Introducing an approach for measuring security level in Smart Grid

Raul Khaydarshin

Master Thesis
Programming and Networks
30 ECTS

Department of Informatics

UNIVERSITY of OSLO

06/2017

Introducing an approach for measuring security level in Smart Grid

2017

Introducing an approach for measuring security level in Smart Grid

Raul Khaydarshin

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Abstract

In the given research evaluations were conducted of the security level for Advanced Metering Infrastructure (AMI) as a part of Smart Grid infrastructure. The solution for an AMI comes from the vendor of Aidon. The evaluations were conducted for various usage scenarios for an AMI. The major focus was on Smart Meter.

The security level has been calculated by using a novel methodology called the Multi-Metrics approach.

The necessity of security level evaluations is based on the fact that the Smart Meter and the measurements it takes are valuable information assets, the loss or corruption of which can have material/financial consequences on the consumer and the utility. The tampering of data exchanged between Smart Meter and the central entity would result in altering Smart Grid operations. Thus, it is of paramount importance to understand the capabilities for an AMI to counter malicious intrusion attempts and to have assurance that the Smart Meter is capable of resisting tampering. Those assessments are reflected in the calculated security level of an AMI.

In this thesis was defined what security level for an AMI is reasonable to achieve for every specific scenarios. Additionally, in the thesis was found that an AMI system can be configured in multiple ways.

The significance of found results was that in this thesis was outlined a method for assisting in resolving the problem of making a right choice between various configurations for an AMI yielding almost the same security goal.

Acknowledgments

I would like to thank my supervisors Seraj Fayyad and Josef Noll for that enormous amount of time they spend correcting me thus not allowing to derail from a right track in my work.

List of Figures

List of Tables

List of Appendixes

Abbreviations

AC	Access Control
AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
AMM	Automatic Meter Management
AMR	Automatic Meter Readings
AMS	Automatic Meter
CC	Common Criteria
CIA	Confidentiality Integrity Availability
CS	Central System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DFD	Data Flow Diagram
DMS	Data Management System
DoS	Denial of Service
DSO	Distributed System Operator
EAL	Evaluation Assurance Level
EMS	Energy Management System
ES	Embedded Systems
ESD	Energy Service Device
HMI	Human Machine Interface
HW	Hardware
ICT	Information and Communication Technologies
IED	Intelligent Electronic Device
IO	Information Object
IoT	Internet of Things
IPSec	Internet Protocol Security
LED	Light Emission Diode
MCD	Multi-Connectivity Device
MCU	Microcontroller Unit
MDMS	Meter Data Management System
MM	Multi Metrics
MSN	Mobile Cellular Network
NVE	Norges Vassdrags- og Energidirektorat
OS	Operative System
PG	Power Grid
PQ	Power Quality
RF	Radio Frequency
RMSWD	Root Mean Square Weighted Data
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SLA	Service Level Agreement
SM	Smart Meter

SPD	Security Privacy Dependability
SPF	Single Point of Failure
SuI	System under Investigation
SW	Software
TPM	Trusted Platform Module
VM	Virtual Machine
WSN	Wireless Sensor Network

Content

1 Introduction

1.1 Introduction

IT security has always been a concern for both users and developers. Alarmingly, we know for a fact that anybody can fall victim to the misuse of IT systems. The US Computer Science and Telecommunications Board, therefore, warns that good cybersecurity is essential to protect national interests. Heeding this warning can act as a guideline for entities on all political levels in every nation (Benioef & Lazowska, 2005).

More components linked together increases complexity. In sum, complexity and connectivity increase the vulnerability of critical infrastructures. Security-related threats to power grids demonstrate how critical it is to keep these infrastructures uncompromised by malign forces who wish to do harm. Impairment of these systems can make societies come to a standstill in the short and long term (Dhanjani, 2015). This scenario exists not only on a theoretical level. Cyberattacks have been carried out on power grids in practice. There were, for instance, incidents in the Ukraine where hackers on multiple occasions have corrupted control systems, disrupting the power supply to end users (Condliffe, 2016).

Thus, to secure IT components in these vital infrastructures from outside tampering is of utmost importance. Best practice in the cybersecurity community posits that the *CIA triangle* is a useful construct when we speak of security objectives in an IT system. CIA is here an abbreviation which stands for confidentiality, integrity, and availability.

- *Confidentiality* means that malicious counter-parties should not understand data.

- *Integrity* deals with the problem of preserving the data in their original state, not altered.

- *Availability* is about keeping access to data constantly on, i.e. data have to be available at any time upon request.

There exist certain mechanisms for reaching these objectives. Unfortunately, most organizations do not live in a perfect world where all goals are easily achievable. The price of using every known tool to achieve all the edges in the CIA triangle might be too high. This is the reason why agents in charge of each system must prioritize among the security objectives and carefully choose among the mechanisms which accomplish the stated goals.

It is hard to fix problems without sufficient awareness of what the crux of the problems actually is. To analyze the security level in the IT system is, therefore, the first step for any entity. Unfortunately, there exists no definitive and standard methodology of accomplishing such measures.

On the bright side, some methods and techniques assist us in the comprehension of the security level, even though these techniques are mostly uncoordinated to each other. Likewise, althoug making comparisons between systems is a complex undertaking, initiating a thorough analysis can result in conclusions which are of great help to users and developers.

1.2 Statement of the problem

Security by definition has no unit of measurement. The security level is usually conveyed by simple categorizations, such as good, bad or average security. However, these broad categorizations say nothing about the most prescient security threats against the system, which are of high importance since attacks can come in the form of Man-in-the-Middle, buffer overflow, message replay and so on. Thus, there is a need for a better classification scheme where the security threats are handled more granularly and where one can get a clearer handle on the actual security level by precise measurements. But how should one go about picking a framework when there is no normative measurement scheme?

The answer is not to let the perfect be the enemy of the good. One must choose one of the competing frameworks which can render the best result for the case in hand. Effective action requires measurements. Furthermore, by measuring, we can turn actions into well-defined engineering problems. In this thesis, we are using a novel Multi Metrics (MM) approach assessing the security level of a smart meter. Particularly, we are going to evaluate one part of an Advanced Metering Infrastructure (AMI) system, concentrating on interactions between the single Smart Meter (SM) and the Head End (HE) system.

1.3 Motivation

By the end of 2018, the old electrical energy metering devices will have been exchanged with new, improved equipment. All these devices will be integrated into local AMIs. Each AMI will provide a more sophisticated method for measuring energy consumption, which gives an opportunity for more flexibility in governing it. This could lead to more smart energy usage and reduced billings and could even lessen the impact on the environment.

The deployment of AMI has its drawbacks too. One side of usage of AMI implies that the vulnerabilities that exist in its implementation may be exploited for malicious purposes. This purpose might be directed against the owner of household as well as the power distributor or billing entity. The latter case does not exclude the possibility of the participation of house owner himself. The malicious entity might gain the knowledge of the absence of the homeowner for the purpose of making an attempt to access the house illegally. Other malicious entities might intend to do damage to the power distributor. This includes that they might execute DoS attacks, which could lead to an outage of the power supply, in an attempt to tamper metering results to cause financial loss to the distributor.

Determination of which product to use out of many existing market solutions can create difficulties for both the power distribution entity and the household owner. Both need to decide what product to choose, having in mind different parameters, such as usability convenience, purchasing and exploitation price, and many others. The

security aspect of this choice will play an important role. For assisting in making a decision on the security qualities of an AMI system, there is a need for a particular reliable methodology.

The novel Multi Metrics approach for security metering of the system under investigation (SuI) is the sought method. The Multi Metrics approach breaks down the whole system into subsystems and components. Then using a composition of scenarios for SuI, the approach is used to determine what component and subsystem is in use for that particular scenario and assesses the security level for that scenario. Afterwards, each of the usage cases are evaluated and compared against the necessary security level for each case. This comparison concludes in an overview of how good system efficiency is for each usage case, and as follows, it shows the total system trustworthiness.

There are several vendors of AMI systems. The two dominating actors in the Norwegian Market are Kamstrup and Aidon (its-wiki.no, 2017).
In this thesis, the solution from Aidon is going to be investigated. The AMI system produced by Aidon is called Automatic Meter Management (AMM). The Aidon AMM is a part of an IoTSec project. The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure (its-wiki.no, 2017). This project is deployed at Department of Technology Systems (ITS), and the current thesis is proposed at this department. This explains why Aidon AMM was chosen as a subject of investigation in this thesis.
As a result, the security level of Aidon AMM was evaluated using the MM approach.

1.4 Research questions

The following research questions were addressed in this study:

- ❏ The promise of MM approach – is it a convenient meterstick for security level assessment in embedded systems ?
- ❏ How to evaluate the security level of particular AMI system – Aidon AMM ?

1.5 Definitions

The definitions, listed below are taken from the standard **NS-ISO/IEC 27000:2009** and are used throughout the thesis.

Access control

Means to ensure that access to assets is authorized and restricted based on business and security requirements

Accountability

Responsibility of an entity for its actions and decisions

Asset

Anything that has value to the organization

NOTE: There are many types of assets, including:

a) information
b) software, such as a computer program
c) hardware, such as a computer
d) services
e) people, and their qualifications, skills, and experience
f) intangibles, such as reputation, and image

Attack

Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Authentication

Provision of assurance that a claimed characteristic of an entity is correct

Availability

Property of being accessible and usable upon demand by an authorized entity

Confidentiality

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Event

Occurrence of a particular set of circumstances

Information asset

Knowledge or data that has value to the organization

Information security

Preservation of confidentiality, integrity and availability of information

Integrity

Property of protecting the accuracy and completeness of assets

Non-repudiation

Ability to prove the occurrence of claimed event or action and its originated entities, in order to resolve disputes about the occurrence of the event or action and involvement of entities in the event

Process

Set of interrelated or interacting activities which transforms inputs into outputs

Reliability

Property of consistent intended behavior and results

Threat

Potential cause of an unwanted incident, which may result in harm to a system or organization

Vulnerability

Weakness of an asset or control that can be exploited by a threat

(Buchla, International Organization for, & International Electrotechnical, 2012)

1.6 Limitations

There are four limitations which may affect the validity of the results obtained in this thesis.

The first limitation is that an AMI consists of several building blocks. The thesis is only looking at one of these blocks, namely, the interactions between a single SM and HE. Although, the analysis of this block gives an indication of the security level of the total system, it is only an indication and not an overall assessment of the system as a whole.

The second limitation is that the thesis is looking specifically into parts of the system where smart meters are implemented in residential installations, but at the same time it is known that an AMI also contains commercial and industrial installations. These factors escape the research's investigation even though they can have an influence on the overall security level of the AMM. An additional factor is that a smart meter from Aidon would be considered in general, although there are several models in the Aidon's production line.

The third limitation is that only security is going to be evaluated. Privacy and dependability issues are not going to be considered.

The fourth limitation is that the analysis is static. This thesis does not take into account how interconnected components may influence each other inside of Aidon AMM.

1.7 Thesis structure

The thesis is organized in following structure:

Introduction

The introduction provides a short overview of IT security objectives and introduces the purpose of security mechanisms. *Statement of the problem* presents necessity of security measurements. *The purpose of the study* presents methodology and case study. Research questions state the questions attempted to be answered with the current study. *Limitations* discuss weaknesses and limitations of the study.

Background and Literature review

Background and Literature review provides explanations of the SPD concept, IoT structure and existing approaches in security measurements. Literature overview presents a review of existing research works regarding the development of methods of measuring security.

Method

Method provides a detailed description of how to apply Multi Metrics approach on the System under Investigation (SuI).

Applicability of Multi Metrics approach on AMI System

Applicability of Multi Metrics approach on AMI System provides a detailed description of Aidon AMM system, application of Multi Metrics approach on Aidon AMM to evaluate its security level and analysis of obtained results.

Discussion

The discussion provides an overview of limitations of the study, suggests recommendations for continuing and expanding the current research and highlights key conclusions of the work as a whole.

2 Background and Literature review

2.1 Background

2.1.1 Security Privacy Dependability (SPD) Concept

Computer security, communication security, information security and information assurance are terms that are connected to three primary objectives of confidentiality, integrity, and availability (Avizienis, Laprie, Randell, & Landwehr, 2004). To this extent, Security is a union of attributes; Confidentiality deals with prevention of unauthorized disclosure of information, Integrity deals with limiting permissions to only authorized entities when storing, processing, transmitting, deleting, and Availability deals with providing immediate access to data upon authorized request. Since all these attributes are connected to authorized entities or requesters, one can summarize that security deals with preventing unauthorized access to data.

One of the most consistent definitions of Dependability is that system should be resilient enough to avoid those service failures that occur more frequently, or that the consequences of their influence are not greater than a certain acceptable level. Dependability is introduced as a global concept including reliability, availability, safety, integrity, and maintainability (Avizienis et al., 2004). In short, dependability is concerned with keeping a system free of faults, errors, and failures to some extent.

Avizienis et al. (2004) propose following relations among those two concepts, as shown in Figure 2.1.

Source: (Avizienis et al., 2004)

Figure 2.1: Dependability and Security relationship.

From this figure, one can see that Availability and Integrity relate to two domains, whilst Confidentiality relates to only the Security domain.

A general definition of Privacy is the ability of a person to seclude himself or information about himself (Wikipedia, 2017). In regards to data privacy, attention needs to be given whenever and wherever personally identifiable information is stored, used, collected and deleted. The privacy domain overlaps with security when it comes to data protection. Personal and sensitive data have to be protected while stored and transmitted.

The author, having analyzed this principle, proposed the view of Privacy and Security composition as shown in Figure 2.2.

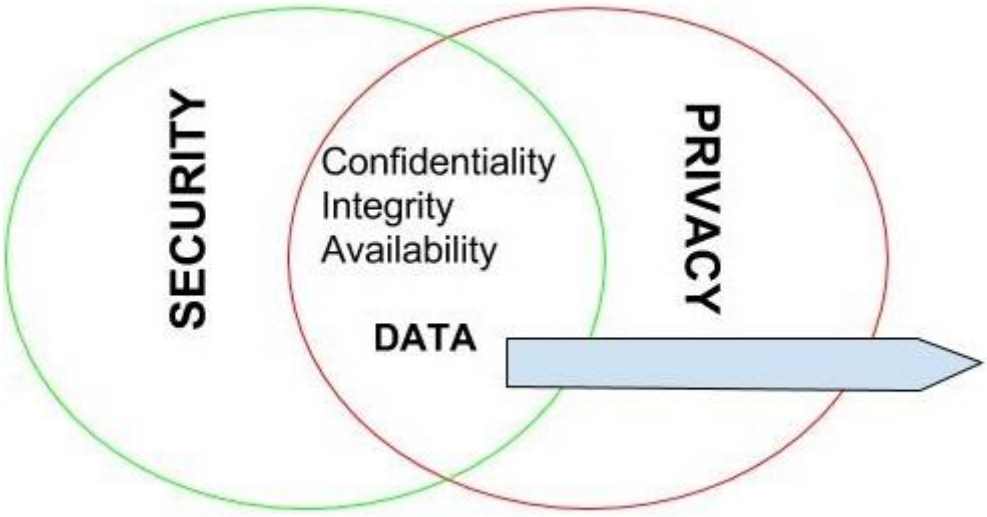
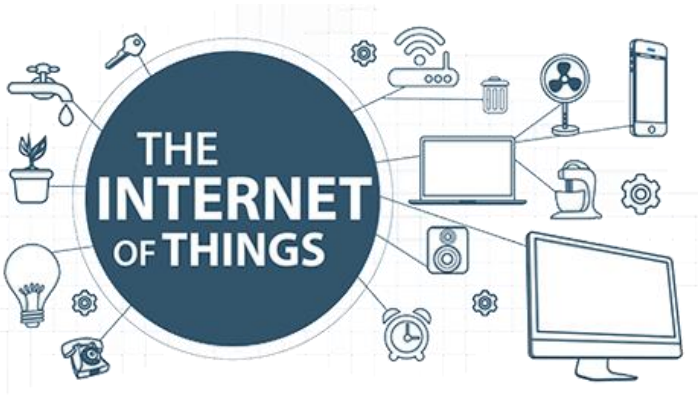


Figure 2.2: Security and Privacy relationship

Security and Privacy have common areas where data security objectives are preserved. From the other side, the owner of the data is able to deliberately givi away data to a third party. In this way, the trustworthiness of the system which owns the data might be altered towards its users.

As follows, the computer system and communications should be dependable, secure and trusted by users.

2.1.2 Internet of Things (IoT) infrastructure



Source: (SynapseIndia, 2017)

Figure 2.3: Simplified view of IoT.

A simplified explanation of IoT is that the numerous Things, which are not human operated, have the ability to collect and exchange data. They have the potential to connect to each other and other units like servers, cloud storages, applications on user computers and so on, through the Internet. Figure 2.3 illustrates this concept. “Things” here mean sensors and sensor networks (WSN), devices with embedded RFID tags, mobile phones, and laptops, just to name a few.

Things might be grouped into infrastructures with intentions to provide certain services like power consumption metering, health assistance, transport flow administrations and so on. Such infrastructures often obtain their names according to the function they execute, e.g. Smart Home, Smart City, Smart Grid, Smart Farming.

In different research sources on IoT, the structure of IoT is described using layered composition. In general IoT architecture should have a layer at the lowest level which contains the devices collecting data, such as measuring devices and actuators. The middle layer should provide network connections. This layer interfaces with the lowest layer. Finally, the layer, which interacts with users and applications, is placed on the top. This upper layer, in turn, interfaces with the middle layer. It is noted that such division of IoT into a limited number of layers has coarse-grained granularity but helps to give an overall picture of the IoT architecture. Jing et al. (2014) define the

IoT infrastructure as it is shown in Table 2.0. Giving layered insight is completed with examples of possible implementation and examples of used technologies.

Table 2.1: IoT layered infrastructure.

Application Layer	IoT applications	Intelligent logistics, Smart Home, Smart Grid, Intelligent traffic
	Application support layer	Middleware technology, Cloud computing, Information development platform
Transportation Layer	Local area network	Ethernet
	Core network	Internet
	Access network	Mobile network, WIFI
Perception Layer	Perception network	RFID sensor network and nodes Wireless sensor network and nodes
	Perception node	

Source: (Jing, Vasilakos, Wan, Lu, & Qiu, 2014)

Perception layer accommodates technologies such as WSN, RFID, GPS and the like. This layer is divided into two sub-layers - Perception node layer and Perception network. Nodes carry out data acquisition and control functions. Perception network is used for communications with the transportation layer.

Transportation layer, in turn, is divided into three layers - Access, Core, and Local area networks. This layer acquires data from a lower layer at the place where devices belonging to lowest layer are placed and hands it out to the upper layer. This means that the transportation layer should carry data to the top layer, which may happen to be at a distant location. Special for the transportation layer is that it consists of a great variety of heterogeneous networking technologies, such as Ethernet LAN and different cellular and wireless networks.

Application layer is divided into two layers - Application support layer and IoT application layer. Application support layer realizes intelligent computation and resource allocation in screening, selecting, producing and processing data. IoT

applications layer includes individual tailor made specific business products (Jing, Vasilakos et al. 2014).

The functional structure of IoT as a vision of Lopez Research LLC (LLC, 2013), comprises three cases. The first one, Communication case, means that manually and infrequently gathered information and information which could not have been accessed before, provided to the people and systems. Aspects, ad considered in this case, play a major role in healthcare systems and transportation services, for example. The second, Control and Automation cases handle the ability of remotely controlled equipment to provide an extra level of freedom to businesses and consumers. Smart home things and SCADA networks take advantage of this functionality. The third case in this row is the purpose of Cost Savings. IoT functionality manages to contribute in reaching this goal to industrial companies, for example, by minimizing equipment failure and performing planned maintenance. Additionally, Advanced Metering Infrastructure, which is the subject of this study, contributes to customers, becoming aware of energy consumption patterns and provides with possibilities for its more intelligent usage.

The layered infrastructure and functional purposes draw the main picture of IoT infrastructure to show how IoT can help businesses gain efficiencies, harness intelligence from a wide range of equipment, improve operations and increase customer satisfaction (LLC, 2013).

2.1.3 Security considerations for IoT

As shown in the previous section, the IoT structure overview, one part of devices, populating lower layer of IoT, consist of sensors and actuators. Those devices might have a less capable CPU or RAM, limited battery power, and be located in open environments. Another part of IoT devices are not limited in the aforementioned resources, for example those belonging to Smart Grid infrastructure, which are supplied from a power network, and are therefore not limited strictly on computing resources. To fully understanding of what is special for global IoT infrastructure,

research, conducted by Cisco, highlights the following security challenges to IoT (Cisco, 2015):

- *Scalability* - meaning that the number of devices connected to IoT infrastructures grows exponentially, potentially to hundreds of thousands of millions of endpoints, which in turn give rise to an enormous amount of data processing needs.
- *Remote locations* - meaning that devices, belonging to IoT infrastructure can be placed in remote locations which increases their physical vulnerability.
- *Availability* - meaning that critical infrastructures, which are participating in IoT, prioritize availability over other security objectives. This can lead to system engineers preferring no inbuilt security controls in a system, designed to not risk an outage resulting from a false positive.

These challenges make security issues unique for IoT infrastructure compared to traditional IT systems. The decisive factor is that IoT infrastructure, which is created to store, process and transport data, faces an increased attack surface. Multiple research projects, aimed to give an overview of threat vector in security issues for IoT, were conducted. An educational and compressed analysis by Whitehouse et al. (2014) shows a summary of threat classes that IoT products will cope with, reviewed in Table 2.01.

