transferred by a authorised party.	
A16	Access to the pricing information shall be restricted to the utility sales department and the consumer.	**Accurate pricing information needs to be pushed to the meter in a way that consumer can rely on the data and react accordingly. Only the sales department shall be granted to write pricing information.**	Pricing information shall be available to the consumer 24h in near real-time. Short outages are tolerable as long as the pricing does not change during that period.	The consumer should not be able to deny having received up-to-date pricing information (non-repudiation of receipt)
A17	Prepayment information shall be restricted to the accounts receivable department and the consumer.	**Prepayment information can be modified by the accounts receivable department only.**	Prepayment information shall be available to the consumer around the clock.	
A18	Reading of the load limit configuration shall be restricted to the accounts receivable department.	**Load limit configuration changes can be done by the accounts receivable department only.**	The current configuration must be available to the accounts receivable department only.	
A19	Reading of the disconnect and load control configuration should be limited to the asset owners.	**Assumed the consumer has agreed on load control the changes to the configuration shall be restricted to the asset owners.**	The configuration shall be permanently available to all owners.	
A20	Reading status and capabilities of DER should be restricted to the consumer and the DSO.	**Neither the DSO nor the consumer shall be allowed to change that information.**	The asset must be permanently available to the DSO. There is no significant impact if the information is not permanently available to consumers.	
A21	There is no need to read the firmware itself.	**Manufacturers, meter management personnel and meter service personnel will need to flash integrity protected firmware.**	Firmware should be available during maintenance task.	

Table 10: Critical Information Asset Profiles (Security Requirements)

Finally, all critical information assets are identified, outlined and assigned the relevant security requirements. The next step in the process [6] will work towards the identification of areas of asset existence, such as storage, networks, processes or people (human interaction).

3.2.2 Identify information asset containers

This section aims to identify all information asset containers. The chosen process considers any physical media, logical process or biomass that can hold the information as a container. Basically, anything that gets in touch with the information asset needs to be examined. Information asset containers are being categorised in either technical, physical or people. Each information asset container is marked as internal or external container whereby internal is to be understood as under control of the metering company for which the threat analysis is being conducted for. Again, as with critical information assets, the ownership of the information asset containers heavily depends on local law and culture. As a result, the identified owners must not necessarily fit a specific environment.

3.2.2.1 Enumeration of technical containers

In machine to machine (M2M) networks the identification of technical containers is in most cases straight forward as peer systems and the network to the systems, both are considered containers. In a metering infrastructure exist the following peers:

- The peer of a meter within the WAN is one or multiple head-end systems (HES)
- The peer of a meter within the NAN is a single collector respectively gateway or a mobile receiver. If the meter serves as a collector or relay then the peers are multiple meters or collectors and relays.
- The peer of a meter within the HAN is a consumer device. This could be a panel to display current consumption, pricing and grid status or it could be a PV system, an EV or HVAC.
- The peer of a meter at the local bus is a hand-held diagnostic, monitoring or installation device (HHU).

Figure 5 shows most of the mentioned technical information asset containers. While this is a very generic view on the meter and its surroundings, the analysis of wireless metering protocols will mainly focus on WAN, NAN and HAN communication.

The analysis of the flow and presence of all critical information assets leads to table 11 which lists all identified technical information asset containers. The fields type and scope indicate whether the identified container is under direct control of the metering company and if it fits the scope for the analysis in chapter 0. A detailed mapping of all containers and information assets is documented in appendix 0.

ID	Container	Owner	Control	Scope
C01	Meter	Metering company	Internal	yes
C02	Metering module	Metering company	Internal	yes
C03	Head-end system	Metering company	Internal	yes
C04	WAN link	Public	External	yes
C05	NAN link	Public	External	yes
C06	HAN link	Public	External	yes
C07	Local bus	Public	External	yes
C08	Third-party meter	Third-party meter service company	External	yes

C09	Appliance	Consumer or 3rd party	External	yes
C10	Hand-held unit	Meter service company	External	yes
C11	Calibration data servers	Calibration company	External	no
C12	Meter manufacturer servers and networks	Device manufacturer	External	no
C13	Meter service company servers and networks	Meter service company	External	no
C14	Metering company DMZ	Metering company	Internal	no
C15	MDM system	Metering company	Internal	no
C16	Load control systems	Utility	External	no
C17	Billing system	Utility	External	no
C18	Utility networks	Utility	External	no
C19	Appliance information portal	Appliance service provider	External	no

Table 11: Technical Information Asset Containers

Apart from the technical containers, the physical location of assets and people that have access to assets needs to be modelled also. As the physical and people containers do not directly fit into the protocol analysis scope, the details have been moved to appendix 6.2.1 and appendix 6.2.2 for reference. Sections 3.2.3 will now focus on the identification of potential areas of concern and section 3.3 will then consider appropriate mitigating controls.

3.2.3 Identify areas of concern

This section aims to identify area of concerns for the scope defined in section 3.1.3 based on the identified critical information assets and the relevant information asset containers. The section basically covers step four of the chosen approach. See figure 3 for reference. It focuses on raising major concerns. The major actors and area of concerns are being examined in sections 3.2.3.1 and 3.2.3.2.

3.2.3.1 Actors

Threat agents have various interests and different capabilities in terms of funding and man power. Table 12 provides an overview of the threat agent groups considered in the identification of areas of concern in section 3.2.

Group	Types	Description
Insiders	Employees, Contractors, Service Providers	That group is made up of threat agents that have specialist know-how and complete design parts of meters or may have access to detailed specifications. The group applies to individuals or corporates that have access to hardware parts either before or after a smart meter finally gets assembled. The insider group furthermore includes people at affiliated partners such as the external IT support and service personnel. Typically, these have special privileges or in-depth expertise.

Frustrates	Individuals, Activists	The group of frustrates is composed of those individuals that have any ethical, personal, moral or political motivation to pose threat to the smart metering infrastructure, its data, a utility or an individual consumer. Typically, frustrates have low funding and mainly focus on causing damage.
Fraudsters	Small-time criminals, Individuals	The major interest of this group is not to pay for the amount of energy consumed. Their know-how and funding is limited but by the time simple and cheap equipment becomes available they might take the chance and realise a threat. Members of this group pose threats to integrity and accountability of the assets.
Surveillants	Burglars, Stalkers, Paparazzi	Surveillants do have limited funds as well. Their major interest is not to attack the smart energy environment but to use the infrastructure to gain knowledge on their victims presence or behaviour. Surveillants are mainly interested in privacy related threats.
Cybercrime	Corporates, Organised crime, Terrorism	The cybercrime group is made up of well organised and well funded types of adversaries. Their interest ranges from defamation of other market players over competitive edge to elimination of rivals. The group may also have interest in manipulation, control and deliberate damage of the infrastructure in order to hide or support other criminal actions or to extort certain demands. Most likely, this group will hire Insiders in order to get hands on details and to effectively support their criminal operations.
Disasters	Natural, Man-made	Disasters target the availability of equipment and services. These mostly hit by accident and cause significant change to the environment.