Table 2.2: Threat classes defined by NCC Group.

Threat	Description	Impact
Compromise: remote	Compromising of the device and its data, either partially or entirely, typically over network.	External security boundary is breached.
Compromise: local	Compromising of device or its data, either partially or entirely locally, through either HW or SW means.	External security boundary is breached.
Privilege escalation	Increase in access, either locally or remotely, breaching a security boundary.	Degradation or failure of a security boundary leading to an increased level of access either on a temporary or permanent basis.
Impersonation	Impersonation of a trusted entity.	Degradation or failure of a security boundary leading to an increased level of access either on a temporary or permanent basis.
Persistence	Persistent access is obtained post-compromise through configuration, modification or HW, SW manipulation.	Integrity of platform or external security boundary enforcement is no longer effective
Denial of service	Service is lost, either partially or entirely, on a temporary or a permanent basis.	Degradation in availability or functionality.

Source: (Whitehouse, 2014)

Threat classes shown in this table have a different probability of occurrence at the present moment. However, this situation might change in time, which must be taken to account since the lifetime of IoT devices may vary drastically. This variation could be from a few years up to ten or more. Another aspect is that degree of influence by a particular threat on the individual IoT device depends on its intended functionality (Whitehouse, 2014).

An IoT device, being a participator in a large IoT system, may be used as an access point to this system by a malicious entity. For this reason attention and care should be paid not to the only device as a separate entity but to the system this device is integrated into as well. The following considerations, with regards to device functionality use cases and potential impacts, might be relevant in IoT system evaluation:

- *Public and Personal Safety and Security.* M2M interactions, such as the health care sector and smart transport systems, elevate life safety and security attitudes.
- *Ad Hoc and Transient Relationships.* Short lived relationships, such as in the case of NFC, Wi-Fi beacons usage. Constructed by wearable devices, Zig-Bee temporary ad hoc networks can mean no implicit trust. Thus, the concern regarding the considerations in ensuring privacy and security araises.
- *Underlying Transport Infrastructure Security and Resiliency*. The lifespan of a particular IoT device might happen to be of many years. An example of technologies which seemed to be secure, such as GSM, WEP and other wireless technologies, were shown to have security holes. Thus, lifespan guarantee in the flawless functioning of the IoT system based on usage of some of those technologies has been proven to be erroneous.
- *Internet Environment Footprint and Impact.* When using the Internet as a transport medium, the designer of an IoT system should consider possible bandwidth-constrained and higher-latency connections. They can impact the faultless functioning of the whole IoT-enabled system. Another aspect consists in the possibility of backtracking internal connections of the system's data flows, which can lead to loss of intactness of security objectives.
- *Intellectual Property Protection.* The vendor might be considering protection of high-value intellectual property, built into the device. However, there are no guarantees of preserving it when the device falls into the physical possession of a malicious entity (Whitehouse, 2014).

The outlined security threats and challenges characterizing IoT infrastructure give an overall understanding of drawbacks that infrastructure can bring with it. To conclude with IoT security aspects, the following contemplations are submitted.

The Internet page dedicated to IoT issues, *internetofthingswiki.com,* points out that “security is one of the major concerns of experts who believe virtually endless connected devices and information sharing can severely compromise one’s security and well-being. Unlike other hacking episodes which compromise online data and privacy with IoT devices can open the gateway for an entire network to be hacked" (Wiki, 2016). Another security expert, Eugene Kaspersky, chief executive of Kaspersky Lab., the world's largest private cyber security company said that Internet of Things for us is Internet of threats for us (Hjelmgaard, 2016).

2.2 Literature review

Existing methods for defining metrics can be classified into two groups, system-centric and attack centric approaches.

Attack centric approach focuses on attacks for the evaluation of system's security level. The factors such as attacker's capabilities, resources and behavior are analyzed for carrying out assessments.

In attacker-centric approach, we can analyze a system by making different assumptions about attacker capabilities and resources, but at the same time, the model formulation requires us to quantify those capabilities (Nicol, 2005).

The system-centric approach concentrates on the system for evaluation of security level for a given system. The factors such as system design, configurations, and capabilities are analyzed in this case (Noll, Garitano, Fayyad, & Abie, 2014).

The scholarly articles for literature review section are chosen with a focus on relation to developing metrics for security assessment of the system under investigation. This choice will address two areas related to security assessments. The first section will address research related to attack centric approach and the second section will focus on research studies on system-centric approach.

2.2.1 Attack centric approach

Cyberattack exposure evaluation framework

The Smart Grid (SG) consists of domains including generation, transmission, distribution and marked operations (Hahn & Govindarasu, 2011). There are interactions inside of a domain as well as interactions between the domains. Smoothly grid operation depends on trust level between domains. The necessity of building a model, reflecting those levels and associated risks arises.

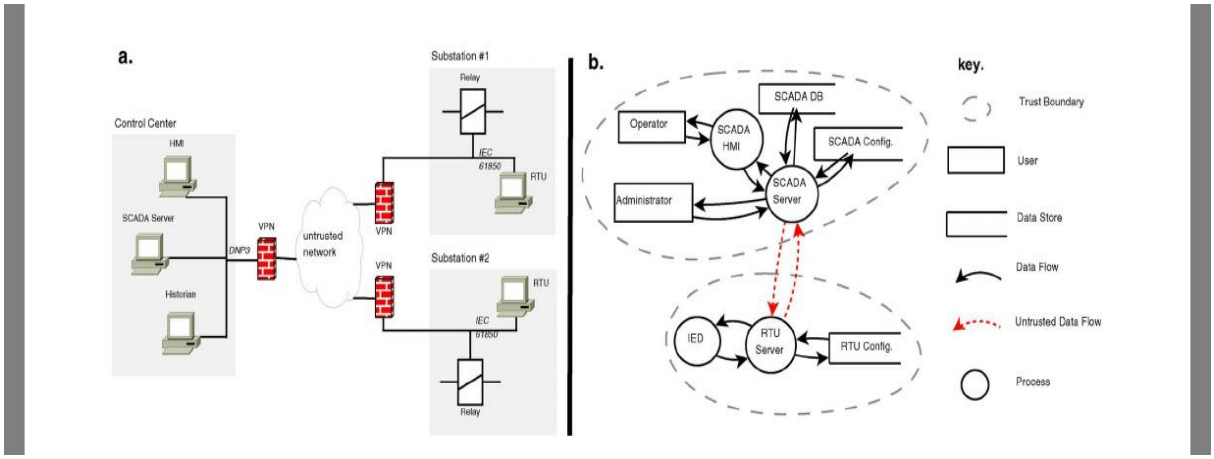
The purpose of study “Cyber Attack Exposure Evaluation Framework for the Smart Grid” is in finding different privilege states in SG architecture. The second goal is the evaluation of possible paths, which an attacker could exploit.

As a result of this study, a framework was developed in which final result is a calculation of an exposure metric *exp*. It is a value, calculated along the path, which an attacker would follow to reach the asset or Information Object (IO) in SG.

In the first place, some definitions used in this framework should be given:

- Privilege (P) represents user/system access permission to particular IO within an infrastructure,
- Security Mechanisms (SM) accounts for a particular mechanism to provide security,
- Untrusted user (A) represents an Attacker.

The framework starts with the process of threats modeling. It defines Data Flow Diagram (DFD), trusted boundaries and untrusted input. Hahn et al. (2011) show a PowerCyber SCADA testbed at Iowa State University (ISU) and DFDs from a Control Center to one of the substations as in Figure 2.4.



Source: (Hahn & Govindarasu, 2011)

Figure 2.4: Cyber Attack Exposure Evaluation Framework:

a) Testbed for SG architecture

b) Testbed DFD

In this figure, two trust zones are identified. The first one is the control center, where operator interact with a Human-Machine Interface (HMI). This interface controls

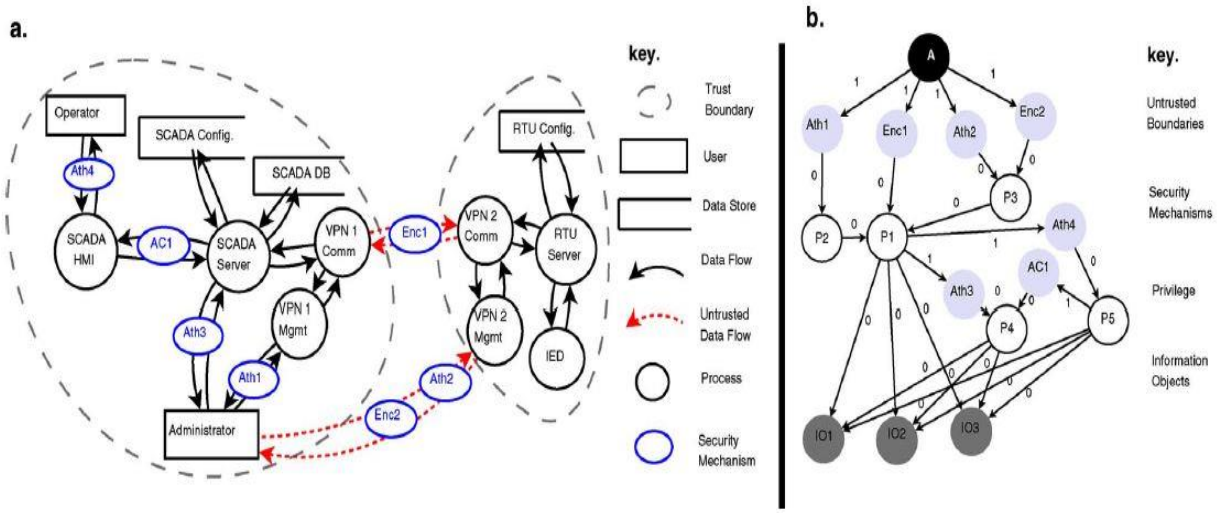
SCADA server, which remotely monitors and controls substation. The second trust zone contains Remote Terminal Unit (RTU), which aggregates data from an Intelligent Electronic Device (IED). Functions of IDE are sensing and actuating. Data flows between those two zones, which considered of being untrusted due to their openness to external access and positioning.

The only necessary data flows for controlling IED are

Control Center ⟷ *RTU* ⟷ *IED*.

For the protection of this environment from cyber attacks, respectful SMs must be provided. Particular attention should be paid to untrusted segments.

When all DFDs are defined, the exposure graph is going to be drawn. This graph formalizes the relationship between SMs, Privileges, and IOs within a system. Node A, representing potential attacker's access, should be connected to all of IO's. Untrusted users should not be able to access IO's without first bypassing some SM's. All edges from A go to correspondent SMs and edge weight of *1* is applied emphasizing an effort of bypassing it. Every SM is connected to set of P nodes identifying privileges obtained in case the corresponding SM failure. The last step is creation an IO set. Every IO node is connected to set of nodes *P* by directed edges with the weight of *0*. Hahn et al. (2011) provide the example of building an exposure graph as in Figure 2.5. What can be observed is that obtaining a privilege *P3* or *P2* leads to gaining privilege *P1* and control over every IO in the system.



Source: (Hahn & Govindarasu, 2011)

Figure 2.5: Exposure graph.

a) DFD flows

b) Resulting graph

After executing calculations, the value of exposure metric is *exp = 4*, since there are only four potential paths. In this case, each of them has a total weight of *1.*
It is easily seen in the figure, that one of the resulting paths is
A->Ath1->P2->P1->all IOs.
Longer paths are considered not to be relevant.

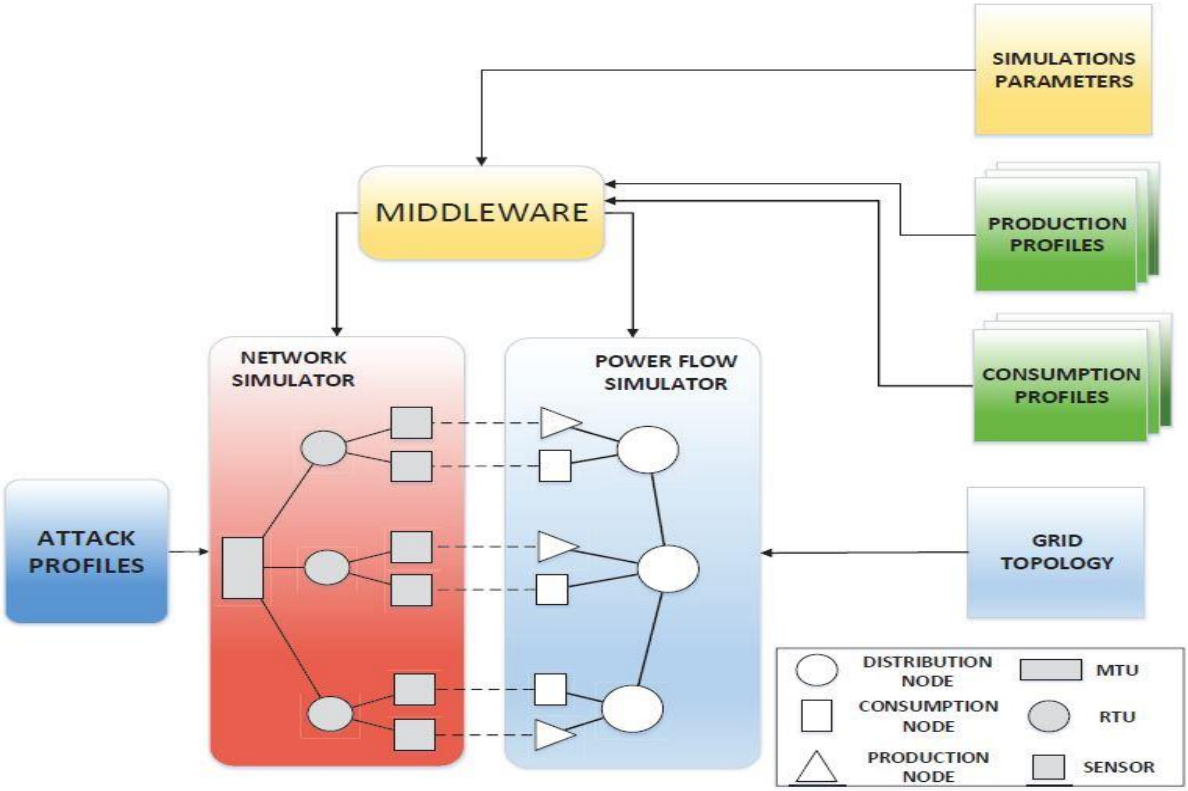
The given approach allows figuring out the paths an attacker might take to reach valuable assets in SG. Another option is that it might help considering other different situations. For example, how a vulnerability of an IO would be affected by compromising one or several SM's.

One of the possible benefits in this framework is that it is not limited to evaluation only SG architecture. Proposed exposure metric *exp* and potential attack vectors give an informative general picture of vulnerabilities in the system. Moreover, it might be useful for preliminary evaluation of an attack surface in an engineered system at an early stage. From the other side, an attacker is assumed to be an outsider, and proper attention is not paid to the presence of disgruntled employees. Choice of

assessing *0* or *1* binary value for edge weight is too coarse. In the real system, the complexity of compromising different SMs might varies drastically, what in turn might lead to wrong evaluation of total system security level. The overlooked fact is that the longer path, regarding number SMs, might have the overall complexity of compromising lower, than the shorter path with greater complexity.

Software for attack simulation in Smart Grid

The more detailed approach presented in the research "ASTORIA: A Framework for Attack Simulation and Evaluation in Smart Grids." This work concerns with building software based system which imitates SG architecture (Wermann et al., 2016). The software system called Attack Simulation Toolset for Smart Grid Infrastructure (ASTORIA) and is built to support simulation of generation, transmission and distribution domains. It supports integrating of consumption units and communication network of SG as well. Different kind of attacks allowed to be simulated thanks to a vast and extensible library of attacks. Wermann et al. (2016) illustrate all of the mentioned building blocks as in Figure 2.6.



Source: (Wermann et al., 2016)

Figure 2.6: ASTORIA framework.

Specifications for simulations are provided by *Simulation Parameters*, *Grid Topology*, *Consumption Profile* and *Production Profile* datasets. An *Attack Profiles* serves for initiating a particular type of attack. For integration all building blocks altogether the *Middleware* layer is deployed.

The research presents results from simulations of two common SCADA cyberattacks, DoS and Software Injection. DoS attack raises an effect of buffer overflow which in turn causes the halt of operations on affected components, in this case, a set of Remote Terminal Units (RTU). Software Injection is malware which intention is to tamper legal data by exchanging these into falsified measurements to cause a financial loss on SG operator.

This approach does not define certain metrics for security evaluation. It draws the picture of system vulnerabilities by presenting sampled data. In author's testbed, the

count of halted RTUs and harsh changes in real power consumption are given. Furthermore, the proposed framework contributes in analyzing and evaluation of the impact of malicious attacks thanks to its reach and extensible database.

Attack graph deployment

Another research, "Towards Measuring Network Security Using Attack Graphs," introduces slightly different approach, comparing to Hahn et al.(2011), of graph composition (Wang, Singhal, & Jajodia, 2007). The graph contains nodes corresponding to two host states, before and after an exploit has been successfully executed. Exploits are defined as various means, which allow exploitation of the vulnerability. Graph edges are reflecting an exploit execution.

As it is seen on Figure 2.7, hosts *1* and *2* are placed behind different firewalls. To access host *3*, what can be a server with valuable resources, an attacker has to go through hosts *1* and *2*. By executing exploits, he gains stepwise access to each of hosts. Virtual link reflects accumulated knowledge, tools or experience, an attacker obtained during an attack execution at some stage and what might assist him at next stage.

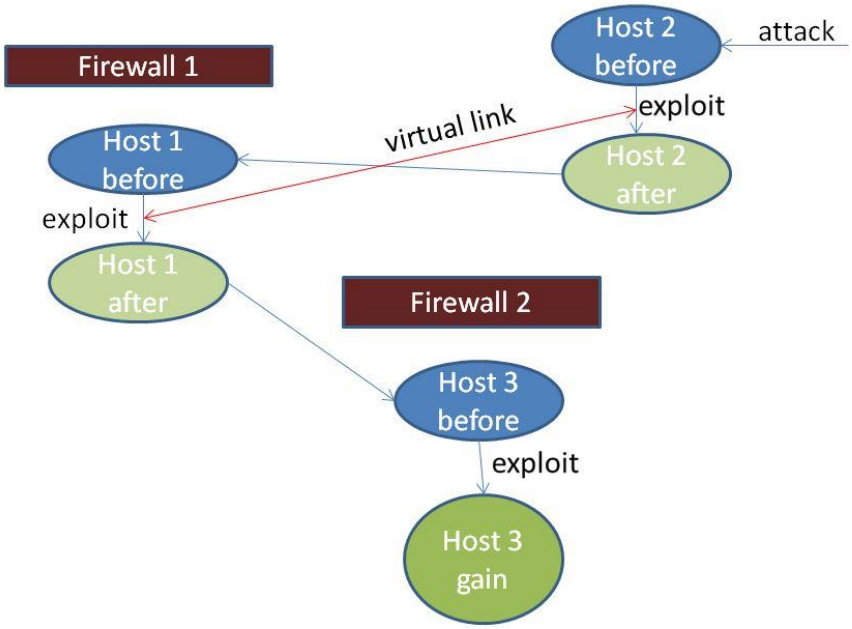


Figure 2.7: Attack graph with elements of network configurations.

Metrics in this framework expressed as *time complexity* and amount of *money*. Former indicates time used for exploit execution. The latter reflects the *significance* of a *resource* or damage induced on the system in case of its loss or expenses of its restoration. Countermeasures of changing network configuration belong to two categories. First one is an *off-line,* with the goal of improving the security of affected network segment. The second type is *on-line*, what expresses a real-time response to the attack.

Figure 2.8 shows a tree-like structure, where metric usage for each case is represented.

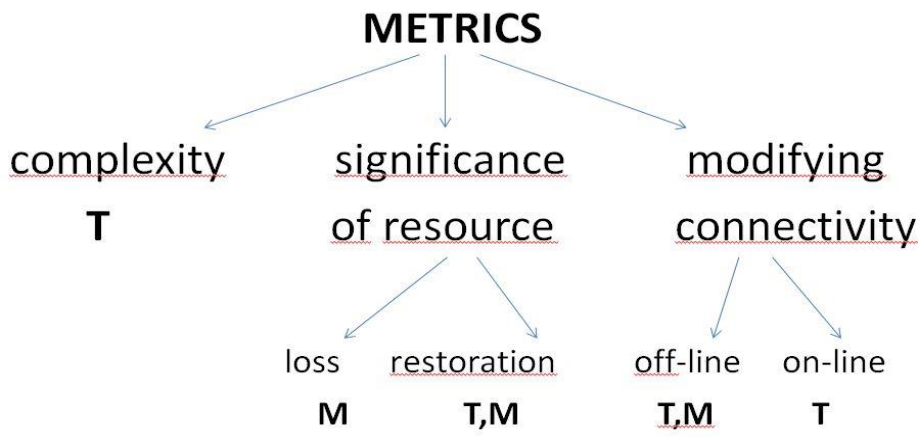


Figure 2.8: Metrics used for evaluation of different damage aspects.

This framework greatly benefits from exploring dependency relationship among vulnerabilities. An option, which makes possible the assessment of metrics on each step along the attack path, brings another advantage. From the other side, neither the method which would guide through accurate, step-by-step process of graph building or the way, how to define all possible vulnerabilities, is given. The researchers let it rely mostly on intuition. This point contrasts with described research of Hahn et al. (2013) on exposure metric evaluation, where data resources, requiring protection, are defined through a particular framework.

Security Matrix for cloud services

Usage of cloud services is becoming more widespread. Those services have security vulnerabilities in common with traditional IT systems, and there are vulnerabilities unique to cloud. Thereby an attack vector surface for cloud services is bringing new concerns. The research "An Innovative Approach to Devise Security Matrix to Measure Impact of Attack Vectors in Cloud Networks" dedicated to the classification of attacks and to working out a methodology to define their impact (Sen, Dey, & Saha, 2014). The authors identified different types of threats, their consequences and investigated all possible circumstances, which might find a place in cloud computing.

The proposed approach based on developing a concept of Security Matrix (SM). This definition includes five different types of matrices. Each of them is used to consider its aspect of an attack surface. Those matrices play a role of intermediaries for further calculations, and are defined as follows:

1. *Asset Matrix* (AM). AM takes into consideration a financial aspect or economic resources. Invested assets values and possible loss due to attack are in focus.
2. *Hazard Matrix* (HM). HM takes to consideration situations that might potentially become to life, health, property and environmental threat.
3. *Vulnerability Matrix* (VM). VM takes to consideration frequency of attacks on the system, presence of Botnets, Service Level Agreements (SLA) failure rate.
4. *Threat Matrix* (TM). TM reflects the speed of response to a threat and time duration of a threat.
5. *Capacity Matrix* (CM). CM takes to consideration number of checkpoints to prevent an attack and number of tenants.

The dimension of all those matrices is varying, keeping the content as simple and practicable as possible. Most of the weighted coefficients, which are representing security metrics, are set in the way, that allows them to be assigned simple boolean or discrete values in a narrow range.

Finally, the resulting *Risk-Matrix* (RM) calculations proposed as following:

$$RM = +/-\{\{ [ALM] * [VM]*[TM]*[HM] \} – [CM] \} .$$

The determinant of this matrix is called a *Risk-factor,* and it expresses an overall influence of an attack vector on a system.

Reviewed research is continued, having an intention in developing decision-making tools. Preceding tools supposed to give the possibility to providers and users obtain an assessment of security level of chosen cloud service quicker and effortless.

Summary for attack centric approach

The three research articles that were evaluated in this section provide the system engineer with an option of considering the ability of an attacker to compromise the system. Another aspect lies in the possibility of potential damage severity evaluation. An engineer can reconfigure the system and go through evaluation again and again in an iterative way. That would assist in eventually arriving at a state where the achieved system satisfies the desired requirements.

2.2.2 System centric approach

Ideal based metrics

The research “Ideal Based Cyber Security Technical Metrics for Control Systems” has developed the model, aimed to assess security level for systems of critical infrastructure. The definition of a critical infrastructure is used for systems in which damages can cause, in the worst case, loss of life (Boyer & McQueen, 2007). Examples of those kinds of infrastructures might be oil- and gas refineries, rail- and air traffic control systems, power plants. Such systems are highly dependent on cyber control systems, where flawless functioning and deep knowledge of performance regarding cyber security, is of high importance.

Development of the framework is proceeded through following stages. First, the researchers, having a base from their previous studies and experience in cyber security field, define a security dimensions set, as follows:

- Security Group (SG) knowledge
- Attack Group (AG) knowledge

- Access points to system under evaluation
- Vulnerabilities
- Damage potential
- Detection
- Recovery

Second, each dimension is associated with an ideal system condition at a given time. The main point of this stage is to make these 'ideals' to be consistent with security objectives. The third stage is an identification of metrics for every dimension. Boyer et al. (2007) show the final result of this proceeding or summoning of established metrics reviewed in Table 2.3 below.

Table 2. 3: Proposed metrics and respectful units of measure.

Security Ideal	Metric	Unit
1.SG knows current system perfectly	Rogue change days --- Component test count	any time unit --- # components not went through security testing Not fully developed
2. AG knows nothing about system	Minimum password strength --- Data transmission exposure	time to crack, any time unit --- Unencrypted data transmission volume, byte
3. System is inaccessible to AG's	Reachability count --- Root privilege count --- Defense depth	# access points --- # user ID's with root privilege --- # compromises required to successful attack fulfilling
4. System has no vulnerabilities	Vulnerability exposure --- Attack surface	time to patch, cumulative --- Not yet developed
5. System cannot be damaged	Worst case loss	amount of money
6. SG detects any compromise instantly	Detection mechanism deficiency count --- Detection performance	# externally device without malware/attack detection mech. --- rate of probability of attack detection to false positives Not fully developed
7. SG can restore system integrity instantly	Restoration time	Time of recovering the system, any time unit

Source: (Boyer & McQueen, 2007)

When calculating metrics, attention should be paid to which of them are applicable for given system. Special data structure might be used for summoning calculated metrics along with ideal metrics and suggested values for metrics, allowing comparisons. Boyer et al. (2007) illustrate an example of one metric representation reviewed in Table 2.4. In this table, “Suggested target value” column indicates the value, a metric might obtain, after performing suggested measures of security improvements.

Table 2.4: Possible outcome.

Metric Name	Metric Value	Ideal Value	Suggested target value
Min password strength	> 10 days	infinity	> 15 days

Source: (Boyer & McQueen, 2007)

Particular attention should an when suggesting improvements for certain metric, meaning that change in one metric value may influence change in some other metric's value. Overall evaluation of metrics, obtained after measurements and calculations, draws preliminary knowledge of security performance for that system.
An advantage of proposed framework is that number of security dimensions might be expanded in accordance with size or importance of a system under evaluation. In consideration of proposed security ideals set, it might be seen, that there is a strong dependency on knowledge of security group. This fact indicates that tight coupling inside of this framework exists. As a consequence, such coupling could be a decisive factor in regards to a practical use case.

Network metrics

Overall secure construction of a system consists of many building blocks, and that is why it is important to consider each of them regarding security level. One of them includes secure communication protocols. The research “Network Security Metrics and Performance for Healthcare Systems Management” envisages implementation of a protocol for network communications, namely Internet Protocol Security (IPSec) (Liu, Tesfamicael, Caelli, Sahama, & Ieee, 2015).

Details of an influence of VPN topology on delivering time of an IP packet and difference in processing time of an IP packet due to the usage of different HW base were in focus. The topologies for evaluation case are shown in Figure 2.9.

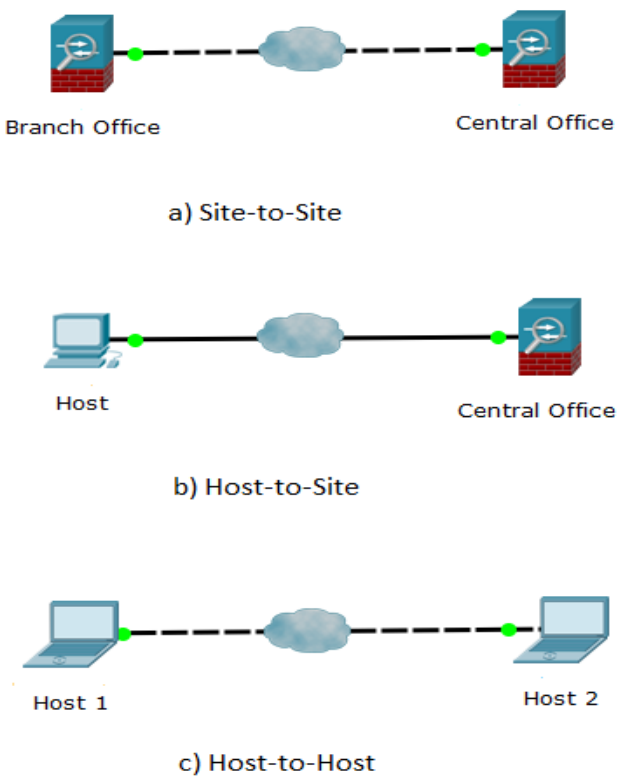


Figure 2.9: Different IPSec VPN topologies

IPSec has been designed to maintain following security objectives: confidentiality, source authentication, data integrity, and anti-replay. For providing them, AES encryption of different key length and hash algorithms of different length were

considered. After conducting simulations, results of using those security mechanisms have been compared. A security metrics set, evaluating security levels such as "High," "Medium" and "Low" was proposed.

Liu et al. (2015) show comparisons reviewed in Table 2.5.

Table 2.5: Metrics and security mechanisms used in simulations.

	SECURITY LEVEL		
METRICS	High security	Medium security	Low security
Confidentiality	AES-256	AES-192	AES-128
Integrity	SHA512	SHA384	SHA256
Delivery	Low priority	Medium priority	High priority
Best practice	AES-128/SHA256	AES-192/SHA384	AES-128/SHA512

Source: (Liu et al., 2015)

While considering experiments, it is noted that ESP protocol was utilized for both Transport and Tunnel modes. The manageability of abovementioned three types of VPN topologies, Liu et al. (2015) summarize the results reviewed in Table 2.6.

Table 2.6: VPN topologies and modes.

Communication Type	Operation Mode	Advantage	Disadvantage
Host-to-Host	Transport	End-to-end security	Low throughput Low manageability
Host-to-Site	Tunnel	Medium throughput Medium manageability	Protection between Tunnel endpoints
Site-to-Site	Tunnel	High throughput High manageability	Protection between Tunnel endpoints

Source: (Liu et al., 2015)

The granularity of established metrics as high, medium and low is notable coarse-grained. In the same time, a real system, which security level is going to be assessed using this framework, might use encryption-hash pairs out of broader variety choice. It might follow in greater deviation in the security assessment. Additionally, the simulation results could be affected by used HW base and OS choice. From the other side, given calculations might assist in making improvements while in system's design process, used as the guideline in choosing security algorithms and IPSec modes.

Risk-based metrics

An approach of combining system- and attack-centric approaches, is proposed by research “Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design” (Vasilevskaya & Nadjm-Tehrani, 2015). Security evaluations of two objectives like confidentiality and integrity of data assets in the context of a given design model for an embedded system are introduced. In this work, attack and system design are treated as two distinct and in the same time correlated elements to achieve a correct elaboration.

There were developed two probabilistic risk metrics. The first one, *Confidentiality Loss* (CL), estimated as a product of the likelihood of an attack that would reveal valuable asset during the time T, and damage, it inflicts on stakeholder R:

$$CL = Prob(T) \times Damage(R) ,$$

By stakeholders are denoted all the entities involved in interactions inside of a system, as e.g. a house owner, a smart meter provider, the National regulatory agency in SG infrastructure. Definition of *Risk* includes the likelihood of a successful attack and the severity of its consequences.

On the other side, the second risk metric is *Integrity Loss* (IL), which reflects the level of damage from an attack during the time T to a data asset in case of integrity breach:

$$IL = Prob(T) \times Damage(Data)$$

For both definitions, the special attention is paid to the fact that probability of a successful attack might change as time progresses. Furthermore, that system may possess different valuable data assets during an attack execution.
A fundamental distinction in metrics definitions lies in affected entities, in the first case, those are stakeholders and in the second case, data assets.

A proposal for necessary likelihood distributions is that they may be obtained in two ways:

a) based on historical or empirical data,
b) based on expert opinion.

Damages are expressed using a common linguistic scale (Lund, Solhaug, & Stølen, 2010). Vasilevskaya et al. (2015) illustrate this proposal for particular SG user case reviewed in Table 2.7. Damages are enumerated as follows:

{ *insignificant, minor, moderate, major, catastrophic* ***}*** ,

Table 2.7: Proposed scaling of damages.

	User	Utility provider	National regulatory agency
Confidentiality	Major	Minor	Insignificant
Integrity	Moderate	Major	Minor

Source: (Vasilevskaya & Nadjm-Tehrani, 2015)

As it might be noticed, those likelihood distribution estimations are in high grade subjective in both cases, regarding stakeholders and data assets.
Figure 2.10 illustrates an example of implementing discussed approach in the light of system improvement for certain set of attacks for proposed participators presented in Table 2.7.

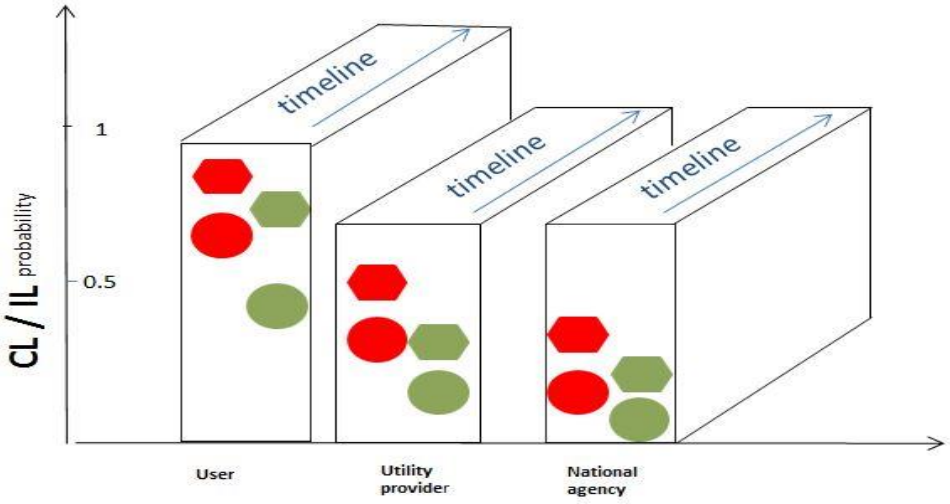


Figure 2.10: Formal metrics approach. CL(rhomb) and IL(circle) - metrics. Red - initial design, green - after improvements applied

System's security assessment using this framework is benefiting from possibility to show different risks to assets of a metering device, which is part of the more global system. Undoubtedly, consideration of the timing aspects gives a great contribution in overall security level measurements. However, those considerations relying in high grade on continuing and future research what might limit the opportunity of their deploying.

Deployment of Mobile Cellular Network router for IoT

Wide deployment of Wireless Sensor Networks in IoT should be supported by smooth and secure communications with the rest of the world. Transactions between WSNs and other participators of a global infrastructure they belong to, often happen via a mobile cellular network. The research "A Risk-Driven Security Analysis and Metrics Development for WSN-MCN Router" analyses security aspects in the usage of such route (Frantti, Hietalahti, & Savola, 2013).

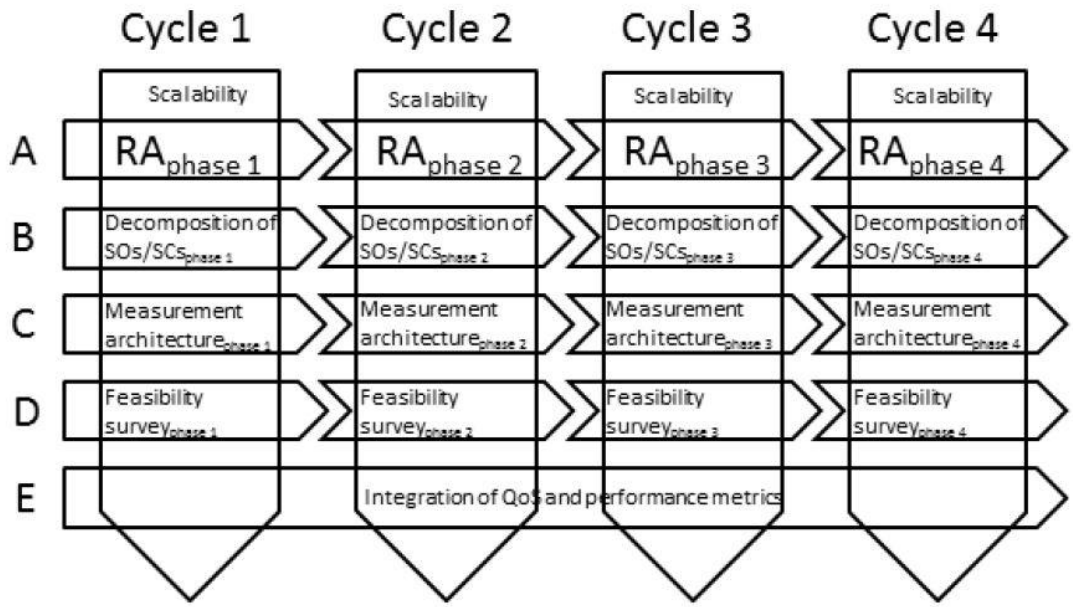
Firstly, the work states functionalities of Mobile Cellular Network (MCN) router, secondly it identifies the risks related to usage WSN networks as part of IoT infrastructure. Then the work offers an informative overview of security objectives and corresponding security controls or mechanisms related to WSN-MCN router. A treelike structure example, showing the process of developing connections between

risk, security objectives it might affect, and security controls is presented. Building a tree starts from the root, which represents a certain risk, down to security objectives and controls. Hence, the security analysis, done by researchers is considered to be risk-driven.

The work itself does not define particular metrics; it rather proposes building blocks for security metrics development and management process.

Frantti et al. (2013) illustrate the main stages of this process as shown in Figure 2.11.

.



Source: (Frantti et al., 2013)

Figure 2.11: Metrics development and management process for IoT device.

The process is iterative, repeated in a certain number of iterations or cycles meaning that on each cycle some security gaps and biases would be revealed. The next cycle is supposed to deal with their covering. Each cycle composed of following activities:

- Activity A: Risk Analysis (RA) and Security Objective/Security Control Analysis
- Activity B: Security Objective Decomposition
- Activity C: Measurement architecture. Supports automated or manual

measurement methods, and includes solutions for non-technical evidence gathering

- Activity D: Feasibility Analysis, which is supposed to find answers about trustworthiness and reasonability of security metrics
- Activity E: Integration of other metrics. Takes into account the usage of non-security metrics with security relevance

The number of cycles connected to following phases:

1) definition of product usage scenarios and use cases,
2) definition of product functional requirements, device and network interfaces,
3) design and specification of the product,
4) verification of the product.

The research provides clear and steady steps for analyzing system under investigation. It highlights common aspects and leads to requirements for the security metrics development process. Unfortunately, the scope of this work is limited and does not present complete metrics models or processes.

Summary for system-centric approach

Articles that were criticized in this section provide an example of the system-centric approach of evaluating security level for the system under investigation. Positive considerations were paid to such qualities as a possibility of adding or removing building blocks inside of a framework in accordance with system's size, importance, and usage scenario.

The MM approach, which is subject to considerations in this thesis, belongs to the family of system-centric approaches.

2.2.3 Summary

The research studies reviewed in this section indicated that there is no general framework allowing measurement of the security level of a system in a standard way.

Conversely, there exist many different methodologies and approaches for doing this. Although these studies showed useful methods for measuring security level, almost all of them depend on the participation of an expert in a given field. That may be a serious drawback because the expert's knowledge may not to be highly accurate, due to the subjective nature of those evaluations. Nonetheless, an advantage of discovering weaknesses in the system during the design stage by discussed methodologies should be underlined as being crucial. From economical and technical perspectives, it is reasonable to embed security in a system while in the development stage, rather than make changes during its life cycle.

3 Method

There are different methodologies and approaches for assessment of the SPD level of given system.

An important task of developing SPD system level assessment methods is finding the ways of doing these assessments which will be beneficial for system engineers and consumers of IT systems. The system's engineers might find use of those methods profitable in the designing and verifying stages of constructing a system. The consumers might benefit from it when making a choice between market proposals.

One part of Smart Grid is Advanced Metering Infrastructure. Like any other system, it contains parts that have vulnerabilities which can be used by the malicious party, thus there is a need to explore these vulnerabilities and to evaluate the security level of an AMI.

The purpose of using the MM approach as tool for measuring security level of a system is that the MM approach would enhance the security level of the system by increasing the system’s immunity.

3.1 Multi Metrics (MM) approach

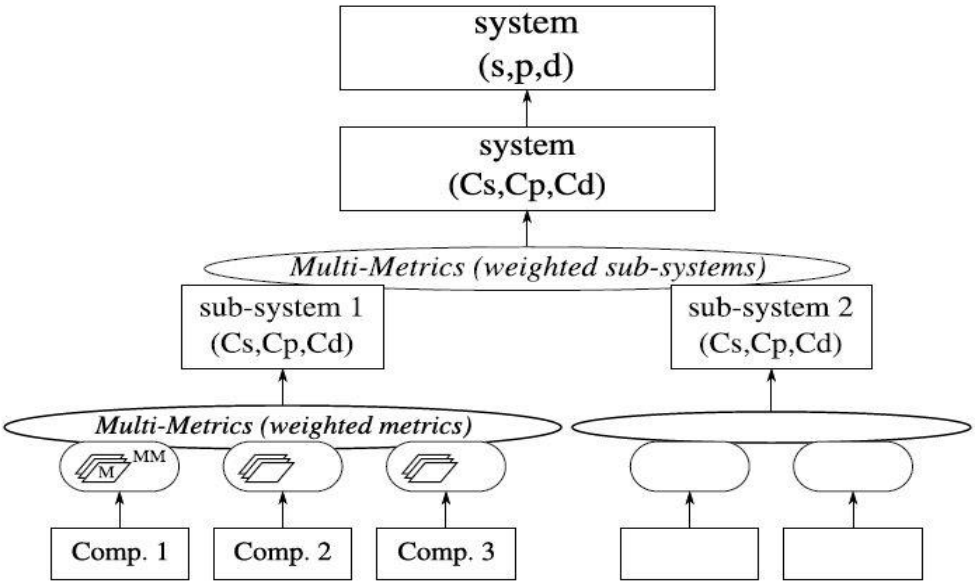
3.1.1 MM approach output

The MM approach is designed to find the Security, Privacy and Dependability (SPD) levels of the System under Investigation (SuI) (Noll et al., 2014). The resulting SPD system level is presented as a vector of three elements (s, p, d) where the elements correspond to Security, Privacy, and Dependability levels of SuI. Each element obtains a value which ranges from 0 to 100. Such a scale is assumed for its convenience due to resemblance to the percentage scale. The 0 value indicates the lowest level of a given element, i.e. the corresponding element is not present for the SuI. The highest value of 100 indicates that the corresponding element of the SuI is

on the top level, which might be achieved only theoretically. The final result would look like:

SPD system = (evaluation for Security, evaluation for Privacy, evaluation for Dependability).