Table 12: Threat Agents in the Smart Meter Environment

The groups defined in table 12 will serve as threat agents for the descriptions of the threats. The groups interests have been described to fit into the analysis scope. Most of the identified actors pose external threat to the information assets. Alternative standards [45] for risk assessment do provide detailed description of threat actors and do additionally distinguish between threat sources and threat actors. However, the approach chosen here is not bound to such detail. Actually, another publication focusing on energy theft [46] in the AMI has less granular description of threat actors.

3.2.3.2 Area of Concerns

With focus on wireless communication the concerns listed in table 13 have been raised. Each area of concern is attributed an actor, the means necessary to realise a threat, the motive and potential outcomes. Entries are being referred to as ARxx since all area of concerns are being listed in the information asset risk worksheet.

ID	Actor	Area of Concern	Means	Motive	Outcome
AR01	Surveillants	Inadequate link encryption could allow to access data	Put a tap on the link	a) gain information on energy use b) monitor consumption behaviour	Disclosure

AR02	Frustrates, Surveillants, Cybercrime	Inadequate traffic control could raise issues when being able to determine consumption behaviour and amount from packet size and frequency	Put a tap on the link and identify frequency and size of meter values sent	a) derive energy use from meter values send frequency b) detect presence of property owner c) derive company turn-over from energy use	Disclosure
AR03	Frustrates, Fraudsters, Cybercrime	Inadequate integrity protection of links allows to tamper with meter values	Alter meter values in transit or send arbitrary meter values to HES. Most likely, this requires the actor to setup a man-in-the-middle scenario.	a) Confuse billing system b) Cause inaccurate bill c) Cause inaccurate load profiling	Modification
AR04	Frustrates	Drop, delay or render values useless.	Cut wires or use radio jammer in order to render the link useless.	a) Avoid use of meter values for load profiling b) Avoid use of meter values for DR	Interruption
AR05	Frustrates, Cybercrime	Pretend to send someone else's billing information to	Pretend to send someone else's meter values.	a) Confuse billing and load profiling system b) Falsify bills	Modification
AR06	Frustrates, Fraudsters, Cybercrime	Resend old meter values	Connect to the link and resend old meter values.	a) Confuse billing system b) Revert to old billing value	Modification
AR07	Fraudsters	Claim not to have sent certain meter values	Hand in a claim.	a) Dispute resolution or a forensic investigation b) Cause charge back	Modification
AR08	Surveillants, Cybercrime	Inadequate encryption might allow to identify and snoop on alerts	Put a tap on the relevant link.	a) recognise issues due to the occurrence of alerts b) Read the exact issues from the alert	Disclosure
AR09	Cybercrime	Alter alerts and audit records in transit	Alter values in transit.	a) Cover attack attempts b) Cause wrong reactions at the	Modification

				DSO side.	
AR10	Frustrates, Cybercrime	Send arbitrary alerts and audit records	Record and send arbitrary meter values using appropriate equipment.	a) Misinterpretation b) Cause truck roll	Modification
AR11	Frustrates, Cybercrime	Pretend to send alerts or audit records for an arbitrary device	Connect to the link and send faked alerts and audit records.	a) cause misinterpretation b) cause a truck roll	Modification
AR12	Fraudsters, Cybercrime	Drop or delay alerts and audit records in transit or render link useless	Cut wires or use radio jammer in order to render the link useless.	Hide attack attempts.	Interruption
AR13	Frustrates, Cybercrime	Resend old alerts or audit records	Connect to the link and send formerly recorded alerts and audit records.	a) Cause misinterpretation b) Cause a truck roll	Modification
AR14	Frustrates, Cybercrime	Alter DER information or send arbitrary DER capabilities	Connect to the link and send arbitrary DER information.	a) DSO could assume wrong capabilities for load management.	Modification
AR15	Frustrates, Cybercrime	Drop or delay DER information or render the link useless	Cut wires or use radio jammer in order to render the link useless.	a) Consumers will not get rewarded b) DSO cannot use DER	Interruption
AR16	Cybercrime	Resend old DER capabilities	Connect to the link and send formerly recorded packets	DSO will assume wrong capabilities for load management.	Modification
AR17	Surveillants, Frustrates	Snoop on pricing information	Put a tap on the link	Get aware of alternative, maybe better pricing	Disclosure
AR18	Frustrates, Cybercrime	Alter pricing information in transit or send arbitrary pricing information	Connect to the link and send formerly recorded or arbitrary pricing information.	Cause loss to consumer due to HAN devices takes wrong decisions based on falsified pricing information	Modification
AR19	Frustrates, Cybercrime	Drop or delay pricing information in transit or render the link useless.	Cut wires or use radio jammer in order to render the link useless.	Prevent consumers to react on increased rates.	Interruption
AR20	Frustrates,	Resend old pricing	Connect to the link and	Cause loss due to	Modification

	Cybercrime	information	send formerly recorded information	HAN devices might take wrong decisions based on falsified pricing information.	
AR21	Frustrates, Fraudsters	Claim not to have received accurate pricing information	Hand in a claim.	a) May require dispute resolution or a forensic investigation b) May lead to charge backs	Modification
AR22	Surveillants	Snoop on commands and configuration changes	Put a tap on the link	a) Detect load limitation or disconnect commands in order to get knowledge on the creditworthiness of a consumer b) Understand custom commands to guess on HAN device types and capabilities	Disclosure
AR23	Frustrates, Cybercrime	Alter commands and configuration in transit or send arbitrary commands and configuration changes	Alter data in transit. Most likely, this requires the actor to setup a man-in-the-middle scenario.	a) Disconnect or load limit a consumer. Disconnection of multiple consumers at once may lead to significant impact on power supply.	Modification
AR24	Cybercrime	Drop or delay commands or disturb link	Cut wires or use radio jammer in order to render the link useless.	a) Delay restoration or to influence control of grid segments b) Avoid disconnects or load limitation	Interruption
AR25	Frustrates, Cybercrime	Resend old commands and configuration data	Connect to the link and send formerly recorded information	Disconnect or load limit a consumer.	Modification
AR26	Frustrates, Fraudsters, Surveil-	Planning to plant a trojan horse or tries to learn about	Put a tap on the link to snoop on firmware. Once the firmware is	a) Learn about the capabilities of a meter	Disclosure

	lants,Cybercrime	the meters hidden features.	recorded it can be analysed.	b) Discover vulnerabilities and create malware	
AR27	Frustrates, Fraudsters, Surveillants,Cybercrime	Try to plant a trojan horse.	Become man-in-the-middle (MitM) and alter firmware in transit or try to access a local interfaces and push the firmware on the device directly	Send manipulated firmware with planted back-door	Modification
AR28	Fraudsters, Cybercrime	Drop or delay firmware or render link useless	Cut wires or use radio jammer in order to render the link useless.	a) Prevent of security updates b) Cause truck roll	Interruption
AR29	Surveillants	Snoops on traffic (upstream meter data and downstream commands or firmware)	Create a malicious relay (rouge man-in-the-middle device)	Total surveillance of NAN activity	Disclosure
AR30	Frustrates, Surveillants,Cybercrime	Intercepts and alters traffic (upstream meter data and downstream commands or firmware)	Create a malicious relay (rouge man-in-the-middle device)	Enables all threats that apply for the WAN container assets as well	Modification
AR31	Cybercrime	Snoop upstream traffic from NAN devices	Malicious device pretends to be the upstream gateway	a) Intercept WAN <=> NAN activity b) Disconnect NAN devices from NAN	Modification
AR32	Surveillants	Access metering values over NAN link	Pretend to be a valid drive-by readout device	a) Receive alerts and audit records b) Receive metering values	Modification
AR33	Fraudsters, Cybercrime	Alter meter assets stored in meter	Pretend to be a valid drive-by maintenance device	a) Read data and receive audit records b) Alter configuration c) Push custom firmware to meter	Modification
AR34	Frustrates, Cybercrime	Snoop on pricing or DER information or gain access to	Pretend to be a valid HAN device	a) Receive pricing to compare price	Modification

		other HAN devices		plans b) Provide falsified information on DER which causes the DSO to calculate with wrong assumptions on available storage and energy resources c) Gain access to other HAN devices	
AR35	Fraudsters, Cybercrime	Pretend to be a valid HHU	Create a malicious HHU based on snooped messages.	a) Read data and receive audit records b) Alter configuration c) Push custom firmware to meter	Modification
AR36	Fraudsters, Cybercrime	Masquerade the HHU interface in order to capture and arbitrarily alter HHU to meter traffic	Create a malicious man-in-the-middle device to snoop on local bus traffic	Gain access to single meter or multiple meters.	Disclosure
AR37	Insider, Cybercrime	Manipulate information assets stored in the meter device.	Bugged hardware or software gets installed	a) Manipulate consumption records b) Provide remote control (Trojan horse)	Modification
AR38	Fraudsters	Avoid meter to count energy consumption	Do some rewiring to bypass the smart meter	Avoid billing.	Modification
AR39	Fraudsters, Cybercrime	Manipulate consumption values or try get hold of information assets stored in the meter	Rip of enclosure to analyse and maybe intercept or reprogram meter logic	a) Avoid energy billing b) Send trusted information c) Prevent disconnects or load-control d) Identify vulnerabilities	Disclosure
AR40	Fraudsters, Cybercrime	Get control over meter	Replace hardware parts with custom malicious hardware parts	a) Manipulate consumption records b) Provide remote	Modification

				control (Trojan horse)	
AR41	Fraudsters	Get control over meter	Manipulation of the available buttons	Discover secret access to hidden functionality	Modification
AR42	Fraudsters	Get control over meter	Manipulation of wired interfaces	Cause power glitches or power drops to fool access control logic	Disclosure
AR43	Fraudsters	Avoid billing	Intercept or alter wired or optical interface	Bypass the card limit	Modification

Table 13: Some Areas of Concern for the Smart Meter Environment

This analysis leaves the process with the identification of some areas of concern. Actually, the process would go further identifying additional threats to create better coverage for a full risk analysis. However, the identified areas of concern, also known as threats are considered sufficient in order to create a list of relevant controls for the analysis of a wireless metering protocol. The next section will identify mitigating controls

3.3 Mitigating Controls

This section focuses on the derivation of mitigating controls to counter the threats listed in table 13. Generally, there are two basic approaches to sufficiently mitigate threats. Either protect the assets accordingly or limit the threat agent opportunities. The latter is hard to achieve especially against well funded threat agents. Moreover, some threats are hard to counter but detective controls do at least help to recognise a related attack and to initiated appropriate procedures such as incident handling.

3.3.1 Primary Controls

The listed requirements predominantly approach to additionally protect the assets. Thereby, each entry will reference the according areas of concern (ARxx). Each entry will be attributed whether it is of preventive (P) or detective (D) type and whether the control applies to the scope of a metering security analysis. Section 3.3.2 will then bring up some implicit and assurance requirements which would need to be fulfilled as well.

ID	Control	Description	Scope	Type	Ref.
PC01	Data Confidentiality	Encrypt links, messages or selected fields which are exchanged between devices to ensure confidentiality of all data in any direction.	yes	P	AR01, AR08, AR17, AR22, AR26, AR36, AR43
PC02	Data Privacy	To avoid leakage of consumer and grid behaviour the smart meter shall send: a) the values on regular time base b) messages with fixed size	yes	P	AR02, AR08

PC03	Data Integrity	A message authentication code shall be applied in order to ensure integrity of connections, messages or fields and to allow for detection of manipulated messages. This could be achieved using: a) cipher-based MACs (CMAC) b) hash-based MACs (HMAC) c) digital signatures Note, digital signatures scheme will require for digital certificates and therefore require a public key infrastructure (PKI) being maintained.	yes	P	AR03, AR09, AR14, AR18, AR23, AR36, AR43
PC04	Event Detection	A message shall include a sequence field in order to detect accidentally or deliberately dropped messages at latest after the next valid message is received.	yes	D	AR04, AR12, AR15, AR19, AR24, AR28
PC05	Event Detection	To detect ongoing denial of service (DoS) conditions a heart beat could be used to indicate availability of the transmission channel.	yes	D	AR04, AR12, AR15, AR19, AR24, AR28
PC06	Entity Authentication	Entity authentication will guarantee authenticity of connections and will prevent adversaries to access devices or service or to run procedures on it. The requirement could be achieved using an authentication scheme.	yes	P	AR10, AR11, AR31, AR32, AR33, AR34
PC07	Freshness	To avoid replay attacks, freshness of messages needs to be verified at the recipient. Senders should apply a token to relevant messages. Note: To avoid tampering with the freshness, the token must be protected using appropriate integrity mechanisms.	yes	P	AR06, AR13, AR16, AR20, AR25, AR35
PC08	Non-Repudiation	Non-repudiation is difficult to achieve. Especially in M2M environments. A meter would need to generate and securely store its own key material. Key material would need to be protected from the utility to ensure non-repudiation of origin for billing relevant data and to ensure non-repudiation of receipt for pricing information. A trusted platform module (TPM) could help to achieve non-repudiation. However, integrity of timestamps, metering and pricing values need to be guaranteed.	yes	P	AR07, AR21
PC09	Data Confidentiality	Ensure data confidentiality over multiple hops to avoid malicious devices to spy on data.	yes	P	AR29, AR31
PC10	Data Integrity	Ensure data integrity over multiple hops to avoid mali-	yes	P	AR30