This final triplet value emerges from evaluations of sub-values for SPD for every building block a system consists of. The structure, illustrating a sequence of evaluations proposed by Noll et al. (2014) is shown in Figure 3.1.



Source: (Noll et al., 2014)

Figure 3.1: Multi Metrics approach tree-like structure.
***M* indicates Metrics analysis.**

As shown in the figure, a system is composed of multiple subsystems which at the same time consist of various components.

Note: Cs, Cp, and Cd are acronyms for Criticality for Security, Criticality for Privacy and Criticality for Dependability. The abbreviation of CsCpCd is used interchangeably with the term *SPD criticality* for simplicity throughout this thesis.

An introduction to term *Criticality*

The MM approach introduces the term Criticality, which is used during the whole process as the main evaluation component (Noll et al., 2014). The definition of criticality is how critical the expert/evaluator sees the entity's capacity to continue working as it was intended to work. Such an approach is more convenient for most of the individuals. When speaking about criticality for security, the goal is to evaluate how vulnerable the entity is. The desired security level is defined as the complement of criticality as shown in Figure 3.2 below.

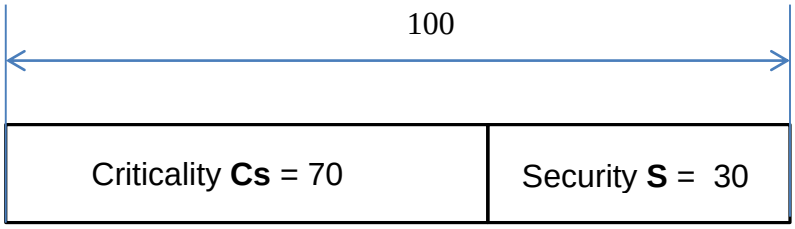


Figure 3.2: Relationship between criticality and security

This figure shows the relationship between criticality for security or **Cs** and security or **S**. These abbreviations are used throughout this thesis.

3.1.2 Involved participants

Each complex system consists of many subsystems. In turn, each subsystem may contain different components. The system might be used in various scenarios. The given usage scenario can imply different interactions of subsystems and their components involved to provide functionality for this scenario as shown in Figure 3.3.

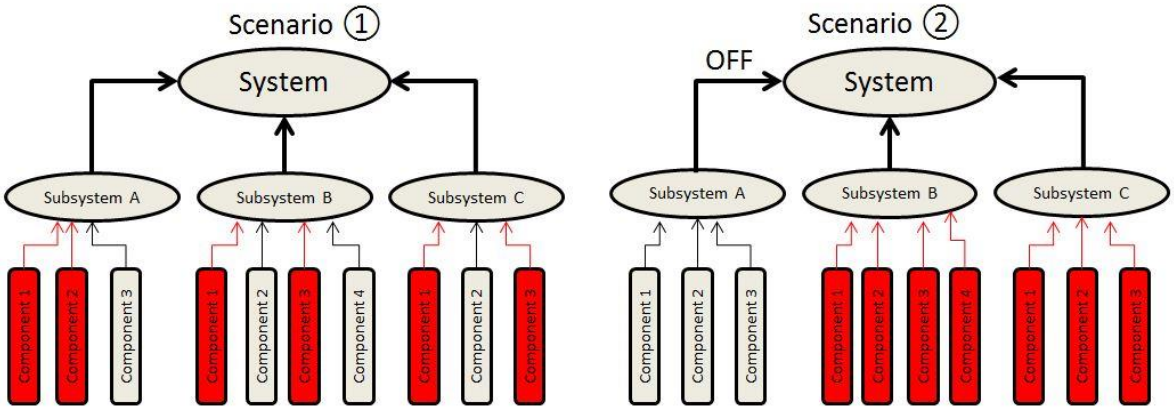


Figure 3.3: Two usage scenarios, components involved in red.

As seen in the figure, the composition of subsystems and components could differ from one scenario to another.

Performing MM approach on System under Investigation

3.1.3 Stage 1, establishing of SPD goal

For every scenario, there will be set SPD requirements or an ***SPD goal***. The number of SPD goals is going to be equal the number of scenarios. In every scenario the system can be configured differently, thus resulting in its SPD level for every configuration under given scenario. In an MM approach, all possible configurations for every scenario are evaluated and results are compared against the established SPD goal for the respective scenario. Such comparison assists in recognizing the most suitable configuration (Noll et al., 2014).

3.1.4 Stage 2, Identification of subsystems

At this stage, all subsystems providing functionalities for the whole system should be identified as shown in Figure 3.4.

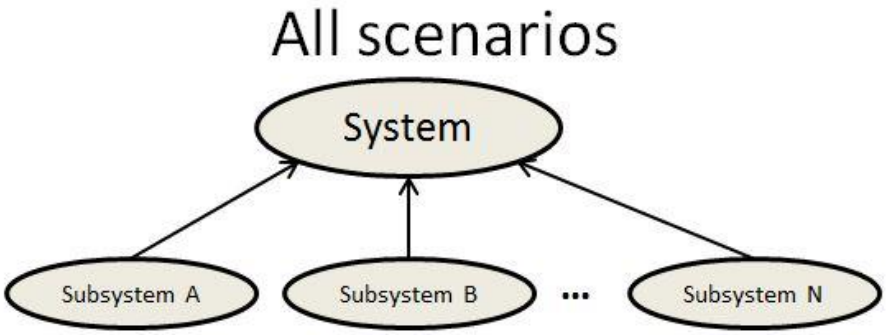


Figure 3. 4: System and its subsystems.

The identification of subsystems is performed by an expert in the field.

3.1.5 Stage 3, Identification of components

At this stage, in turn, for each subsystem, there should be components it consists of, identified as shown in Figure 3.5.

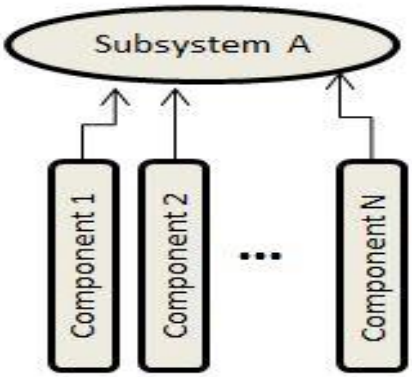


Figure 3. 5: Components of subsystem.

The identification of subsystems is performed by an expert in the field.

3.1.6 Stage 4, Identification of metrics

This stage has two sub-stages: *a)* Identification of a metric and *b)* Identification of a Parameter.

Introduction to term *Metric*

The metrics are objects or entities used to measure the SPD criticalities of components (Noll et al., 2014).
Thus the core of the discussed approach is a definition of metrics describing the corresponding component. The components and metrics are coupled together as shown in Figure 3.6.

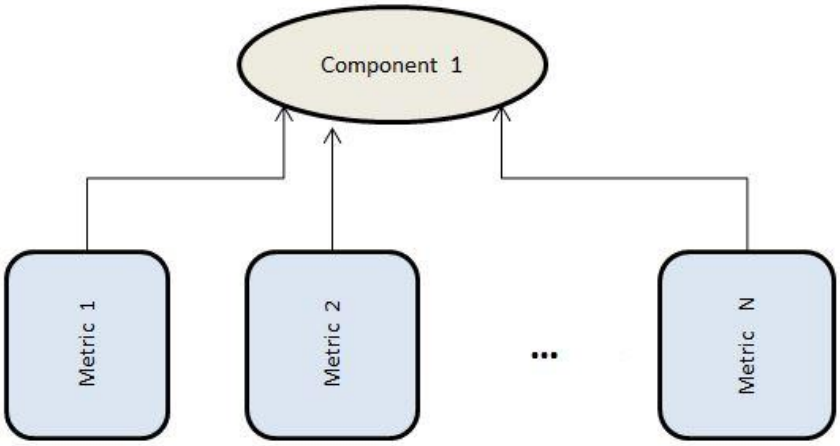


Figure 3.6: Component-metric linking.

a) Identification of metric

At this sub-stage, the set of metrics is identified. The number of metrics ranges from *1* to *N* as shown in the figure above.

The choice of what kind of metrics should be in use for a given component is based on expertise level of a system engineer (Noll et al., 2014).

b) Identification of a Parameter

At this sub-stage, for each metric, a Parameter, based on component purpose and its characteristic, is identified (Noll et al., 2014). Figure 3.7 shows the relationship between a metric and its Parameter.

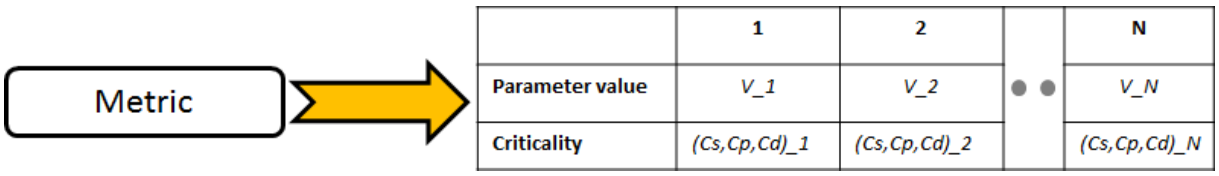


Figure 3.7: Metric and Parameter relationship.

The Parameter takes from *1* up to *N'* values. For each value of the Parameter, the expert in the field evaluates the SPD criticality value.

3.1.7 Stage 5, Identification of weights

Introduction to term *Weight*

For assessment of the role and function which an element might exert on the system, the term *weight* is introduced. The expert in the field defines the significance of an element in the form of establishing a weighting index to it in the range between 0 and 100. The higher is the number, the greater significance this element has (Noll et al., 2014).

Note: the weight will be different for each SPD aspect (Garitano, Fayyad, & Noll, 2015), but because this thesis has a limited scope, only the weight of Security is

taken into consideration. Thus, instead of using three values as Weight for Security, Weight for Privacy and Weight for Dependability only Weight for Security is used throughout this thesis, or weight for short.

Consequently, at this stage, the weighting for metrics, components, and subsystems is performed.

Metric weighting

The weight is defined for each metric of the component. Figure 3.8 shows an example where a set of metrics, parameters, criticalities and weighs are summarized for one component.

Component #													
	Metric 1				Metric 2					Metric K			
Parameter value	1	2	● ● ●	N	1	2	● ● ●	M	● ●	1	2	● ●	K'
Criticality (Cs,Cp,Cd)	#,#,#	#,#,#		#,#,#	#,#,#	#,#,#		#,#,#		#,#,#	#,#,#		#,#,#
Weight	w_3				w_2					w_K			

Figure 3.8: Set of metrics, parameters, and weights for one component.

Component weighting

The weight is defined for each component in every subsystem. Figure 3.9 shows an example where the components and their weights for one subsystem are summarized. The components deployed in the scenario are shown in red.

Scenario 1				
	Subsystem 1			
Component	1	2	3	4
Weight	w_1	w_2	w_3	w_4

Figure 3. 9: Components and weights for subsystem. Components participating in scenario in red.

Weight assessment is based on expertise.

Subsystem weighting

The weight is defined for each subsystem. Figure 3.10 shows an example where subsystems and their weights are summarized. The subsystems deployed in the scenario are shown in red.

Scenario 1					
Subsystem	1	2	3	4	5
Weight	w_1	w_2	w_3	w_4	w_5

Figure 3.10: Subsystems and weights. Subsystems participating in scenario in red

Weights assessment is based on expertise.

3.1.8 Stage 6, Calculation of the SPD criticality

Reason for having multiple Configurations

Before proceeding to the main part of stage 6, there is a need to describe the configuration of the system. The system is deployed in different scenarios.

In this particular scenario, only those subsystems are taking part which guarantee operability in this scenario.
For each subsystem involved in this particular scenario, all or a set of components of the subsystem participate for providing operability.
Further down, the component is configured in a specific way. The possible configurations for a component might have multiple forms as shown in Figure 3.11.

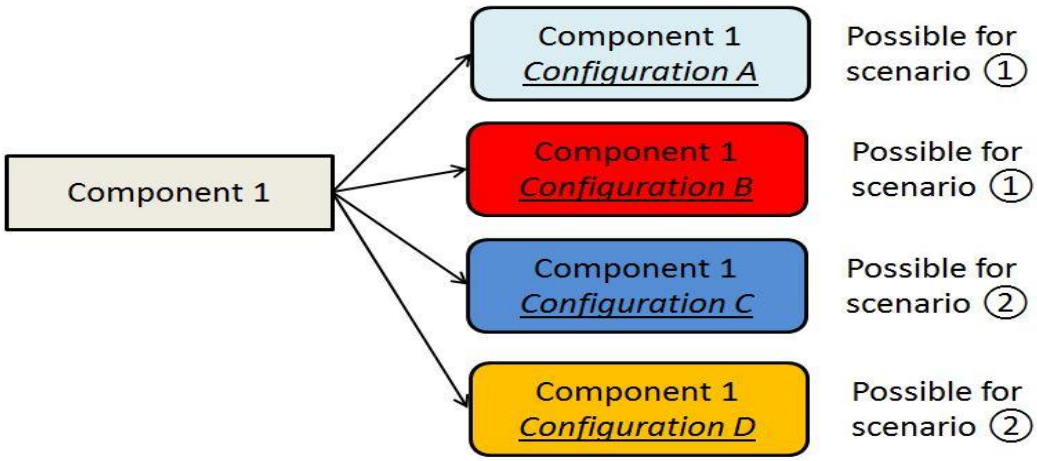
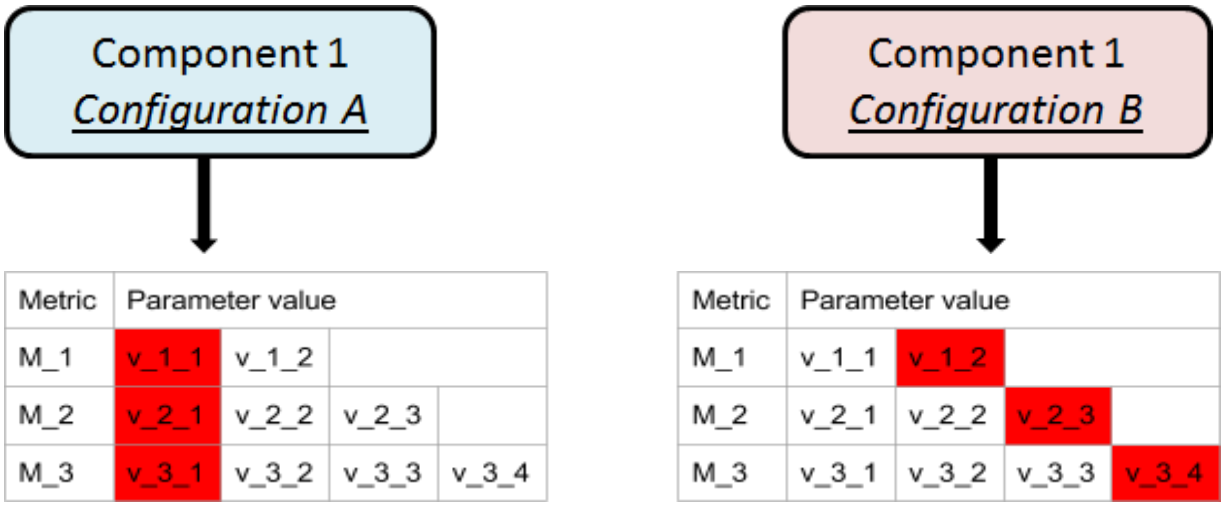


Figure 3.11: Multiple configurations of component.

Each configuration is defined by a set of Parameter values, chosen for a single configuration. The reason for having multiple configurations is that the various Parameter values can be chosen for the same scenario as shown in Figure 3.12.



Metric	Parameter value			
M_1	v_1_1	v_1_2		
M_2	v_2_1	v_2_2	v_2_3	
M_3	v_3_1	v_3_2	v_3_3	v_3_4

Metric	Parameter value			
M_1	v_1_1	v_1_2		
M_2	v_2_1	v_2_2	v_2_3	
M_3	v_3_1	v_3_2	v_3_3	v_3_4

Figure 3.12: Possible configurations of component.
Parameters for running configuration in red.

Regarding the configuration example above, there exist *24* possible configurations for this component.
Thus, the broad choice for the configurations of a component yields a broad choice for the overall system's configuration.

Calculations of the SPD system

The final result is obtained by converting criticality triplet CsCpCd into the SPD system by using the formula:

$$SPD_{system} = (100,100,100) - (Cs, Cp, Cd) \quad , \qquad (1) \quad \text{(Noll et al., 2014).}$$

The system's criticality (Cs, Cp, Cd) triplet is obtained from a sequence of calculations of criticalities, starting at the lowest level in the following steps:

- ❑ Component criticality - for a particular configuration.
- ❑ Subsystem criticality - including every component involved in the scenario.
- ❑ System criticality - including every subsystem involved in the scenario.

Formula

General *Root Mean Square Weighted Data* (RMSWD) formula for criticality calculation is:

$$C = \sqrt{\sum_i \frac{c_i^2 * W_i}{\sum_i^n W_i}} \quad (2)$$ (Noll et al., 2014),

where c_i is criticality value and W_i is *modified* weighting index of the corresponding element *i* . The modified weighting index is calculated as

$$W_i = \left(\frac{w_i}{100}\right)^2 \quad (3)$$ (Noll et al., 2014) ,

where w_i is weighting index of the corresponding element *i*.
A sensitivity analysis has shown that a linear significance level of the weight is not appropriate to end up with representative SPD levels. Thus modified weight will maximize the impact of high weight values towards the lowest ones (Noll et al., 2014).

Role of weighting index in RMSWD formula

The expression under the root in formula *(2)* might be seen as sum of squares of criticalities multiplied by the coefficient k_i , as

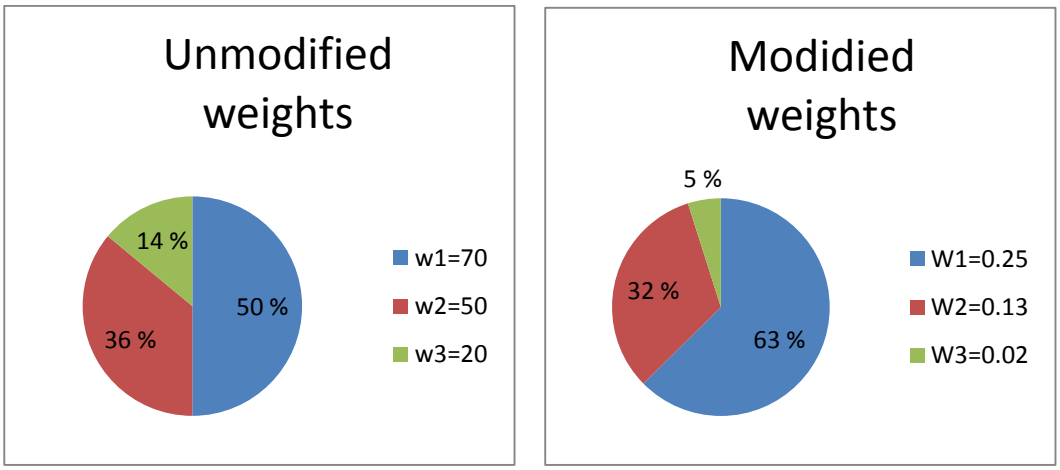
$\sum_i \frac{c_{i*}^2 W_i}{\sum_i^n W_i} = c_1^2 * k1 + c_2^2 * k2 + \ldots$, where the coefficient

$$k_i = \frac{W_i}{\sum_i^n W_i}$$ and

$$\sum k_i = 1 .$$

Thus, the coefficient k_i is used to normalize the contribution of every criticality value.

The following simple example shows the differences between weighting index and *modified* weighting index. In the case that there are only three weighting indices: w1 = 70, w2 = 50, w3 = 20, the coefficients are calculated for unmodified and modified weights, as shown in Figure 3.13 below.



a) b)

Figure 3.13: Difference between *a)* unmodified and *b)* modified weights.

This figure shows that *w1=17* has 50% share, but after modifying its share, it increases up to 63%. On the other hand, *w2=20* has 14% share, but after modifying its share, it decreases down to 5%.

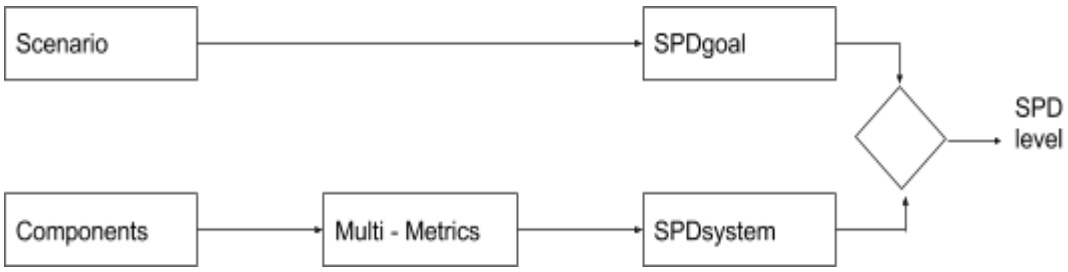
Summarization of steps for stage 6

1. Choice of parameters for metrics which would yield a particular configuration
2. Applying RMSWD calculations on the components in the chosen configuration
3. Applying RMSWD calculations on the components within each subsystem
4. Applying RMSWD calculations on the subsystems within a system
5. Applying formula *(1)* for converting the SPD criticality into the SPD system.