		cious devices to manipulate data.			
PC11	Data Origin Authentication	Data origin authentication will allow to verify the origin of data and to ensure a command originated from the HES or to ensure billing data did really originate from a certain meter. Data origin authentication can be achieved using: a) cipher-based MACs (CMAC) b) hash-based MACs (HMAC) c) digital signatures	yes	P	AR05, AR11
PC12	Access Control	To avoid data leakage a smart meter should employ appropriate access controls. Records, configuration and firmware should only be accessible by trusted entities such as the HES or HHU but not by a collector or relay.	yes	P	AR32, AR33, AR34
PC13	Platform Assurance	Assure integrity of the firmware and hardware to avoid deliberately or accidentally bugged meters. This could be achieved using trusted computing platform, by organisational measures and approval through third parties. a) Evaluation of source code, firmware and hardware parts or designs through third parties b) Protection of approved firmware build by digital signatures c) The trusted computing base shall ensure the integrity of the firmware and hardware parts d) Implementation of an information security management frameworks (ISMS) at the hardware and software suppliers and at the utility. e) Suppliers shall establish and maintain a security development live (SDL) cycle.	no	P	AR37, AR40
PC14	Fraud Detection	The utility will need to run some form of fraud detection systems. Near real-time metering will certainly provide to the accuracy of such detection systems.	no	D	AR38
PC15	Tamper Evidence	Smart meters need to implement mechanisms that prevent getting undetected access to any parts of the circuitry.	yes	D	AR39, AR40
PC16	Tamper Resistance	It should be considered that adversaries can read-out the firmware and memory contents of "lost" smart meters. Custom cryptographic boot loaders and blown micro controller interface (JTAG) fuses only provide limited protection [47], [48]. Accordingly, a smart meter shall not hold any shared secrets nor should the firmware contain hidden functionality.	no	P	AR41
PC17	Tamper Resistance	To improve tamper resistance, smart meters should make use of storage and processing devices that implement additional protection over common integrated circuits. Known protection techniques in smart cards	no	P,D	AR39

		[49] are: a) Put the read-only memory (ROM) in one of the middle layers in order to hide the ROM contents between outer layer logic b) Apply shields using layers and planes or wires which are carrying signals to complicate delayering c) Scramble transistors (glue logic) to complicate logic reversing. d) Hide buses in intermediate layers to avoid direct access to snoop on bus signals e) Apply encryption to memory contents and bus traffic f) Use anomaly sensors to detect temperature, voltage, current, clock issues g) Measures to counter fault injection			
PC18	Tamper Resistance	Hardware parts should be protected from power glitches and power drops at external interfaces.	no	P	AR42
PC19	Tamper Resistance	The meters should employ measures to counter common tampering attempts. Some of the measures [38], [50] include: *h) "Use rogowski coils* *i) Use ferrite beads, capacitor line filters and surface mounted devices (SMD) resistors* *j) Use high tolerant I/O* *k) Use active anti-tamper switches* *l) Use ball grid array (BGA) or chip on board (COB) techniques* *m) Disable writes on low voltage* *n) Protection against power glitches* *o) Protection against battery removal.* *p) Time stamping a tamper event* *q) Use monotonic counters" [38]*	no	P/D	AR38, AR39, AR40, AR41, AR42

Table 14: Primary Security Controls for Smart Meters

All listed entries make some assumptions and rely on maybe further implicit controls not identified so far. In order to provide adequate security services and mechanisms, the implicit controls must be fulfilled to.

3.3.2 Implicit Controls

This subsection will list implicit controls. These implicit controls will be the base assumption for primary controls. In case implicit controls are not fulfilled, their primary control will base on wrong assumptions and might not sufficiently mitigate a threat. Additionally, the listed implicit security controls in table 15 does also include security assurance requirements that have not been considered so far. Some of the implicit controls have been identified under aid of the common criteria standard [44].

ID	Implicit Control	Description	Scope	Type	Ref.
IC01	Encryption Algorithm	The meter shall implement an adequate stream or block cipher. Fall back to weak ciphers shall be denied.	yes	P	PC01
IC02	Encryption Mode	Meters that use block cipher shall implement adequate block cipher modes and avoid initial vector (IV) reuse.	yes	P	PC01
IC03	Encryption Mode	For modes that turn block ciphers into key stream generators, such as counter mode (CTR) or output feedback mode (OFB), keys and IVs shall never be reused to avoid key stream repetition.	yes	P	PC01
IC04	Encryption Mode	The meter shall apply encrypt-then-MAC instead of MAC-then-encrypt if not relying on an authenticated cipher mode such as counter mode with CBC-MAC (CCM) or EAX [51], [52].	yes	P	PC01
IC05	IV	IVs shall be carefully chosen. Ciphers that require random IVs will need a cryptographically strong random number generator (RNG).	yes	P	PC01
IC06	Encryption Key	The encryption algorithm should support sufficient key length. Assume a meter life cycles of up to 15 years, the symmetric encryption algorithm should support adequate key length until 2028.	yes	P	PC01
IC07	Cipher Suite	Ideally, smart meters would allow an upgrade of encryption algorithms in order to be able to react on issues.	yes	P	PC01, PC03
IC08	MAC Key	The message authentication code or signature shall use comparable key length [53] as the key used for data confidentiality.	yes	P	PC03
IC09	Key management	The meter should follow the key separation principle. Therefore, encryption and integrity algorithms should rely on different keys	yes	P	PC01, PC03
IC10	Key management	Key management and key derivation and destruction shall rely on approved standards.	yes	P	PC01, PC03
IC11	RNG	Ensure cryptographically strong random number generator to provide adequate IVs, key derivation and nonces. In addition, the source of entropy shall provide sufficient data during peaks and should remain steady over time.	yes	P	PC01, PC03

IC12	Audit Logs	The meter shall log all security relevant actions and events regardless whether the action passed or failed. Log records shall contain a) fine-grained reliable time stamps b) adequate information (e.g. reference to subject) to allow reconstruction of events. c) pass or fail	no	D	PC04, PC05, PC11, PC12,
IC13	Audit Logs	Audit logs shall be protected of modification and deletion.	no	D	PC04, PC05, PC11, PC12,
IC14	Audit Logs	Logs and events shall be collected and reviewed on regular base.	no	D	PC14
IC15	Passwords	If relying on passwords for authentication, the device shall enforce a password policy a) Ensure minimal password length b) Ensure complex passwords c) Ensure password change d) Remember password history e) Apply password ageing f) Avoid default passwords	yes	P	PC06
IC16	Passwords	Passwords shall be stored in irreversible and salted form.	yes	P	PC06
IC17	Authenticatio n	The chosen authentication scheme shall a) Prevent replay and reflection attacks b) Prevent user enumeration c) Prevent password brute-force attacks d) Ensure equal processing time for correct and wrong tries	yes	P	PC06
IC18	Session Handling	Devices that support multi-user access shall provide user session security after successful authentication. a) Provide random session identifier b) Ensure confidentiality of the session identifier c) Provide mechanism to free session (logout) d) Reject arbitrarily chosen session identifiers from client e) Change session identifier on user role changes	yes	P	PC06
IC19	Software bugs	Software running on smart meters shall be analysed for programming bugs [54] to avoid remote code execution or denial of service conditions. The major vulnerabilities include: a) Buffer overflows b) Format string vulnerabilities c) Integer overflows d) Of-by-one errors	no	P	PC13

		e) Race conditions f) Null pointer dereferences g) Use after free h) Double free			
IC20	Certificates	When relying on certificates the meter shall ensure a) Verify certificate revocation list (CRL) b) Proper certificate chain checking	yes	P	PC11
IC21	Configuration bugs	Ensure strong default configurations and avoid static secrets.	no	P	PC13
IC22	Device Time	Adequate timestamps will need synchronisation with a trusted time-source. The provided time needs to be protected from manipulation and its origin needs to be verified. Insufficient accuracy of the meter time may lead to denial of service or to security issues in mechanisms that relay on timestamps.	yes	P	PC03
IC23	Roles	The meter shall enforce a least-privilege principle for a set of roles and associated privileges on data assets.	yes	P	PC12
IC24	Information leakage	The meter shall not disclose information on version, type or build to unprivileged entities.	yes	P	PC01