Note: Criticality values for each aspect in a CsCpCd triplet are obtained by executing calculations for each aspect separately.

3.1.9 Stage 7, Comparison with SPD goal

The final step in the MM approach is the comparison of the obtained SPD system values with SPD goal values for every scenario, which ends up in the SPD level as shown in Figure 3.14. Such comparison would show how close the level achieved is to the requested level.



Source: (Noll et al., 2014)

Figure 3. 14: Comparison of SPD goal vs. SPD system.

This step is executed by using a visual presentation which considerably simplifies the process of comparing the SPD system with the SPD goal for a given scenario. For fulfilling this comparison, every element in a triplet of SPD level is substituted with a green, yellow or red circle by using following criteria:

- | SPD goal – SPD system | = < 10, green
- | SPD goal – SPD system | > 10 <= 20, yellow
- | SPD goal – SPD system | > 20 red

  (Garitano et al., 2015)

Note: The MM approach penalizes if the obtained value of the SPD system exceeds the value of the SPD goal. The reason for this, regarding security, is that exceeding

the required security level leads to unnecessary complexity, and a possible increase in CPU and battery power usage, which is imperative for an embedded system. It might reduce the security capabilities of a system in the long run as well, due to the impossibility of increasing the security level in the case that some of the underlying subsystems were to fail.

Note: The MM approach does not require execution of stages in sequence, as given in this section (Method). A researcher, who uses the MM approach, has the possibility to choose what sequence of stages is more convenient to him.

3.1.10 Illustration of criticality calculations

An example of criticality calculation for a component under a particular configuration

An example, showing the choice of elements for criticality calculation for some *Configuration A* is shown in Figure 3.15. In this example, for simplicity, only a limited set of parameters and metrics is taken into consideration for a *Component 1*.

Scenario 1							
Configuration **A**							
	Component 1						
	Metric 1			Metric 2		Metric 3	
Parameter value	v_1_1	v_1_2	v_1_3	v_2_1	v_2_2	v_3_1	v_3_2
Criticality Cs,Cp,Cd	c_1_1	c_1_2	c_1_3	c_2_1	c_2_2	c_3_1	c_3_2
Weight	w_1			w_2		w_3	

Figure 3.15: Set of metrics and weights for Configuration A. Elements chosen for this configuration in red.

The use of formula (*2)* for criticality calculation for *Component 1, Configuration A* is:

$$C_{conf.A} = \sqrt{\frac{c_{1_1}^2 * W_1 + c_{22}^2 * W_2 + c_{32}^2 * W_3}{W_1 + W_2 + W_3}}.$$

The values for W_1, W_2, and W_3 are obtained from weight values *w_1, w_2* and *w_3* using formula (*3*) first.

Calculations of criticalities for Security, Privacy, and Dependability, are conducted separately.

Consequently, every component in every subsystem gets assigned a criticality value for each aspect in SPD triplet.

Subsystem criticality calculation

For calculating the SPD criticality for *Subsystem,* the formula (2) is used.

The values for SPD criticality for components are obtained in the previous step and *w_comp* is the weight of the corresponding component, shown in Figure 3.16. In this example, a subsystem consists of three components.

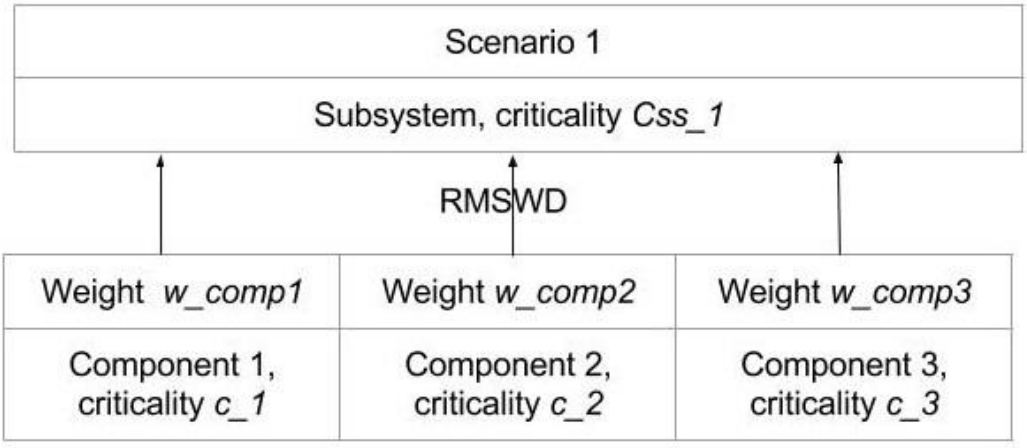


Figure 3.16: Subsystems criticality calculation.

Final result for subsystem's criticality is:

$$C_{Subsystem1} = \sqrt{\frac{C_{c\_1}^2 * W_{w_{comp1}} + C_{c_2}^2 * W_{w_{comp2}} + C_{c_3}^2 * W_{comp3}}{W_{comp1} + W_{comp2} + W_{comp3}}}$$

The values for W_{w_comp1}, W_{w_comp2} and W_{w_comp3} are obtained from weight values *w_comp1, w_comp2* and *w_comp3* using formula (*3*) first.

Calculations of criticalities for Security, Privacy, and Dependability, are conducted separately.

Consequently, every subsystem gets assigned a criticality value for each aspect in SPD triplet.

System criticality calculation

The calculation of criticality for a system is similar to the previous example. The difference is only in criticalities and weights used at this stage, belonging to subsystems participating in the particular scenario as shown in Figure 3.17. In this example, a system consists of three subsystems.

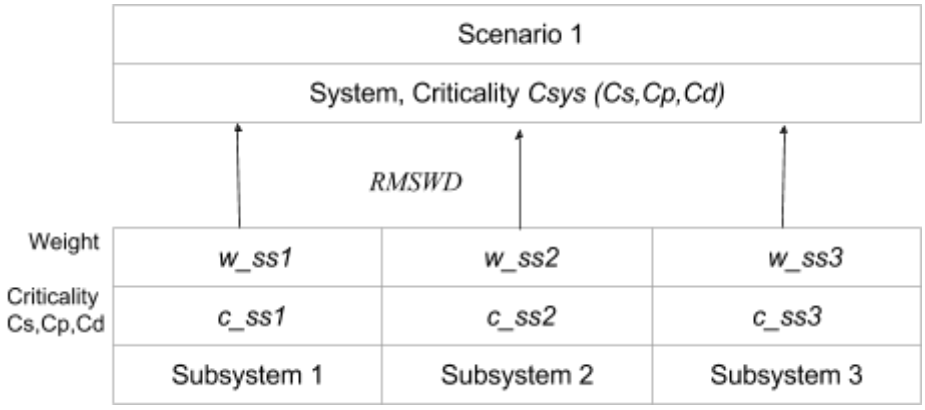


Figure 3.17: Participants in system's criticality calculations.

Final result for system's criticality is calculated by using formula *(1)*:

$$C_{system} = \sqrt{\frac{C_{c\_ss1}^2 * W_{w_{ss1}} + C_{c_{ss2}}^2 * W_{w_{ss2}} + C_{c_{ss3}}^2 * W_{w\_ss3}}{W_{w\_ss1} + W_{w\_ss2} + W_{w\_ss3}}}$$

The values for W_{w_ss1}, W_{w_ss2} and W_{w_ss3} are obtained from weight values *w_ss1, w_ss2* and *w_ss3* using formula (*3*) first.

Calculations of criticalities for Security, Privacy, and Dependability, are conducted separately.

Consequently, the system gets assigned a criticality value for each aspect in SPD triplet.

Note: components and subsystems not participating in this particular scenario are not taken into calculations.

As shown, the resulting SPD criticality for a system depends upon a certain number of metrics and on their weights, hence the name Multi Metrics.

In Table 3.1, the comparison of the SPD system vs. the SPD goal for the definition of the SPD level is shown. All the values are chosen for illustrative purposes.

Table 3.1: Final evaluation of obtained SPD system.

		SPD_{goal}	SPD_{system}	SPD_{level}
Scenario 1	Conf. A	(80,70,90)	(58,72,69)	(🔴 🟢 🔴)
	Conf. B		(67,56,84)	(🟡 🟡 🟢)
	Conf. C		(71,52,68)	(🟢 🟡 🔴)

Source: (Noll et al., 2014)

From obtaining a similar table for an SuI, the system engineer can make a commitment and select the most convenient configuration for a given scenario (Noll et al., 2014).

3.2 Interconnections

3.2.1 Interconnection Consideration and Positioning

Regarding described MM approach, it should be noticed that final SPD triple values in evaluation of the whole system have a relationship between components not only in tree-like structure as in Figure 3.1 but as shown in Figure 3.18; the components belonging to different subsystems might have an influence on each other.

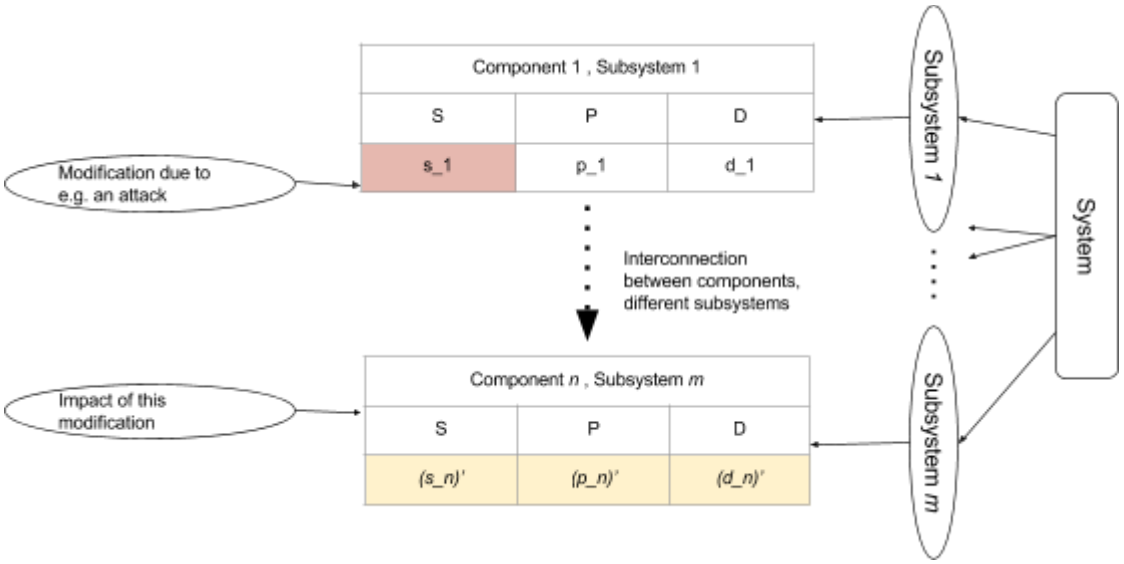
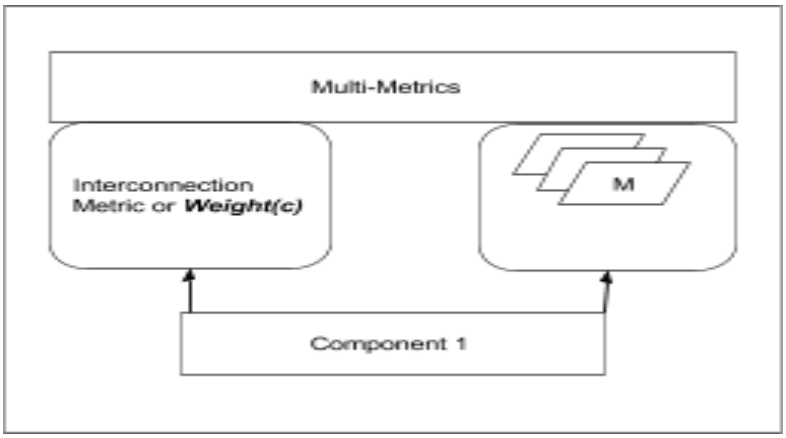


Figure 3.18: Illustration of interconnections.

This phenomenon is called interconnection of components and recognized as a separate interconnection metric additional to an already existing set of metrics of a component. The presence of this metric is going to be the default for every

component. For considering the impact of interconnection on SPD level, this metric is chosen to be the default for every component. As proposed by Fayyad et al. (2015), the Figure 3.19 shows the positioning of interconnection metric as part of the MM approach.



Source: (Fayyad & Noll, 2015)

Figure 3.19: Interconnection metric positioning in MM approach.

As it is seen from this figure, Interconnection metric and Weight(c) are interchangeable definitions. Interconnection metric is positioned at a higher level due to it shows the influence of interconnections on all components and their SPD parameters (Fayyad & Noll, 2015).

3.2.2 Interconnection metric

The system is considered as a set of interconnected components which interact through passing data and control messages. Based on this consideration Fayyad et al. (2015), proposed a definition of an interconnection graph for system components which model the interconnection and interaction of system components.

Interconnection graph definition

Given a set of components C, having a set of control relations, $R_c \subseteq C \times C$ and a set of data relations $R_d \subseteq C \times C$, then the components interconnection graph G is the directed graph $G\,(C, R_c \cup R_d)$, where C is the vertices set and

$R_c \cup R_d$ is the edge set.

Building a graph is an essential part for identifying interconnection metric for each component.

To illustrate building process an example of a system containing a limited number of parts is presented. An assumption is made that there are a wireless sensor and a wireless receiver. A sensor senses the environment and generates some data which are being sent to a receiver. A receiver has its operative system, application and tasks of temporary storage of data and wirelessly forwarding data to some storage in the cloud. The illustration of this scheme is given in Figure 3.20.

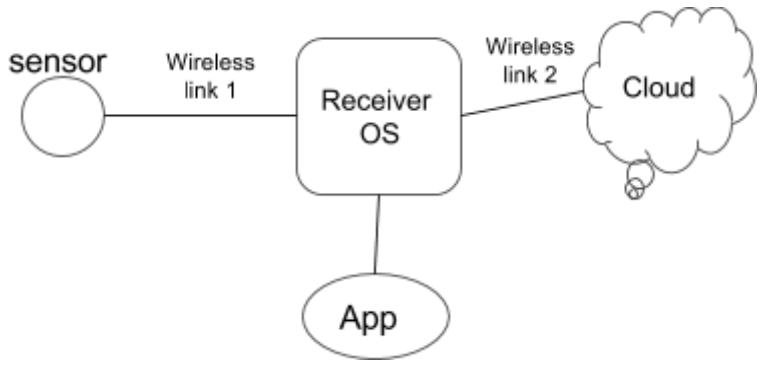


Figure 3.20: Example of simple system.

Based on this sketch, the interconnection graph for system components should be initiated. To simplify the demonstration of interconnectivity between system's components, the high-level analysis of a given simple system is applied. Each node

shown in Figure 3.20 is considered to be component. Nodes connected via edges and flows of data and control messages are identified as shown in Figure 3.21.

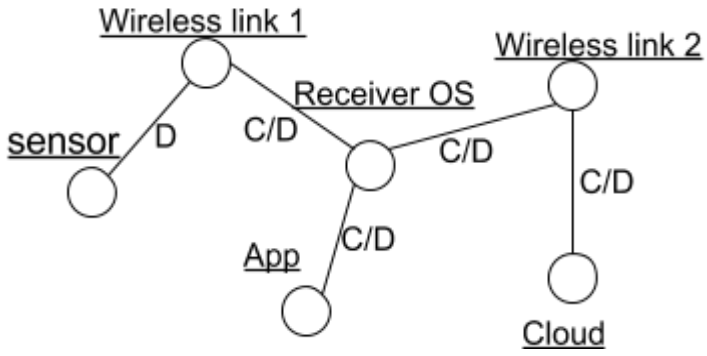


Figure 3.21: Interconnection graph.
C: control relation, D: data exchange relation.

For defining an interconnection metric for components of a system, Fayyad et al. (2015) propose interconnection-based weighting algorithm. The proposed algorithm is used for deriving a weighting equation:

$$Weight(c) = A*(S + R + 2*Ct + D + (\sum_{v=0} \frac{1}{DIST(c,v)}) + Vr)$$

(3), (Fayyad & Noll, 2015), where

- *c*: targeted component for weighting, where $c \in C$ and *C*, is set of all components in the system.
- *R*: number of sub/system components reachable from weighted component *c*.
- *S*: number of components reachable from weighted component *c* through one edge within system interconnection graph. In other words, surrounded component for component *c* is a component, which interacts directly with *c* without any intermediate component.
- *Vr*: number of the system's valuable or key components, reachable from *c.*
- *Ct*: number of control relation or edges between weighted component *c* and other system components.

- *D*: number of data relations between weighted component *c* and other system components.
- *A*: component *c* activation rate, ranges from 0 to 1. The higher the value, the more active the component, i.e. 0 - component is totally inactive, 1 - continuously active.
- *v*: a valuable component within the system.
- *DIST*: number of components between *c* and *v* components.
  (Fayyad & Noll, 2015)

3.2.3 Interconnection metric calibration

The value of weight for interconnection metric calculated using formula (3) may vary in range. Before integrating of this value in processes of SPD calculation, it should be calibrated into the range between 0 and 100. For achieving this goal, first, the architecture-based reference value, *Weight(m)*, representing the maximum weight of interconnection for a component within given system is defined.
For calculation of *Weight(m)*, the formula (3) is used, where

- *A* = 1.
- *R* = number of all system components(max number of components reachable from *m*)
- *S* = number of all system components (max number of components surrounded m).
- *Ct* = number of all control edges within system interconnection graph.
- *D* = number of all data edges within system interconnection graph.
- *Vr* = number of all valuable components within the system.
  (Fayyad & Noll, 2015)

Next, using this *Weight(m)*, the calibration of the weight of component '*c*' (*Weight*$_C$*(c)*) is executed by using the formula :

$$Weight_c(c) = \frac{Weight(c)}{Weight(m)}$$ (4) , (Fayyad & Noll, 2015), where

- *c*: given component within the system.
- *m*: a most interconnected component within the system.
- *Weight$_c$(c)*: calibrated weight in the range between 0 and 100.
- *Weight(c)*: component evaluated weight using equation (3).
- *Weight(m)*: system maximum weight of interconnection.

Based on interconnection graph for a SuI, Interconnection metric or *Weight(c)* for every component should be calculated and calibrated. Next step is defining weighting index for this metric which is going to be made by an expert in the field. The last step is an integration of Interconnection metric into criticality of a component under certain configuration as it is shown in Figure 3.22.

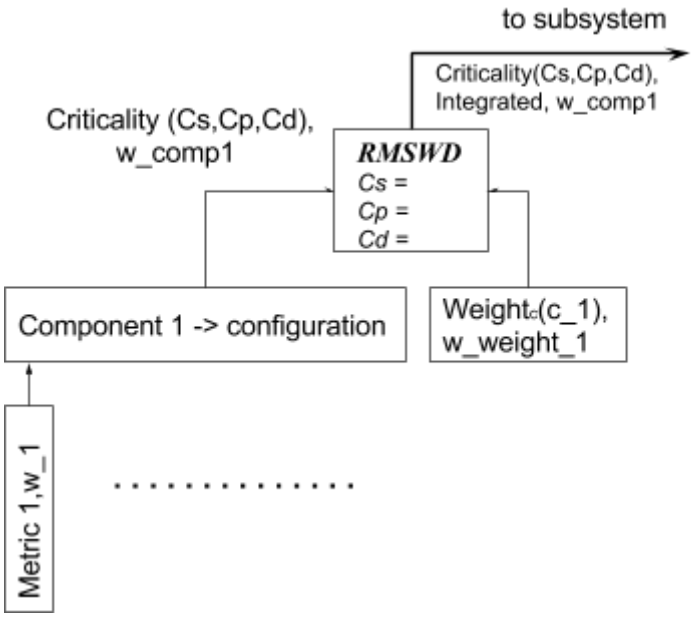


Figure 3.22: Integration of Interconnection metric.

In this figure, integration is executed by usage of RMSWD formula (2) for a Component 1, to which a certain number of metrics under chosen configuration are connected. Output value for criticality (Cs,Cp,Cd) should be calculated for security, privacy, and dependability separately. Further calculations of criticality for subsystem

and the system are not changed and executed as it is given in the description of Multi-Metrics approach in section 3.1.

3.2.4 Conclusion

The evaluation of system's security, privacy, and dependability level executed by applying the Multi-Metrics approach is not sensitive to interconnections of components within the system. In this way, the highly interconnected components' possible impact onto the system's SPD level is not appropriately considered.
By taking into consideration interconnection of components in the system influencing its SPD level, the Multi-Metrics approach obtains newly enhanced qualities, and it is becomes more objective as well (Fayyad and Noll 2015).

Limitations

Getting all three SPD level values at a green level in practice it is not possible to achieve. This fact is explained by the inverse relation between security and dependability. To obtain a highly secure system, an engineer must make sacrifices when choosing parameters for e.g. reliability and maintainability, which are building blocks of dependability. The limited scope of current research does not allow going deep into consideration of the dependencies mentioned above.

3.3 Summary

One of the important features of the Multi-Metrics approach is its comprehensiveness. It starts with component evaluation, then subsystem evaluation and ends up with complete system evaluation. It allows demonstrating that different configurations might create different SPD levels (Garitano, Fayyad et al. 2015). Another important feature of this approach is that it is highly scalable, i.e. an entire

system is allowed to be divided into an unlimited number of smaller subsystems. Alternatively, a system as a whole might integrate additional subsystems into itself. Subsystems division reduces the complexity of the process as well (Noll, Garitano et al. 2014).

System of systems

Another useful feature of the MM approach is that it allows considering any component as a system itself, as shown in Figure 3.23.

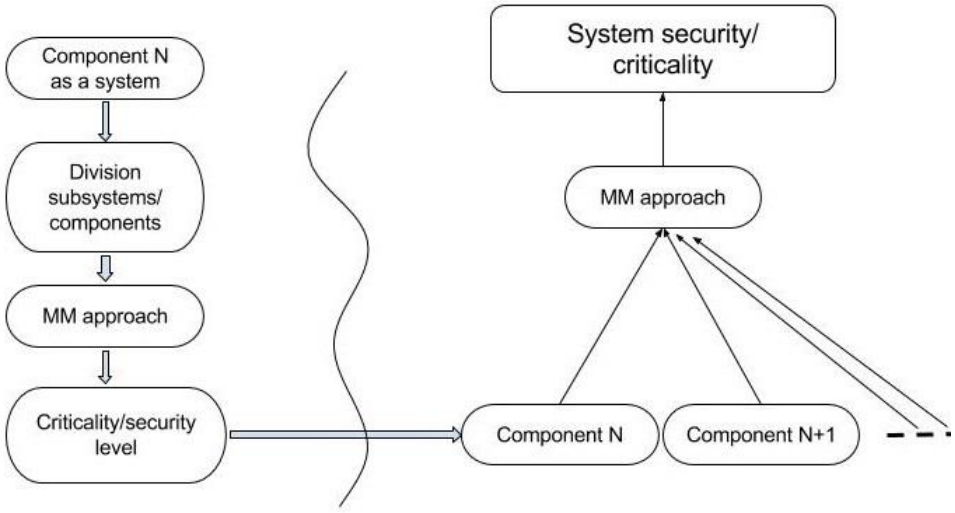


Figure 3.23: Principle system of systems.

This feature allows dividing an SuI into more complex building blocks. Considering the security, privacy, dependability level in this way gives the highest level of abstraction evaluations, hiding details of smaller levels and obtaining an overall general picture. From this level, it would be easier to distinguish weaker and stronger sides of a system. From the general picture, a researcher, who uses the MM approach, might choose a part of a system and apply an MM approach to it separately, thus making evaluations of that part more accurate.

The next unique feature of the proposed approach is that if the SPD system level is not satisfying, it allows going back in calculations to find the element that is the weakest link and reevaluate its components and configurations and make a change

in parameters. By doing this, the system engineer might achieve an SPD system which is the closest possible to the SPD goal. At the same time, specific security, privacy and dependability levels require a compromise between one another, implying a balance between all three of them. The main advantage of the MM approach consists in the simplicity of evaluating and selecting the most appropriate configuration for a given scenario. The Multi-Metrics approach reduces the complexity of the evaluation process; the visual representation of SPD simplifies the selection process (Garitano et al., 2015).

Further down, an additional feature of the MM approach is that it allows conducting evaluations of the SPD triplet according to the choice of attributes set.

For instance, for security, an evaluation could be performed for a limited set of attributes such as confidentiality, integrity, and availability. Moreover, this set could be extended to include any number of the security attributes.

The MM approach makes it easier to add or remove attributes from evaluations, depending on the task put before the researcher, and even allows making assessments separately for each of the attributes.

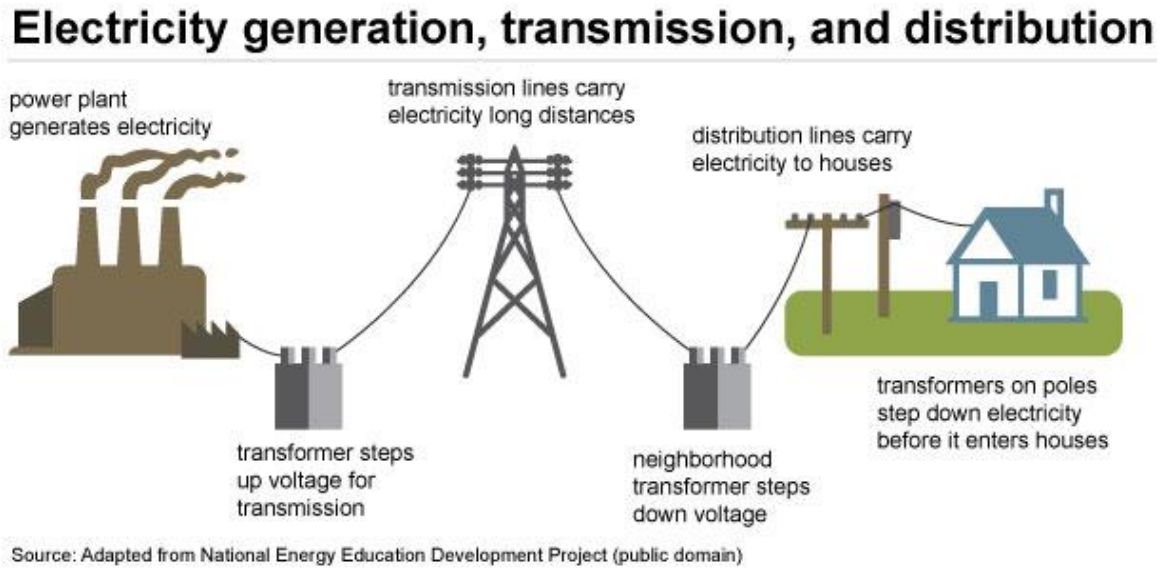
4 Applicability of Multi Metrics on Advanced Metering Infrastructure (AMI) System

4.1 AMI description

The abbreviations AMM, AMI, and AMS are used interchangeably throughout.

Power Grid

The chain of delivering electrical energy to the customer contains production, transmission and distribution parts. The production part is about producing power at the coil or other types of power plants. The transmission part is about moving electricity from where it is produced to the place where it is going to be distributed to the consumer. The distribution part is the location where power is delivered to the customer as shown in Figure 4.1.



(Administration, 2016)

Figure 4.1: Power Grid.

This structure is called Power Grid (PG) and consists of interconnected networks of transmission and distribution lines. This interconnection gives the possibility of switching of power circuits to back up in case of an outage or to direct additional electrical power to places with higher demand.
For real-time monitoring and control of the power system, after the U.S Northeast blackout 1965, there were introduced the following components of the PG:

1. Energy Management Systems (EMS) for conducting automatic generation control (AGC) and network analysis of the interconnected system;
2. Remote Terminal Units (RTUs) at generator and transmission/distribution networks for collecting real-time measurements.

However, the consumers and the distribution networks were not visible to the control center in real time. Such constraints get the name of limited visibility in space. Also, the PG suffer from limited visibility in time due to latency in traditional EMS systems (Varaiya, Wu, & Bialek, 2011).

Smart Grid

The PG should undergo transformation in the following ways (Varaiya et al., 2011):

- ❑ Increasing penetration of renewable generation, like wind and solar, whose characteristics are fundamentally different from conventional fossil fuel based generation;
- ❑ Increasing participation of demand response from consumers, replacing the traditional passive load demand;
- ❑ Fast development and deployment of energy storage systems, including grid-connected flywheels and batteries, which add a new dimension to the grid operation.

Thus PG is going to be transformed into Smart Grid (SG) which is a general term to mean a modernized and upgraded electricity grid that makes the most of the advanced information and communication technologies (ICTs) to optimize its operation and fully accommodate new technologies of renewable generation, storage and demand response (Amin & Wollenberg, 2005).
According to the U.S. Department of Energy (U.S. Department of Energy, 2008), the objectives of the smart grid are:

1. Accommodation of all generation, including renewable resources, and storage options

2. Optimizing assets and operation efficiency
3. Providing good power quality for electricity supply
4. Self-healing capability from power disturbance events
5. Operating resiliency against physical and cyber-attacks and natural disasters
6. Enabling new products, services, and markets

The vision of smart grid calls for ubiquitous and seamless communications throughout the grid to enable monitoring, management, and control power system components. Thus the traditional EMS and newly developed Advanced Metering Infrastructure (AMI) or interchangeably used term of Advanced Meter Management (AMM) are going to be integrated with PG. The introduction of new smart grid elements such as sensors, smart meters, demand response and communications would provide more accurate information about the power system and more refined means of control (Varaiya et al., 2011).

4.1.1 AMI role in Smart Grid

AMI characteristics

According to U.S. Department of Energy, Advanced Metering Infrastructure is going to be part of SG, and it is described by following features:

1. *Motivation and inclusion* of the consumer is enabled by AMI technologies that provide the fundamental link between the consumer and the grid

2. *Generation and storage options* distributed at consumer locations can be monitored and controlled through AMI technologies

3. *Markets are enabled* by connecting the consumer to the grid through AMI and permitting them to actively participate, either as a load that is directly responsive to price signals, or part of load resources that can be bid into various types of markets

4. AMI smart meters equipped with *Power Quality* (PQ) monitoring capabilities enable more rapid detection, diagnosis and resolution of PQ problems

5. AMI enables a more distributed operating model that reduces the *vulnerability of the grid to terrorist attacks and natural disasters*

6. AMI provides for *self-healing* by helping outage management systems detect and locate failures more quickly and accurately. It can also provide a ubiquitous distributed communications infrastructure having excess capacity that can be used to accelerate the deployment of advanced distribution operations equipment and applications

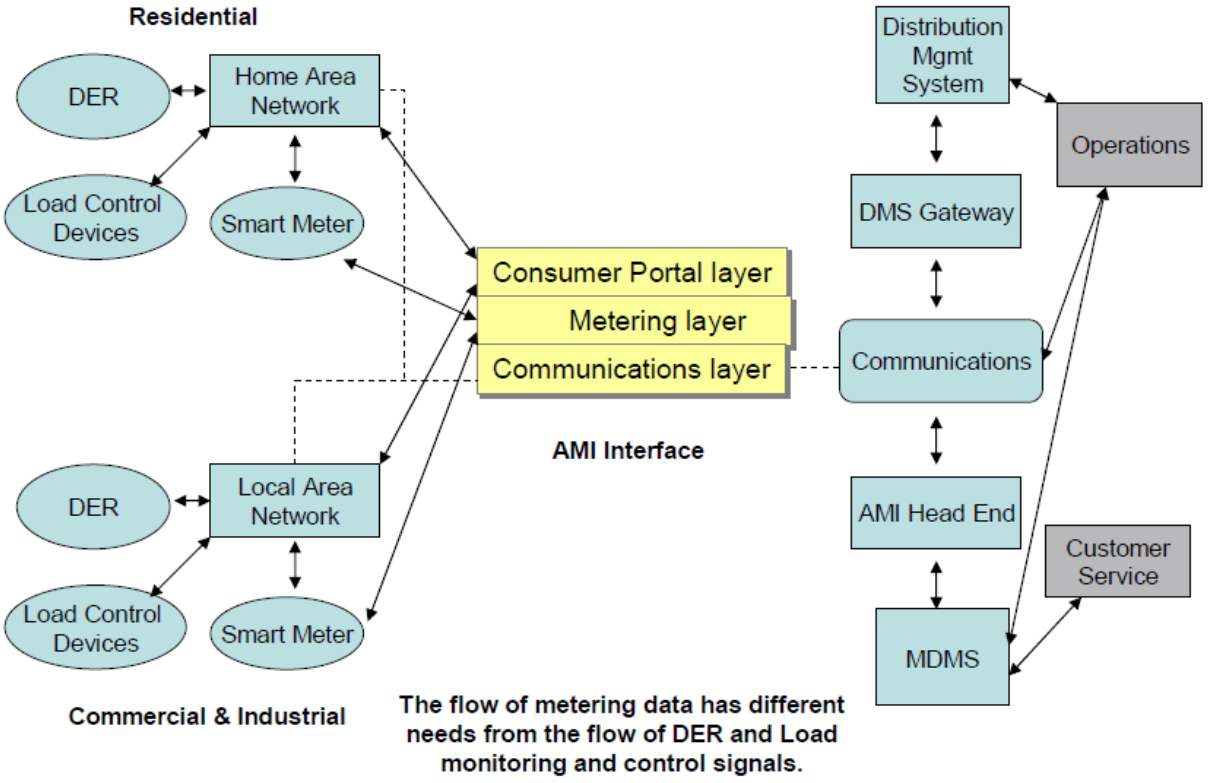
7. AMI data provides the granularity and timeliness of information needed to greatly *improve asset management and operations*

(Strategy, 2008)

In conclusion, AMI is going to provide an essential link between the grid, consumers, and their loads, generation, and storage resources.

AMI infrastructure

AMI would include a home network system, as communicating thermostats and other in-home controls, smart meters, and communication networks from the meters to local data concentrators (Strategy, 2008). Backhaul communications networks to corporate data centers, meter data management systems (MDMS) and data integration into existing and new software application platforms would part of AMI as well. Graphical description of AMI technologies and the way they interface each other as the U.S. Department of Energy defines it, is shown in Figure 4.2.



Source: (Strategy, 2008)

Figure 4.2: Overview of AMI.

At the consumer level, SM communicates consumption data to both the user and the service provider. SM communicates with in-home displays to make consumers more aware of their energy usage. Additionally, pricing information supplied by the service provider enables load control devices like thermostats to modulate electric demand, based on pre-established consumer price preferences. Another convenient feature based on such preferences, is the ability to deploy Distributed Energy Resources (DER). DER are small, grid connected devices for energy generation and storage. Consumer portals process the AMI data in ways that enable more intelligent energy consumption decisions.

The service provider (utility) employs existing, enhanced or new back office systems that collect and analyze AMI data to help optimize operations, economics and consumer service. AMI would provide immediate feedback on customer outages and power quality, enabling the service provider to address grid deficiencies rapidly. AMI's two-way communications infrastructure supports grid automation at the station and circuit level as well. The vast amount of new data flowing from AMI allows improved management of utility assets as well as better planning of asset maintenance, additions, and replacements. Thus, these features contribute to establishing a more efficient and reliable grid (Strategy, 2008).

4.1.2 Privacy and Security concerns

Data exchange between SM and CS gives rise to concern regarding execution of passive and active attacks on AMI. An active attack would lead to both consumer and retailer parts being affected. Such unauthorized access might cause e.g. power outage and financial loss. A passive attack involves observation of data traffic, thus revealing information about energy usage habits of consumers and information about the presence of consumers on their premises. In this way, the privacy of consumers is affected. Those concerns regarding security and possible privacy breaches require implementation of robust security mechanisms which can prevent an unauthorized access to AMI infrastructure. Regardless, even if the security mechanisms would protect from this, the consumer's concerns include a possibility of their lifestyle being

observed by the AMI owner. Hence, to avoid privacy breaches from the side of the AMI owner, there is a need to establish certain legal regulations as well.
What the Energy Community, an international organization dealing with energy policy, has underlined is:

> "Personal data should in general be protected by privacy law. Within the European Union certain requirements are set by Directives 95/46/EC and 2002/58/EC.39 However, special attention should be given to smart metering as the amount of personal data collected (and the potential harm which could be caused with it) is much greater than ever before. Privacy standards and access rights should be in place before a smart metering roll-out is started."
> (Balmert, Grote, & Petrov, 2012)

The Norwegian Water Resources and Energy Directorate (NVE) has additional regulations regarding AMI systems including collected data storage and usage (NVE, 2015).

4.1.3 Requirements for AMI system

All of the Norwegian electricity consumers are going to be included into the AMS system by the end of the year 2019.
According to Norwegian standards and regulations, an AMS system must satisfy a certain set of requirements. According to NVE, those requirements are stated in following hierarchy (AMS for Smart Strøm Østafjells, [s.n]), an excerpt:

3. Requirements to functionality
    - 3.0 Functional requirements in connection to AMS
    - 3.1 Metering
        - 3.1.1 Registering of measurements
        - 3.1.2 Transmission of measurements
        - 3.1.3 Control of transmission
        - 3.1.4 Storing of measurements

6.2 Relationship in metering point

6.3 Information processing during mounting

7. Requirement to cost effective operations and maintenance

7.1 General cost of operations

7.2 Requirements for future changes and scalability

7.3 Requirements for diagnostic tools communications

8. Requirements for security

8.1 Privacy

8.2 Authentication

8.3 Robustness against malware and intrusion

8.4 Encryption

8.5 General requirements for security

8.6 Protection against Electromagnetic Interferences (EMI)

8.7 Protection against Electromagnetic Pulse (EMP)

9. Additional requirements, alternative communication solutions.

All requirements in the NVE document are divided into three categories and labeled as:

- Mandatory,
- Desirable,
- Informative,

or a combination of above named.

The Aidon AMM system should satisfy at least all requirements with the label mandatory.

The processing all these requirements named above is done with some limitations, collecting only those details which are most necessary for this study and summarizing in a separate document. For detailed information see Appendix A.

Application

All of the requirements named above are going to be used in the evaluation of the security level of the Aidon AMM system by using the Multi Metrics approach in the this study.

4.1.4 Aidon Advanced Meter Management (AMM) infrastructure

The Aidon AMM infrastructure, as it is shown in Figure 4.3, consists of three major parts:

- Smart Meters (SM),
- Central System (CS),
- Communication links.

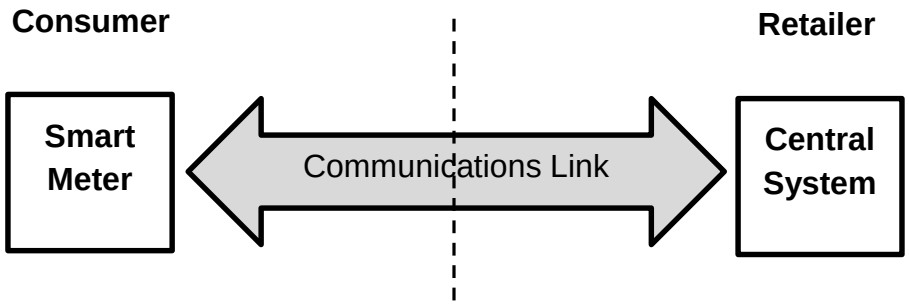


Figure 4.3: Infrastructure of AMM.

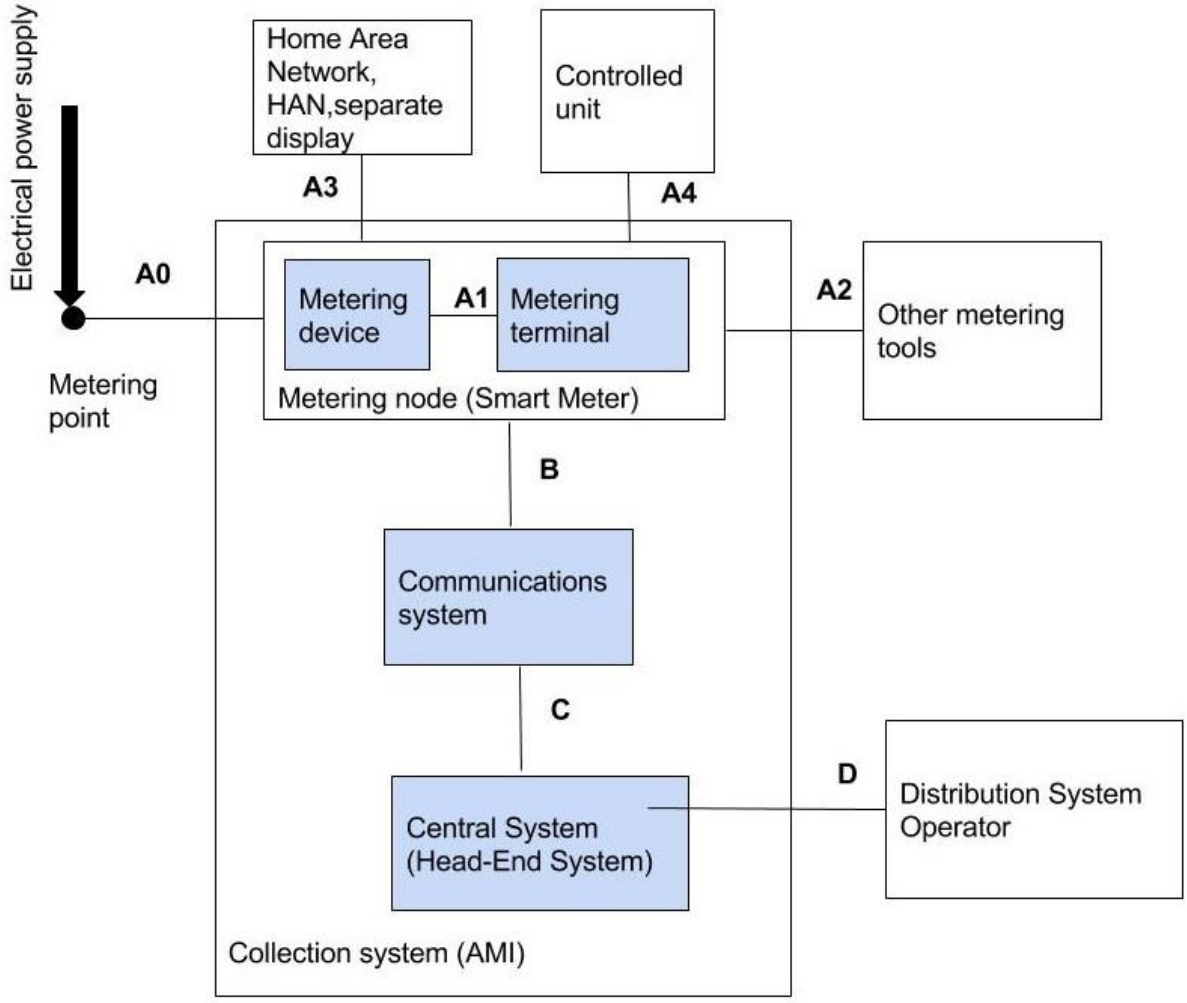
Smart Meter core functions measure electrical power consumption, preprocess of measurement data and forward data to CS. The minimum requirement defined by NVE is that data about energy usage should be delivered to the HE one time every twenty-four hours (NVE, 2011). The granularity of readings in SM plays a significant role, i.e. readings are supposed to happen much more often in comparing to older systems, thus the amount of information to transmit, store and process is drastically increased. NVE puts the limit on frequency of taking measurements of power usage as one to four reading per hour (Lovdata, 2017).