Table 15: Implicit Security Requirements for Smart Meters

4 Conclusion

It is not the intent if this whitepaper to provide a thorough threat analysis on smart meters. However, the extent presented should allow to follow the structured identification of items of relevance using the OCTAVE Allegro risk assessment method [6]. A total of 43 controls have been defined. The identified information assets, security requirements, threat agents and areas of concern very much apply to any metering environment. Although the analysis is very much tailored to the analysis of wireless metering protocols, the listed controls provide a good starting point to any government, metering company, utility or meter manufacturer to verify their guidelines and meters' protection level.

5 Bibliography

[1] European Commission. Energy Efficiency Plan. 2011

[2] United States of America. H.R. 6582: American Energy Manufacturing Technical Corrections Act. 2012

[3] B. Cook et al. The smart meter and a smarter consumer:quantifying the benefits of smart meter implementation in the United States. In Chemistry Central Journal. 2012 (DOI 10.1186/1752-153X-6-S1-S5)

[4] CEN-CENELEC eMobility Co-ordination Group. Standardization for road vehicles and associated infrastructure. 2012

[5] W. Galand. Elster REX2 Smart Meter Teardown. iFixit . Jul. 2011. [Online]. Available: http://www.ifixit.com/Teardown/Elster+REX2+Smart+Meter+Teardown/5710/1 [Accessed: 31. Jan. 2013]

[6] R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson. The OCTAVE Allegro Guidebook, v1.0. Cert Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213. May 2007

[7] K. Boutorabi. You Can't Have The Smart Grid Without Smart Meters. Electronic Design. Jun. 2010. [Online]. Available: http://electronicdesign.com/article/power/you_can_t_have_the_smart_grid_without_smart_meters-60529 [Accessed: 31. Jan. 2013]

[8] F.M. Cleveland. Cyber security issues for Advanced Metering Infrastructure (AMI). In Proceedings of IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–5. 2008 (DOI 10.1109/PES.2008.4596535)

[9] S. McLaughlin, D. Podkuiko and P. McDaniel. Energy theft in the advanced metering infrastructure. . 2010 (ISBN 978-3-642-14378-6)

[10] J. Liu, Y. Xiao, S. Li, W. Liang and C.L.P. Chen. Cyber Security and Privacy Issues in Smart Grids. In IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 981–997. 2012 (DOI 10.1109/SURV.2011.122111.00145)

[11] A. Hahn and M. Govindarasu. Cyber Attack Exposure Evaluation Framework for the Smart Grid. In Proceedings of IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 835 –843. Dec. 2011 (DOI 10.1109/TSG.2011.2163829)

[12] M.A. Rahman, P. Bera, and E. Al-Shaer. SmartAnalyzer: A noninvasive security threat analyzer for AMI smart grid. In Proceedings of IEEE INFOCOM. Mar. 2012 (DOI 10.1109/INFCOM.2012.6195611)

[13] G.N. Sorebo and M.C. Echols. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. CRC Press. 2011 (ISBN 978-1-4398-5587-4)

[14] ENISA. Smart Grid Security: Annex I. General Concepts and Dependencies with ICT. 2012

[15] E.D. Knapp. Industrial Network Protocols, AMI and the Smart Grid. In Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress. 2011 (ISBN 978-1-59749-645-2)

[16] NIST. Security Profile for Advanced Metering Infrastructure. v2.0, Jun. 2010

[17] ENISA. Smart Grid Security: Recommendations for Europe and Member States. Jul. 2012

[18] M. Rafiei and S.M. Eftekhari, A practical smart metering using combination of power line communication (PLC) and WiFi protocols, In Proceedings of 17th Conference on Electrical Power Distribution Networks (EPDC), 2012, pp. 1–5, May 2012

[19] Federal Office for Information Security (BSI) Germany. Technische Richtlinie BSI-TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, v0.5. 2012

[20] EN 13575-1:2002: Communication system for meters and remote reading of meters - Part 1: Data exchange

[21] IEEE Std 802.15.4:2011. IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)

[22] C. Bennet and D. Highfill. Networking AMI Smart Meters. In Proceedings of Energy 2030 Conference. ENERGY 2008. IEEE. pp 1-8. Nov. 2008 (DOI 10.1109/ENERGY.2008.4781067)

[23] V. Aravinthan, V. Namboodiri, S. Sunku and W. Jewell. Wireless AMI Application and Security for Controlled Home Area Networks. In Proceedings of IEEE Power and Energy Society General Meeting, pp. 1-8. Jul. 2011 (DOI 10.1109/PES.2011.6038996)

[24] ZigBee Alliance. Home Automation Public Application Profile. ZigBee Profile: 0x0104 Revision 26, Version 1.1, Feb. 2010

[25] ZigBee Alliance. Smart Energy Profile Specification. ZigBee Profile: 0x0109, Revision 16, Version 1.1, Mar. 2011

[26] A. Sikora, P. Villalonga, and K. Landwehr. Extensions to wireless M-Bus protocol for smart metering and smart grid application. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, New York, pp. 399-404. Aug. 2012 (DOI 10.1145/2345396.2345462)

[27] EN50090-4-1:2004. Home and Building Electronic Systems (HBES) Part 4-1: Media independent layers - Application layer for HBES Class 1

[28] S. Cavalieri, G. Cutuli and M. Malgeri. A Study on Security Mechanisms in KNX-based Home/Building Automation Networks. In Proceedings of 2010 IEEE Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-4. Sep. 2010 (DOI 10.1109/ETFA.2010.5641237)

[29] EN 13575-6:2008: Communication system for meters and remote reading of meters - Part 6: Local Bus

[30] EN 62056-21:2002, Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange

[31] E. Zountouridou, E. Karfopoulos, S. Papathanassiou and N. Hatziargyriou. Energy-Efficient Computing and Networking. In Review of IEC/EN Standards for Data Exchange between Smart Meters and Devices, pp 95-103. N. Hatziargyriou, A. Dimeas, T. Tomtsi and A. Weidlich, Eds. Springer Berlin Heidelberg (ISBN 978-3-642-19321-7). 2011

[32] K. De Craemer and G. Deconinck, Analysis of state-of-the-art smart metering communication standards, In Proceedings of the 5th Young Researchers Symposium, Mar. 2010

[33] European Commission. Smart Grid Mandate: Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. Mar. 2011

[34] European Commission. Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441. Mar. 2009