The Central system's main function is processing and storage of the measurements, received from SM.

The communication link function enables two-way data exchange between SM and CS.

Aidon AMM system's block structure

In Figure 4.4 the block structure of the Aidon AMM system is shown.



Source: (AMS for Smart Strøm Østafjells, [s.n])

Figure 4.4: Block structure of AMM.

The measurement value chain of Collection system (AMM) contains:

1. A Metering device which registers energy consumption at the Metering point

2. A Metering terminal which preprocesses data from obtained from Metering device
3. A Communication system which provides transmissions between SM and CS
4. A Central System or Head-End System for receiving, processing, storing of data

As Figure 4.4 shows, the critical interfaces of the value chain are:

- **A0**: Metering point - Metering device
- **A1**: Metering device - Metering terminal
- **A2**: Metering terminal - Other tools for metering oil, gas, water consumption
- **A3**: Metering node - Separate display, HAN
- **A4**: Metering node - Controlled unit, local control
- **B**: Metering node - Communications system
- **C**: Communication system - Central System
- **D**: Central - Distribution System Operator

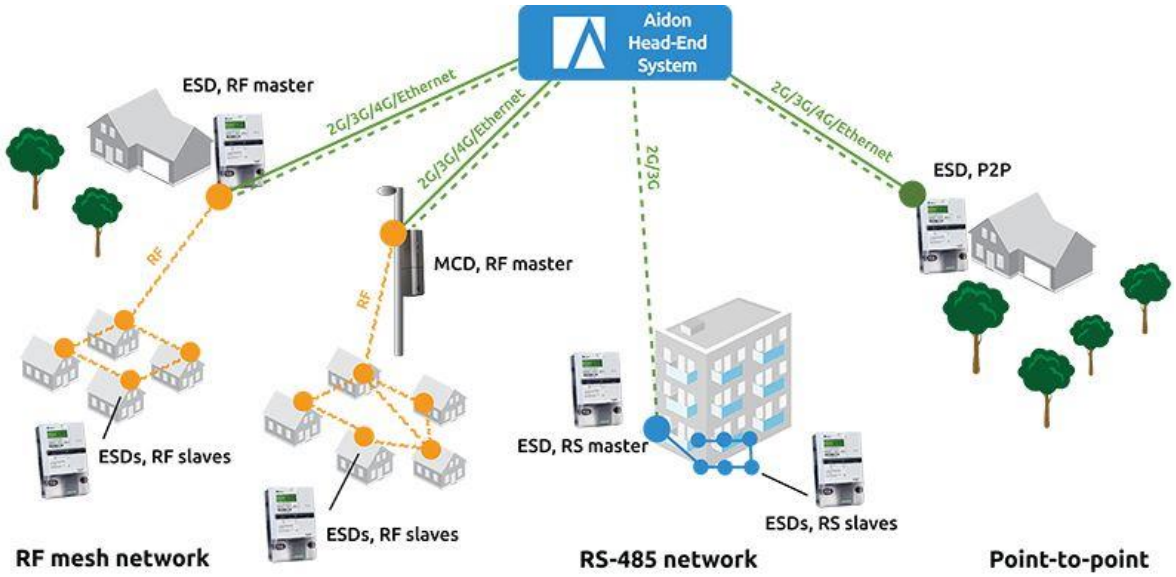
(AMS for Smart Strøm Østafjells, [s.n])

Structure of Aidon AMM

The Aidon AMM scheme for integration into different household structures is going to be implemented as shown in Figure 4.5.

The Aidon Energy Service Device (ESD) plays the role of SM in Figure 4.3 and consists of a meter and a system module with the communication unit. The Aidon Head-End system plays the role of CS, Figure 4.3. The Link (L), Figure 4.3, for Aidon AMM is represented by mobile 2G/3G/4G networks or utility's Ethernet network.

The ESD communication unit is a Radio Frequency (RF) part which can be used as an RF master or RF slave device. There is an additional type of device named Multi-Connectivity Device (MCD). MCD is an independent wireless RF communication unit without a meter, which in turn can be an RF master or RF slave device. A unit with a Master RF device is supposed to be a gateway for a group of ESD devices which forwards data further to the Head-End System (Aidon, 2017b).



Source: (Aidon, 2017a)

Figure 4.5: Aidon AMM system integration.

The figure above shows that consumer installations might use different technologies to establish a connection to Aidon Head-End such as:

- RF wireless mesh network for group of houses near each other,
- RS-485 standard loop network for blocks for multi-story buildings,
- P2P connections for standalone houses.

For networks built on the wireless mesh and RS-485 technologies, a gateway is used. It could be either ESD or MCD devices. For standalone households, as in the figure, an ESD would be a gateway itself.

4.2 Applying MM approach

Metrics are objects or entities used to measure the SPD criticality of components (Noll et al., 2014). This thesis concentrates on security evaluation of a system. Thus metrics must be chosen in accordance with the following:

- There should be defined a primary object in the system in which a secure state to be preserved

- Metrics should reflect complete preservation of security attributes

The primary objects for security evaluation in the current master thesis are data readings of electrical power use, stored at Smart Meter and all messages sent between Smart Meter and Head End.
The following limited set of security attributes was chosen:

- *Confidentiality* of data readings
- *Integrity* of data readings and Head End messages
- *Availability* of data readings and communication channels
- *Authenticity* of data readings and Head End messages
- *Accounting* of user interactions
- *Non-repudiation* of user interactions

In this section, identification of subsystems and components is undergone. The set of metrics for an AMM is defined. The preliminary values for the weights and values of criticality for the security of each participator are estimated. Based on obtained values, the evaluation of security level of Aidon AMM deployed for four usage scenarios is assessed. Those scenarios are defined as:

- Consumption measurement
- Meter Reading Services
- Outage Detection and Restoration
- Remote Connection/Disconnection of Meter

The set of metrics has been identified from the following considerations:

- Limited set of security attributes defined above

- ❖ Requirements prepared by NVE to an AMI system, Appendix A.

The values for criticality and weights have been defined by the author of this research based on his experience and theoretical knowledge.
The Aidon data sheets were used as a guideline in defining values for criticality. Because the current research is limited only to evaluations of security out of SPD triple, the terms Cs or criticality are used in place of criticality for security.

4.2.1 Identification of subsystems participating in use case scenarios

For assessment of a security level of an AMM for chosen usage scenarios, the following participants are considered, shown in Figure 4.6.

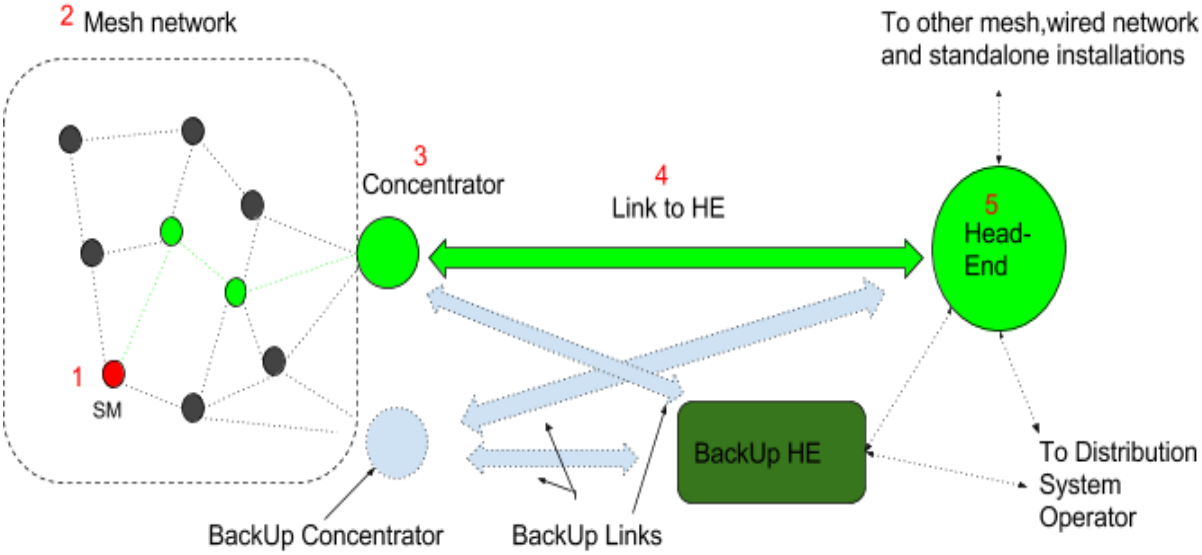


Figure 4.6: Identified participants.

Considered SM is chosen as one of the participant nodes in the wireless mesh network.

The following subsystems are identified for usage scenarios and shown in Table 4.1.

Table 4.1: Subsystems participating in use case.

	Subsystem	**Description**	**Number**
1	Smart Meter	RF slave, Energy Service Device	one
2	Wireless Mesh	RF slave, ESD	multiple
3	Concentrator	RF master	one
4	Link Concentrator-Head End	2G,3G,4G, Ethernet	one
5	Head-End	Head End system	one

The assumption is made that the BackUp Concentrator, shown in gray in Figure 4.6, is in sleeping mode and activated in case of main Concentrator failure. BackUp Links, shown in gray in Figure 4.6, are established when needed, i.e. in the case of the main Link Concentrator- HE failure or Head End system failure.

In this thesis, the researcher applied the MM approach at high-level for Hub, Concentrator, HE, since the focus of this study is Smart Meter.

4.2.2 Subsystem 1, Smart Meter

The Smart Meter block structure is given in Figure 4.4, and accordingly, the deployed interfaces for considered SM are shown in Figure 4.7 below.

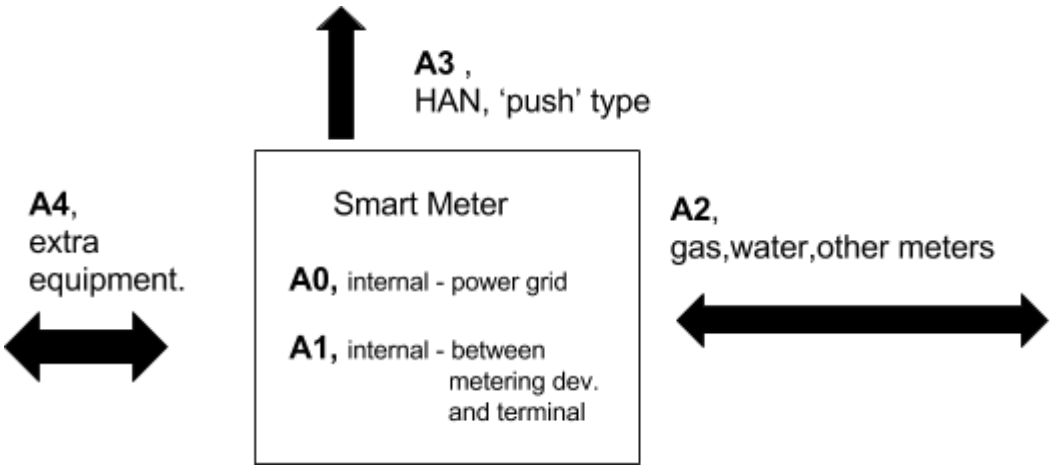


Figure 4.7: Structure of SM. **Only participating interfaces shown.**

Smart Meter objectives

- **A0** interface between the power line and metering device considered to be secure due to very limited access by personnel and no access by a possible attacker under normal drift. Excluded from further considerations.
- **A1** interface between metering device and metering terminal considered to be secure due to very limited access by personnel and no access by a possible attacker under normal drift. Excluded from further considerations.
- **A2** interface is used to process, receive and forward data traffic to and from other smart meters in the mesh as well as data traffic from other meter types such as gas and water.
- **A3** interface is used to forward readings to the HAN.
- **A4** interface is used to connect to handheld equipment of technician personnel, and data goes two ways, in and out of SM
- **B** interface is not present for a slave ESD

The metering device itself, shown in Figure 4.4 is located inside of SM and considered to be secure and excluded from further considerations.
Interface **A2** is recognized as most heavily loaded. For providing the functionality of AMM, the following regular data traffic is identified for interface A2:

- Downstream of data from HE going through SM and data addressed to SM:
  - *Commands from HE*
  - *Tariffs, possible multicast*
  - *Software updates, possible multicast*
  - *Keepalive messages, confirmation that HE is ON, possible multicast*
  - *Additional requests from HE, like unscheduled request of logs of SW status/configuration*
  - *Time messages to all SMs, synchronized with Statnett NTP server, possible multicast*
  - *Acknowledgments, ACKs (e.g. on receiving logs)*
  - *Routing traffic*

- Upstream of data going through SM and data traffic generated by SM (towards HE):
  - *Readings of electrical power consumption*
  - *Logs*
  - *Another type of information, like SW status/configuration,*
  - *Acknowledgments, ACKs (e.g. on receiving updates)*
  - *Additional requests to HE (e.g. authenticate new node in mesh request)*
  - *Keepalive messages, confirmation that SM is up and running*
  - *Routing traffic*

All aforementioned considerations are important for establishing of the SPD goal and identification of metrics.

Weight of Subsystem 1, SM

Because SM is the part that obtains, stores and processes data on electrical power use and is involved in interactions with HE system, its weight is defined to be *90*. This value highlights its great importance in the AMM system.

Identification of components for SM

For subsystem Smart Meter the identified components are reviewed in Table 4.2 below.

Table 4.2: Components identified for subsystem SM.

Subsystem 1, Smart Meter, weight = 90		
	Component	**Description**
1	OS	Operative System
2	Interface A2	Connection to other SMs, gas/water meters
3	Interface A3	Connection to HAN
4	Interface A4	Connection to extern technical equipment
5	Physical Protection	Physical protection of SM

Justification

Component **OS**: an SM contains the OS, the features of which are essential to preserving the secure operation of an SM.

Component **Interface A2**: this interface is the most loaded of all interfaces because it processes and forwards data traffic for other nodes in the wireless mesh. Moreover, SM uses this interface to forward its own generated data traffic.
The presence of routing traffic in the wireless mesh network raises concern, as this traffic is not controlled via HE, i.e. routing is more vulnerable to an unauthorized change. Important for this interface is the ability to detect a jamming signal and a

possible attempt of an attacker to simulate entrance of new nodes into the mesh network.

Component **Interface A3**: this interface pushes the readings and tariff information towards the HAN.

Component **Interface A4**: this interface is used by technician personnel for maintenance and other types of work. It should require identification, authentication, and authorization of personnel and authentication of handheld equipment and integrity check of SW inside of equipment.

Component **Physical Protection**: EMI, EMP, deviations in humidity and temperature from nominal values might affect secure operations of SM. Reflects the physical DoS protection. Sealing cannot be trusted due the general availability of sealing tools.

Identification of metrics

At this stage identification of metrics for each component, the weight of each component, the weighting of metrics and defining values for the criticality of parameters of each component's metric is conducted.

Component 1, OS:

Table 4.3: Set of metrics for component OS.

Component 1, OS, weight = 90					
Metric		**Description**	**Weight**	**Cs**	
				Applied	
				Y	N
1	Secure Boot	Sealed boot loader holding a public key of vendor/utility, e.g. TPM	90	20	80
2	Secure Memory	Memory buffer wiping	70	30	70
				In use	
				Y	N
3	Antivirus SW	Malware protection	50	30	60
				112bits	
				Higher	Lower
4	Cryptography	Describes cryptographic suit for encryption, hashing	80	10	90
				Applied	
				Y	N
5	Logging	Secure store of logs, taking care of confidentiality, integrity, access upon HE decision	70	30	70

Metric 4, *Cryptography*, refers to the security level in bits chosen for cryptographic suits.

Note: Security level in bits is defined according to specifications of NIST SP 800-57; 112 bits and higher yields protection up to the year 2030 (Barker, 2016).

The weight of the Component **OS** is defined as *90* due to its responsibility for obtaining, storing and processing raw data that has a crucial importance for secure operations in SM.

Component 2, Interface A2:

Table 4.4: Set of metrics for component Interface A2.

Component 2, Interface A2, weight = 70					
Metric		**Description**	**Weight**	**Cs**	
				In use	
				Y	N
1	Mesh Authentication	Source authentication check, integrity, replay check – at joining mesh	30	20	80
				Y	N
2	Node Authentication	Source authentication check, integrity, replay check- at forwarding data traffic from other nodes	80	30	80
				Session establishing	
				Y	N
3	Session	Secure end-to-end sessions for traffic originated from SM, e.g. SSL session vs. non-protected traffic	90	15	90
				Implemented	
				Y	N
4	Jamming Detection	Jamming signal sensing, alarm sent, interface switched off	80	30	70
5	DoS prevention	Abrupt the effort of joining mesh if more than 20 nodes involved, number is adjustable	70	40	60

The weight of the Component **Interface A2** is defined as *70* because it is not involved in the processing of raw data, in contrast to component **OS**.

Metric 3, *Session* reflects that it is assumed that SM communicates with HE either by establishing e.g. SSL session or by transmitting data in plain text.

Note: Important for security evaluations is the fact that routing traffic is not authenticated via HE

Component 3, Interface A3:

Table 4.5: Set of metrics for component A3.

Component 3, Interface A3, weight = 60					
Metric		**Description**	**Weight**	**Cs**	
				Applied	
				Y	N
1	Crypto	Use of crypto protection data sent to HAN	60	20	60
2	Authentication	Authentication of HAN towards SM via HE	80	15	70

There are two options for configuring component Interface A3 (Aidon, 2017b):

a) Non-secure :
   i. Data traffic between SM and HAN is not encrypted
   ii. Authentication of HAN towards SM is neither performed or confirmed by HE
b) Secure :
   i. Data traffic between SM and HAN is encrypted
   ii. Authentication of HAN towards SM confirmed by HE

The weight of Component **Interface A3** is defined as *60* because it transmits confidential data which might be vulnerable to eavesdropping, especially in the case of wireless connection to HAN and in the event that data are not encrypted, and HAN is not authenticated properly. The application of the two last options is left for the customer's consideration.

The weight of the metric *Authentication* is higher than the weight of the metric *Crypto* because the authentication of HAN has higher importance than encryption of data exchange.

In the case of choice for unencrypted communication without authorization: because the absence of encryption data makes easy eavesdropping, criticality values are set high, for metric *Crypto Cs = 60*. Due to the lack of authentication, a possibility of a fake HAN connection request to be satisfied has high probability. This case allows an attacker to receive data directly. Therefore criticality is greater, for metric *Authentication Cs = 70*. The values for criticality are not set to highest possible values as an attacker would need some skills, time, and equipment for executing such an attack.

In the case of choice for encrypted communication with authorization: because encryption data is not vulnerable to passive traffic analysis, criticality is low, for metric *Crypto Cs = 20*. Authentication via HE is the most reliable option, criticality is of lesser value, for metric *Authentication Cs = 15*.

Component 4, Interface A4:

Table 4.6: Set of metrics for component A4.

Component 4, Interface A4, weight = 90					
Metric		**Description**	**Weight**	**Cs**	
				Applied	
				Y	N
1	Accessibility	Authentication, authorization of personnel via HE	95	20	95
2	Equipment	Equipment authentication, SW integrity check	95	20	95
3	Crypto	Crypto protection of traffic between SM and equipment	50	15	90

This component is by definition a connector of an SM to external equipment. This fact makes it an attractive target for an attacker. Tampering with it might give the malicious intruder a great benefit. Because of this, the weight of the Component **Interface A4** is defined to be of high value *90*.

The weight of *Identification* and *Equipment* metrics are defined to be of great value at *95* because they reflect features which are vital in keeping secure operations of SM. Criticality in "Not applied" state, Table 4.6, are defined to be of high values at *95* for both metrics. It emphasizes weakness in case of absence of the described features.

The metric *Crypto* has lower weight because in the event that a personnel is not authorized, and equipment is not authenticated, the encryption of data exchanged would not be of high importance. However, if first and second metrics parameters are applied; the data exchange might be a subject for eavesdropping, thus explaining the choice for criticality for security values of *90* in the case of unencrypted and *15* in the case of encrypted data exchange.

Component 5, Physical protection:

Table 4.7: Set of metrics for component Physical Protection.