[35] Smart Meters Co-Ordination Group. Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441: Final Report v0.7. Dec. 2009

[36] CEN/CENELEC/ETSI Joint Working Group. Final report Standards for Smart Grids. Jun. 2011

[37] ISO-27000:2009: Information technology - Security techniques - Information security management systems - Overview and vocabulary

[38] M. Arora. Smart Metering: Security Threats and Countermeasures. MALCON Conference 2012, New Delhi. Nov. 2012. [Online]. Available: http://www.malcon.org/research/2012/03%20Arora%20Mohit%20-Smart_Metering_Security_threads_MALCON.pdf [Accessed: 21. Feb. 2013]

[39] ISO-7498-2:1989: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture

[40] R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. CMU/SEI-2007-TR-012, CERT Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213. May 2007

[41] G. Sindre and A.L. Opdahl. Eliciting security requirements with misuse cases. Requirements Engineering Vol. 10 No. 1, pp. 34-44. Jun. 2004 (DOI 10.1007/s00766-004-0194-4)

[42] ISO 27002:2005: Information technology - Security techniques - Code of practice for information security management

[43] NIST. Security and Privacy Controls for Federal Information Systems and Organizations. Special Publication 800-53, Rev. 4, Final Public Draft, Feb. 2013

[44] ISO 15408-2:2008. IT - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components

[45] HMG Infosec Standard No. 1 (IS1), Part 1: Technical Risk Assessment

[46] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy Theft in the Advanced Metering Infrastructure. In Proceedings of the 4th International Conference on Critical Information Infrastructures Security (CRITIS'09), pp. 176–187. 2009. (ISBN 978-3-642-14378-6).

[47] T. Goodspeed. Side Channel Timing Attacks on MSP430 Microcontroller Firmware. Black Hat USA Briefings and Trainings, Las Vegas. Aug. 2008. [Online]. Available: www.blackhat.com/presentations/bh-usa-08/Goodspeed/BH_US_08_Goodspeed_Side-channel_Timing_Attacks_Slides.pdf [Accessed: 31. Jan. 2013]

[48] N. Lawson. Highway to Hell: Hacking Toll Systems. Black Hat USA Briefings and Trainings, Las Vegas. Aug. 2008. [Online]. Available: http://www.root.org/talks/BH2008_HackingTollSystems.pdf [Accessed: 31. Jan. 2013]

[49] M. Tunstall. Smart Card Security. In Smart Cards, Tokens, Security and Applications. Eds. K.E. Mayes and K. Markantonakis. Springer, New York. 2008 (ISBN 978-0-387-72197-2)

[50] M. Conner. Tamper-resistant smart power meters rely on isolated sensors. EDN Network. Mar. 2009. [Online]. Available: https://edn.com/design/power-management/4313844/Tamper-resistant-smart-power-meters-rely-on-isolated-sensors [Accessed: 24. Feb. 2013]

[51] M. Bellare, P. Rogaway, D. Wagner: The EAX Mode of Operation, Proceedings of the 11th International Workshop on Fast Software Encryption (FSE 2004), Lecture Notes in Computer Science, Vol. 3017, Delhi, India (Feb. 2004), pp. 389-407 (DOI 10.1007/978-3-540-25937-4_25)

[52] A. Moise, E. Beroset, T. Phinney and M. Burns. EAX' Cipher Mode. Computer Security Resource Center (CSRC), NIST. May 2011. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/eax-prime/eax-prime-spec.pdf [Accessed: 11. Feb. 2013]

[53] ECRYPT II. Yearly Report on Algorithms and Keysizes (2011-2012), Rev. 1.0. ECRYPT II Network of Excellence(NoE), funded within the Information Societies Technology (IST) Programme of the European Commission's Seventh Framework Programme (FP7). Sep. 2012. [Online]. Available: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf [Accessed: 11. Feb. 2013]

[54] R.C. Seacord. The CERT C Secure Coding Standard. Addison Wesley Professional. 2008 (ISBN 978-0-32156321-7)

6 Appendix Threat Analysis

6.1 Smart Meter Use Cases

These use cases have been considered in order to understand how information flows between systems in an AMI.

6.1.1 Wide Area Network Use Cases

This section gives a short description of services or use cases the WAN side interface need to manage. This is independent of meter software and the protocol being used for communication. Note, the major focus of these use cases lies on electricity metering. However, some of the cases do also apply to heat, gas and water meters.

Case	Description
UC_WAN_1	Transfer billing data to the HES.
UC_WAN_2	Transfer PQ measurements to the HES in order to guarantee PQ for the grid.
UC_WAN_3	Send alerts and audit records to the HES in order to react on issues with power supply or on issues with the meter itself.
UC_WAN_45	Populated available DERs to the HES in order to use it for demand response and peak shaping.
UC_WAN_6	Accurate pricing information needs to be pushed to the meter in a way that consumer can rely on the data and react accordingly
UC_WAN_7	Received and execute commands for load limitation, disconnects and consumer device control or device maintenance.
UC_WAN_8	Receive and upgrade system firmware to remain flexible for new business

Table 16: Wide Area Network Use Cases for Smart Meters, Gateways and Collectors

The list of use cases is not to be considered as an exhaustive list. It reflects some relevant cases which need to be handled by implementations. If not in current installations then in future installations. Therefore, the use cases in table Error: Reference source not found will be considered for the analysis of a wireless metering protocol.

6.1.2 Neighbourhood Area Network Use Cases

This section gives a short description of services or use cases the NAN side interface need to provide. These services are not dependent on meter software or any protocols. Meters in a mesh or multi-hop network are typically connected by their NAN interface only. Thus, for these devices, all of the use cases in table Error: Reference source not found need to be considered for devices which are connect by the NAN interface only

Case	Description
UC_NAN_1	A collector, gateway or repeater collects and relays metering information or alerts to its

	WAN interface.
UC_NAN_2	A collector, gateway or repeater forwards WAN initiated commands and data to NAN connected devices.
UC_NAN_3	A meter is registered within the NAN and with its upstream device (gateway, relay, collector, master)
UC_NAN_4	A meter sends alerts or billing information to a temporarily assigned NAN device (drive-by meter reading)
UC_NAN_5	A meter receives commands and configuration changes (provisioning) from temporarily assigned devices (installation and maintenance)
UC_NAN_6	A collector, gateway or repeater collects and relays metering information or alerts to its WAN interface.
UC_NAN_7	A collector, gateway or repeater forwards WAN initiated commands and data to NAN connected devices.

Table 17: Neighbourhood Area Network Use Cases for Smart, Gateways, Relays and Collectors

Some smart meter devices will need to support all of the NAN use cases listed in table Error: Reference source not found. However, the supported use cases mainly depend on the "smartness" of a meter. For example, a simple gas meter without remote controlled valve will maybe just need to send meter infos. The majority of these devices need local bus connectivity to be provisioned and will send bursts of meter information on pre-configured intervals. Thus, there is no need to evaluate complex use cases for such devices. Nonetheless, that section intends to capture more than just the current minimal set of use cases.

6.1.3 Home Area Network Use Cases

This section list a few major use cases for the HAN service interface. Although the term HAN is often used to refer to that interface it must not necessarily be restricted to "home installations". Thus, the interface could also provide services for a broader range of applications within building or industry automation. The general nature of the use cases listed in table Error: Reference source not found applies for a wide range of communication medium and protocol types and basically fit HAN, BAN and IAN.

Case	Description
UC_HAN_1	The HAN services can receive and forward information, actions and alerts from home, building and industrial automation systems
UC_HAN_2	Detect and report devices, storage and load to allow for demand-response
UC_HAN_3	Push grid status information, pricing information, consumption values and notifications to the home and building automation system or displays
UC_HAN_4	Grant access to specific devices and their information or services for load management purposes

Table 18: Home Area Network Use Cases for Smart Meters

The purpose of the HAN interface services is to integrate various applications and devices. This may also include fire alarms, health care applications or support of EVs as a DER. It seems that there are currently few implementations that rely on M-Bus for these services.

6.1.4 Local Bus Use Cases

This section gives a short description of services or use cases the HAN side interface need to manage. This is independent of meter software and the protocol being used for communication.

Case	Description
UC_LBUS_1	The local bus should simplify the initial and re-configuration effort of a smart meter
UC_LBUS_2	The local bus provides instant access to records such as metering values and alerts in order to support analysis purposes
UC_LBUS_3	The local bus allows to upgrade the meter firmware

Table 19: Local Bus Use Cases for Smart Meters

The local bus is intended to provide access during installation or maintenance. Typically, smart meters do support some form of serial protocol for communication. This could be traditional three-wire serial protocol or could be a two-wire or current loop interface.

6.1.5 Physical Use Cases

Finally, use cases which require physical access to the smart meter will be considered. The two actors identified will be the service technician as well as the property or facility manager.

Case	Description
UC_PHYS_1	A service technician installs smart meters. Thus, he does some wiring work around the meter and mounts the enclosure.
UC_PHYS_2	A service technician replaces a smart meter in case of faulty hardware that cannot be recovered from remote.
UC_PHYS_3	A service technician opens the smart meter and replaces broken hardware parts with new replacements or upgrades.
UC_PHYS_4	The facility manager accesses the meter and pushes buttons to flip through the smart meter menu to read different values at the meter display.
UC_PHYS_5	A consumer inserts its pre-pay card into the device.

Table 20: Physical Access Use Cases for Smart Meter

6.2 Enumeration of Information Asset Containers

6.2.1 Enumeration of physical containers

The enumeration of the physical information asset containers does normally not create many entries when analysing highly IT integrated organisations. However, a few physical locations with the presence of critical information assets have been identified. Again, the control and scope columns indicate whether the physical container is under direct control of the metering company and whether the physical container matters for a wireless metering protocol analysis.

ID	Container	Owner	Type	Scope
C20	Calibration data written on paper	Calibration company	External	no
C21	Physical backup media	Calibration company, Meter service company, Metering company, Utility	External	no
C22	Identification on meter instruction leaflet	Device manufacturer, Meter service company	External	no
C23	Initial credentials on meter instruction leaflet	Device manufacturer, Meter service company	External	no
C24	Consumption data on monthly invoice (paper)	Utility, Consumer	External	no
C25	Mobile storage media (CD-ROM, USB Stick)	Device manufacturer, Meter service company	External	no

Table 21: Physical Information Asset Containers

As expected, table 12 does not list many physical information asset containers. Moreover, the listed containers are not of major relevance for the protocol analysis. Nevertheless, they should be considered in the full context of an AMI analysis.

6.2.2 Enumeration of people containers

People information asset containers describe specific people or groups of people which have access to any of the critical information assets among an organisation.

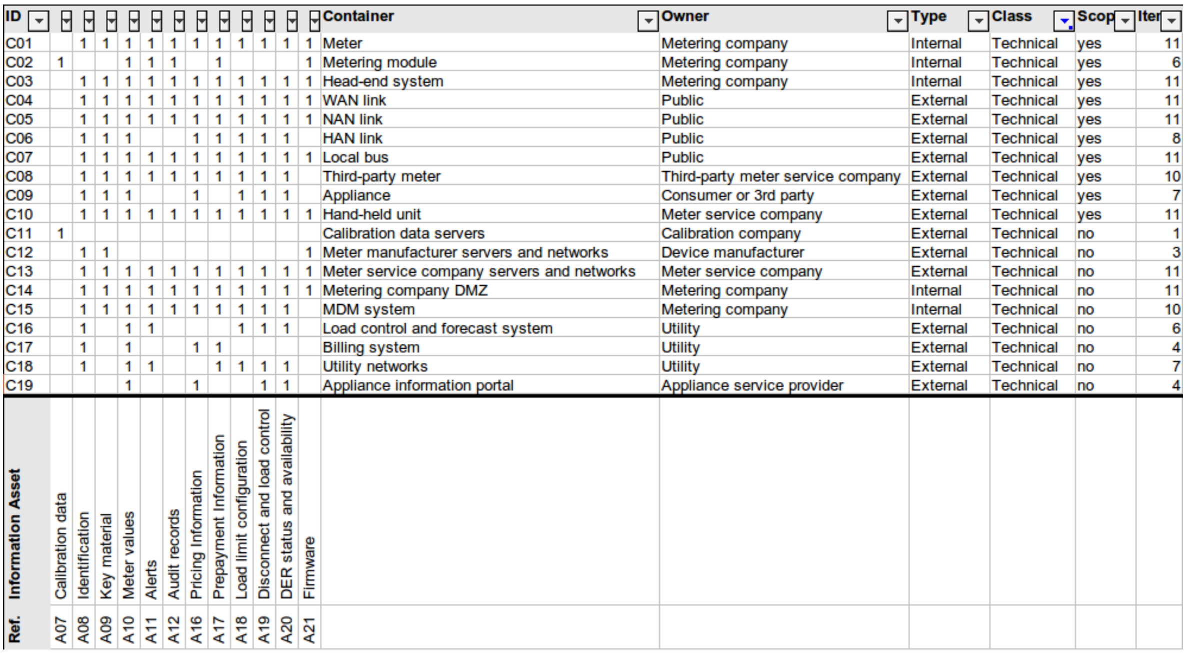
ID	Container	Owner	Type	Scope
C26	People at the calibration facility	Calibration company	External	no
C27	Service Technician	Meter service company, Third-party meter service company	External	no
C28	Consumer	Consumer	External	no
C29	MDM enrolment personnel	Metering company	Internal	no
C30	MDM maintenance personnel	Metering company	Internal	no
C31	Utility billing personnel	Utility	External	no
C32	Utility load mgmt. and forecasting personnel	Utility	External	no

Table 22: People Information Asset Containers

All groups listed in table 13 have been marked whether they belong directly to the assumed metering company and have been attributed whether they are relevant for the remainder of the analysis. The enumeration of the people information asset containers is the final activity of step three in [6].

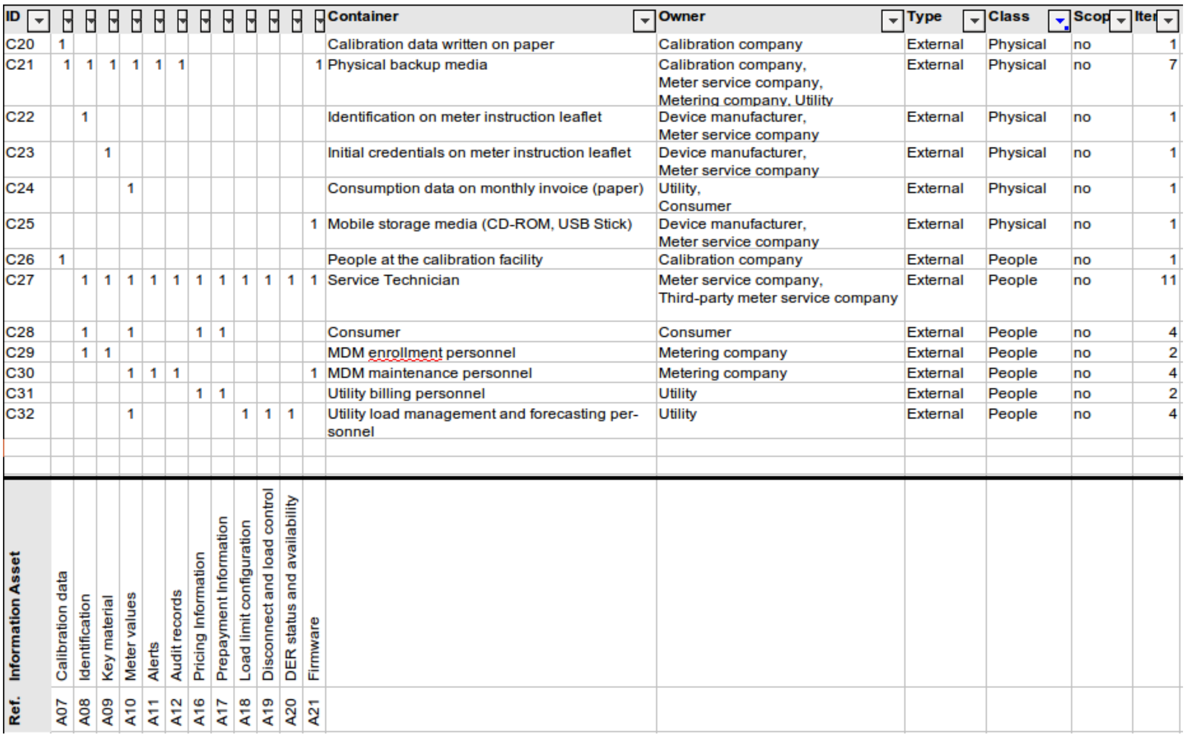
6.3 Supporting Materials

The below spreadsheets have served for the identification of all relevant information asset containers – of technical, physical or of people nature.



ID													Container	Owner	Type	Class	Scop	Iter
C01		1	1	1	1	1	1	1	1	1	1	1	Meter	Metering company	Internal	Technical	yes	11
C02	1			1	1	1		1				1	Metering module	Metering company	Internal	Technical	yes	6
C03		1	1	1	1	1	1	1	1	1	1	1	Head-end system	Metering company	Internal	Technical	yes	11
C04		1	1	1	1	1	1	1	1	1	1	1	WAN link	Public	External	Technical	yes	11
C05		1	1	1	1	1	1	1	1	1	1	1	NAN link	Public	External	Technical	yes	11
C06		1	1	1			1	1	1	1	1		HAN link	Public	External	Technical	yes	8
C07		1	1	1	1	1	1	1	1	1	1	1	Local bus	Public	External	Technical	yes	11
C08		1	1	1	1	1	1	1	1	1	1		Third-party meter	Third-party meter service company	External	Technical	yes	10
C09		1	1	1			1		1	1	1		Appliance	Consumer or 3rd party	External	Technical	yes	7
C10		1	1	1	1	1	1	1	1	1	1	1	Hand-held unit	Meter service company	External	Technical	yes	11
C11	1												Calibration data servers	Calibration company	External	Technical	no	1
C12		1	1									1	Meter manufacturer servers and networks	Device manufacturer	External	Technical	no	3
C13		1	1	1	1	1	1	1	1	1	1	1	Meter service company servers and networks	Meter service company	External	Technical	no	11
C14		1	1	1	1	1	1	1	1	1	1	1	Metering company DMZ	Metering company	Internal	Technical	no	11
C15		1	1	1	1	1	1	1	1	1	1		MDM system	Metering company	Internal	Technical	no	10
C16		1		1	1				1	1	1		Load control and forecast system	Utility	External	Technical	no	6
C17		1		1			1	1					Billing system	Utility	External	Technical	no	4
C18		1		1	1			1	1	1	1		Utility networks	Utility	External	Technical	no	7
C19				1			1			1	1		Appliance information portal	Appliance service provider	External	Technical	no	4
Information Asset	Calibration data	Identification	Key material	Meter values	Alerts	Audit records	Pricing Information	Prepayment Information	Load limit configuration	Disconnect and load control	DER status and availability	Firmware						
Ref.	A07	A08	A09	A10	A11	A12	A16	A17	A18	A19	A20	A21						

Figure 6: Technical Information Asset Containers Raw Material



ID													Container	Owner	Type	Class	Scop	Iter
C20	1												Calibration data written on paper	Calibration company	External	Physical	no	1
C21	1	1	1	1	1	1						1	Physical backup media	Calibration company, Meter service company, Metering company, Utility	External	Physical	no	7
C22		1											Identification on meter instruction leaflet	Device manufacturer, Meter service company	External	Physical	no	1
C23			1										Initial credentials on meter instruction leaflet	Device manufacturer, Meter service company	External	Physical	no	1
C24				1									Consumption data on monthly invoice (paper)	Utility, Consumer	External	Physical	no	1
C25												1	Mobile storage media (CD-ROM, USB Stick)	Device manufacturer, Meter service company	External	Physical	no	1
C26	1												People at the calibration facility	Calibration company	External	People	no	1
C27		1	1	1	1	1	1	1	1	1	1	1	Service Technician	Meter service company, Third-party meter service company	External	People	no	11
C28		1		1			1	1					Consumer	Consumer	External	People	no	4
C29		1	1										MDM enrollment personnel	Metering company	External	People	no	2
C30				1	1	1						1	MDM maintenance personnel	Metering company	External	People	no	4
C31							1	1					Utility billing personnel	Utility	External	People	no	2
C32				1					1	1	1		Utility load management and forecasting personnel	Utility	External	People	no	4
Information Asset	Calibration data	Identification	Key material	Meter values	Alerts	Audit records	Pricing Information	Prepayment Information	Load limit configuration	Disconnect and load control	DER status and availability	Firmware						
Ref.	A07	A08	A09	A10	A11	A12	A16	A17	A18	A19	A20	A21						

Figure 7: Physical and People Information Asset Containers Raw Material