Component 5, Physical Protection, weight = 70					
Metric		**Description**	**Weight**	**Cs**	
				Applied	
				Y	N
1	EM Protection	EMI, EMP protection	50	15	70
2	Temperature	Alarm, steps as switching OFF a SM	40	20	60
3	Humidity	Alarm, steps as switching OFF a SM	40	20	60
4	Tampering	Authorization via HE to open the case, sealing cannot be trusted	70	15	80

The weight of the Component **Physical Protection** is defined as *70* since the ability of SM to sustain physical damage provides stability in secure operations of SM. It is worth noting that one of the interested parties in tampering with SM is the owner of a household. This assumption justifies the choice of high value for criticality for the metric *Tampering* in the case of absence of authorization via HE, *Cs = 80.* The

general availability of sealing tools justifies this choice.

4.2.3 Subsystem 2, Head-End (HE)

Weight of Subsystem 2, Head-End

Subsystem **Head-End** is considered to be a highly secured system in itself. This assumption is the reason why the value of weight for this subsystem is defined as *20*.

Identification of metrics

Because of applying a high-level analysis of **Head-End** subsystem, only metrics concerning secure operations of HE are identified, and calculations are made without components identification as shown in Figure 4.9.

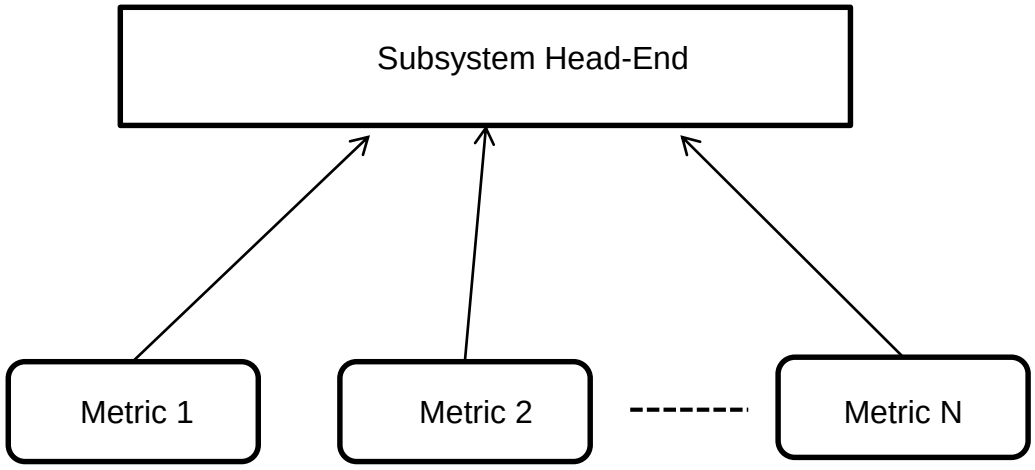


Figure 4.8: Subsystem and metrics relationship.
High-level analysis.

This figure shows that when evaluating the SPD system using the MM approach, there is a possibility of using different combinations of subsystems, components, and metrics. Such flexibility makes the MM approach a very convenient tool.

The set of metrics for subsystem **Head End** is summarized in Table 4.8 below.

Table 4.8: Set of metrics for subsystem Head-End.

Subsystem 2, Head-End, weight = 20					
Metric		**Description**	**Weight**	**Cs**	
				Least once every 24 hrs.	
				Y	N
1	Antivirus Update	Issue of update/upgrade	80	30	80
				Within 24 hrs.	
				Y	N
2	Patching	Average time between vulnerability discovery and patch issue	80	20	80
				Greater than 72 hrs.	
				Y	N
3	Compromisation	The average time between discovery of compromised SM and necessary measures taken, e.g. 72 hrs.	50	60	20
				Applied	
				Y	N
4	Intrusion	IDS, IPS usage	80	20	85
5	Access Control	AC policy and procedures applied	85	20	90

Justification

Metric 1, *Antivirus Update*, refers to the frequency of update/upgrade of antivirus software, distributed from HE towards all SMs.

Metric 2, *Patching*, refers to an amount of time between vulnerability discovery and patching, distributed by HE towards all SMs.

Note: in wireless mesh installations, the multipath propagation can introduce a jitter for a signal arriving at multiple SMs.

Metric 6, *Compromisation*, refers to the rapidness with which the HE reacts to discovery of SM compromisation. E.g., in the case of SM theft, the data might be extracted from compromised SM.

Metric 7, *Intrusion*, refers to the usage of the Intrusion Detection Systems and Intrusion Prevention Systems. These increase the capability of system monitoring to detect and isolate penetration attempts (Grid, 2010). Special attention should be paid to the fact that intruders might use encrypted malicious traffic which would be difficult to distinguish from authorized encrypted traffic.

Metric 8, *Access Control*, refers to establishing of appropriate access control policy and procedures. This focuses on ensuring that resources are accessed only by appropriate personnel, and that personnel are correctly identified (Grid, 2010).

4.2.4 Subsystem 3, Concentrator

The role of Concentrator is to be a gateway towards Head End for all Smart Meters in wireless mesh installation.
The concentrator and its interfaces are shown in Figure 4.9.

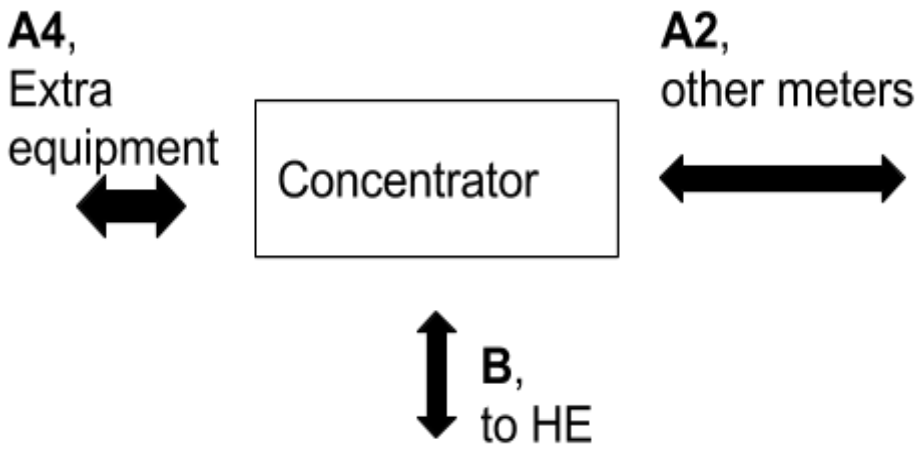


Figure 4.9: Subsystem Concentrator. Participating interfaces were shown.

As it might be seen, in contrary to SM, the interface **A3** is absent for concentrator. Interface **B**, through which the communications with HE system goes, is presented.

Because of applying a high-level analysis of **Concentrator** subsystem, only metrics concerning secure operations of Concentrator are identified without components identification, as for subsystem Head End.

Weight of Subsystem 3, Concentrator

Since subsystem **Concentrator** is by assumption an RF device, which only forwards data traffic without access to raw data, the weight of this subsystem is defined as *50*.

Identification of metrics

Emphasizing the features, which are mandatory for the secure functioning of an AMM and which are relevant to this thesis, the identified metrics are reviewed in Table 4.9 below.

Table 4.9: Set of metrics for subsystem Concentrator.

Metric		**Description**	**Weight**	**Cs**	
				Provided	
				Y	N
1	BackUp	Presence of backup Concentrator	50	20	60
				Applied	
				Y	N
2	Authentication Limit	Limit numbers of unsuccessful authentications attempts, e.g. max 10/min	70	15	80
				112bits	
				Higher	Lower
3	Cryptography	Describes cryptographic suit for encryption, hashing			

Justification

Metric 1, *BackUp*, refers to whether a single concentrator is going to be a Single Point of Failure (SPF), and for providing redundancy there should be a possibility of installing/switching on a backup Concentrator.
The additional backup route is located in the proximity of 600m from the master node (Aidon, 2017a).

Metric 2, *Authentication Limit*, refers to a mechanism that restricts continuous authentication login attempts via interface A4 and A2. The importance of implementing of such mechanism is explained by the fact that the Concentrator is

installed at the remote location. Additionally, many of data flows are concentrated at one point, thus making the concentrator an attractive target for an attacker.

Metric 3, *Cryptography*, refers to the security level in bits, chosen for cryptographic suits.
Note: Security level in bits is defined according to specifications of NIST SP 800-57; 112 bits and higher yields protection up to the year 2030 (Barker, 2016).

4.2.5 Subsystem 4, Wireless Mesh

Because of applying a high-level analysis of **Wireless Mesh** subsystem, only metrics concerning secure operations of Wireless Mesh are identified, and calculations are made without components identification, as for subsystem Head End.

Weight of Subsystem 4, Wireless Mesh

Since subsystem Wireless Mesh only deals with routing protocol issues and has no connections to raw data processing, the weight of this subsystem is defined as *50.*

Identification of metrics

Emphasizing the features, which are mandatory for the secure functioning of an AMM and which are relevant to this thesis, the identified metrics are reviewed in Table 4.10 below.

Table 4.10: Set of metrics for subsystem Wireless Mesh.

	Metric	Description	Weight	Cs	
				Simple	Complex
1	Path Cost	Path cost calculation for routing	60	60	30
				used	
				Y	N
2	QoS	Traffic priority, packets marking	70	20	70

Justification

Metric 1, *Path Cost*, refers to the method of calculation a paths cost for building up routing tables. The path cost may be calculated by use of the hop count metric. Another way is when the path cost is based on a complex set of parameters such as delay, bandwidth, reliability, and load, thus making protocol very accurate in selecting the proper route. This is the reason why criticality in the case of simple route calculation is greater than for complex route calculation.
Routing scheme used by Aidon AMM system belongs to the family of dynamic routing protocols with proactive scheme of routing table calculations (Aidon, 2017a).

Metric 2, *QoS***,** refers to the provisioning of QoS, an emergency traffic prioritization feature in wireless mesh networks, which can be reflected in e.g. route selection, packet marking (Ashraf, 2010).

4.2.6 Subsystem 5, Link Concentrator – HE

Because of applying a high-level analysis of **Link Concentrator-HE** subsystem, only metrics concerning secure operations of Link Concentrator-HE are identified, and calculations are made without components identification, as for subsystem Head End.

Weight of Subsystem 5, Link Concentrator-HE

The author of this thesis assumed the weight of this subsystem to be *20.*

Identification of metrics

Emphasizing the features which are mandatory for the secure functioning of an AMM and which are relevant to this research, a metric was identified:

Table 4.11: Set of metrics for subsystem Link Concentrator-HE.

Metric		Description	Cs	
			Provided	
			Y	N
1	BackUp	Backup link establishing between Concentrator and BackUp HE	20	70

Justification

Metric 1, *BackUp*, refer to establishing a backup link to BackUp HE system according to the requirements of NVE, thus assisting in providing redundancy.

4.2.7 Establishing the SPD goal

In this part, there was the SPD goal for four specific usage scenarios established.

Scenario 1 – Consumption Measurement

In this scenario, the SM obtains and processes data readings and stores them locally. The system is in a steady state or normal drift.

Key objectives:

- Consumption measurement readings are stored at SM

In this scenario, availability is not critical as consumption measurement readings do not leave SM. Integrity is of high importance. Confidentiality is of moderate importance.
Established SPD goal = (50,p,d).

Scenario 2 - Meter Reading Services

Meter reading services provide the basic meter reading capabilities for generating customer bills. Different types of metering services are usually provided, depending upon the applicable customer tariff.
Services included:

- Periodic Meter Reading
- On-Demand Meter Reading
- Feed-In Tariff Metering
- Bill - Paycheck Matching
  (Grid, 2010)

Key objectives:

- Data readings are sent to HE

In this scenario, confidentiality is put at a high level to avoid serious breaches of privacy and potential legal repercussions. Integrity is important, but the impact of incorrect data is not large. Availability of meter data is not critical in real-time (Grid, 2010).
Established SPD goal = (60,p,d).

Scenario 3 - Remote Connect/Disconnect of Meter

In the AMM system, remote connect/disconnect can be performed for the following reasons:

- Remote Connect for Move-In
- Remote Connect for Reinstatement on Payment
- Remote Disconnect for Move-Out
- Remote Disconnect for Nonpayment
- Remote Disconnect for Emergency Load Control
- Unsolicited Connect / Disconnect Event
  (Grid, 2010)

Key objectives:

- SM receives a connect/disconnect command from HE

In this scenario, the integrity of control commands *connect/disconnect* is critical to avoid unwarranted disconnections. The impact of invalid switching could be very large if many meters are involved. Confidentiality of commands is not very important (Grid, 2010). Availability to turn meter back on when needed is critical.
Established SPD goal = (70,p,d).

Scenario 4 - Outage Detection and Restoration

The AMM system detects customer outages and reports it in near real time to the HE. The process includes the following steps:

- Smart Meter detects one or more power losses
- Outage management system at HE collects meter outage reports
- Outage management system determines location of outage
- Work management system schedules a technician to resolve outage (Grid, 2010)

The assumption is made that outage affected the entire wireless mesh network.

Key objectives:

- SM detects an outage and reports to HE

In this scenario, integrity is important to ensure outages are reported correctly. Confidentiality is not very important. Availability is of paramount importance to ensure outages are reported in timely manner (Grid, 2010).

The HE has to report an outage further to distribution utility, thus, lowering delay and ensuring outage message delivery has a great importance for the entire Smart Grid reliable functioning.

Additional requirements for this scenario is that even if an outage occurs, and SM starts using the battery power, the secure operations of an AMM must not be disturbed.

Established SPDgoal = (60,p,d).

The values for SPD goal are summarized in Table 4.12 below:

Table 4.12: The SPD goal for different scenarios.

	Scenario	**SPDgoal**
1	Consumption Measurement	(50,p,d)
2	Meter Reading Services	(60,p,d)
3	Remote Connect/Disconnect of Meter	(70,p,d)
4	Outage Detection and Restoration	(60,p,d)

For all described scenarios, the levels of importance of security attributes as confidentiality, integrity, and availability were considered. The security objectives of authenticity, accounting, and non-repudiation are mandatory for all scenarios. All the security attributes belongs to a limited set of security attributes which is given in section 4.2.

4.2.8 Calculation of the SPD criticality

In this part, calculations of the SPD criticality for the System under Investigation Aidon AMM, was conducted.

Configuration

The total number of possible configuration is huge: *2**30* (the total number of metrics is *30*, each metric has two parameters). Because of the limited scope of this thesis, the author of this thesis decided to prune the total number of all possible configurations down to five, and evaluate if those configurations matching SPD goal for use case scenarios for Aidon AMM.

There were considered following configurations:

- Configuration Worst case – this configuration includes the changing all parameters to have maximum values for Cs.
- Configuration 1, Configuration 2, Configuration 3 and Configuration 4 where chosen in a such way, so that the resulting values for security would appear in the range, close to established SPD goals range, i.e. between 50 ± 10 and 70 ± 10.

The tables in Appendix B reviews the sets of metrics, the parameters for metrics, criticalities for parameters and the SPD criticality, obtained for all five chosen configuration.

For the SPD criticality, only values for the Criticality for Security were shown for simplicity.

SPD criticality calculations

All calculations were made according to summarization given in section 3.1.8, are executed using Excel spreadsheet, supplied in Appendix C. For the SPD criticality, only values for the Criticality for Security were shown for simplicity.

4.3 Result analysis

4.3.1 Obtained values

Results of calculations are shown in Table 4.13:

Table 4.13: Multi Metrics evaluation of an Aidon AMM system.

Configuration	SPD Criticality, Cs	SPD system, S	Scen.1	Scen.2	Scen.3	Scen.4
SPD goal			(50,p,d)	(60,p,d)	(70,p,d)	(60,p,d)
Configuration Worst Case	76	24	🔴	🔴	🔴	🔴
Configuration 1	44	56	🟢	🟢	🟡	🟢
Configuration 2	31	69	🟡	🟢	🟢	🟢
Configuration 3, Best Case	21	79	🔴	🟡	🟢	🟡
Configuration 4	38	62	🟡	🟢	🟢	🟢

Configuration Worst Case

The worst configuration involves changing all parameters to have maximum values for Cs. It yields overall security level for system S = 24. The obtained value might be used as a guide for real usage scenarios and comparison purposes.

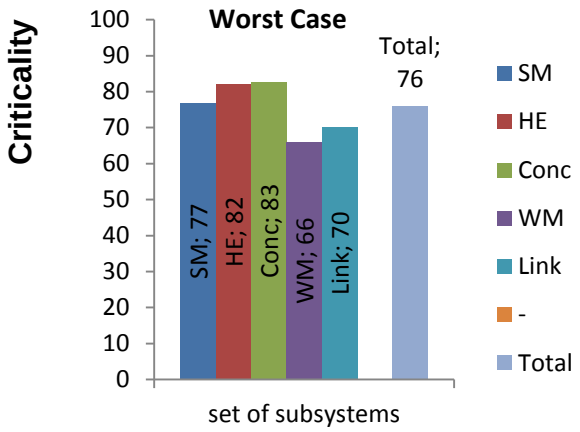


Figure 4.10: Contribution of subsystems, Cs values shown

As seen in the figure above, all subsystems contribute almost equally.

Configuration 1

According to comparison, shown in Table 4.13, this configuration matches the SPD goal for Scenario 1, Consumption Measurement and Scenario 2, Meter Reading Services.

Configuration 2

According to comparison, shown in Table 4.13, this configuration matches the SPD goal for Scenario 2, 3 and 4.

Configuration 3

According to comparison, shown in Table 4.13, this configuration matches perfectly the SPD goal only for Scenario 3.

Configuration 4

According to comparison, shown in Table 4.13, this configuration matches the SPD goal for Scenario 2, 3 and 4.

4.3.2 Analysis

Choice for scenarios

The main point for considerations while choosing the configurations for scenarios is that the MM approach does not recommend going for highest security value in the case if there are other options. Reasons to it are described in the section 3.1.9. The other main point is that it is necessary to choose such a configuration, what would guarantee preservation the security attributes, separately defined for each scenario in section 4.2.7.

For Scenario 1:

The Scenario 1 used for the deployment of AMM system for the most of the time, i.e. the system is in a steady state, normal drift.
The green label assignment yields that this configuration of a system satisfied the preservation of security objectives defined for this scenario.
Because of that other alternatives does not yield green label, the choice for Scenario 1 is Configuration 1.

For Scenario 2:

Having compared configurations 1, 2 and 3, the researcher concluded that Configuration 2 is the best choice for this scenario.

Justification:

Table 4.14: Parameters comparison. Scenario 2 in focus.

			Conf. 1	Conf.2	Conf.4
Subsystem	**Component**	**Metric**	**Parameter**	**Parameter**	**Parameter**
Concentrator		BackUp	Provided,N	Provided,Y	Provided,Y
Link SM-HE		BackUp	Provided,N	Provided,Y	Provided,Y
Smart Meter	OS	Session	Session establishing,N	Session establishing,Y	Session establishing,N
Smart Meter	Interface A2	Node auth.	In use,Y	In use, Y	In use, N
Smart Meter	Phys.prot.	EM protect.	Applied,Y	Applied,Y	Applied,N
Smart Meter	Phys.prot.	Temperature	Applied,Y	Applied,Y	Applied,N
Smart Meter	Phys.prot.	Humidity	Applied,Y	Applied,Y	Applied,N
Head-End		Antivirus Update	Least once every 24hrs,Y	Least once every 24hrs,Y	Least once every 24hrs,N
Head-End		Patching	Within 24hrs,Y	Within 24hrs,Y	Within 24hrs,N
Wireless Mesh		QoS	Used,N	Used,N	Used,Y
SPD system			**60**	**69**	**62**

The table above shows that redundancy is added only for Configuration 2 and 4 giving lower chance for choosing Configuration 1. Secure session established in only Configuration 2, thus lowering chances for choosing Configuration 1 and 4. The authentication for messages which are going to be transferred hop by hop towards concentrator is in use only in Configuration 2, thus increasing the chances for choosing this configuration. Physical protection almost completely switched off in Configuration 3, what have a downgrading impact on physical DoS protection of a Smart Meter. Antivirus updates and patching assist in keeping the SM in secure state during a daily drift. QoS feature is not of high importance for Scenario 2. After considering parameters configuration, the rational choice for Scenario 2, the Meter Reading Services is Configuration 2.

For Scenario 3:

Having compared configurations 2, 3, and 4 the researcher concluded that Configuration 3 is the best choice for this scenario.

Justification:

Table 4.15: Parameters comparison. Scenario 3 in focus.

			Conf. 2	Conf.3	Conf.4
Subsystem	**Component**	**Metric**	**Parameter**	**Parameter**	**Parameter**
Concentrator		BackUp	Provided,N	Provided,Y	Provided,Y
Link SM-HE		BackUp	Provided,N	Provided,Y	Provided,Y
Smart Meter	OS	Session	Session establishing,Y	Session establishing,Y	Session establishing,N
Smart Meter	Interface A2	Node auth.	In use,Y	In use, Y	In use, N
Smart Meter	Phys.prot.	EM protect.	Applied,Y	Applied,Y	Applied,N
Smart Meter	Phys.prot.	Temperature	Applied,Y	Applied,Y	Applied,N
Smart Meter	Phys.prot.	Humidity	Applied,Y	Applied,Y	Applied,N
Head-End		Antivirus Update	Least once every 24hrs,Y	Least once every 24hrs,Y	Least once every 24hrs,N
Head-End		Patching	Within 24hrs,Y	Within 24hrs,Y	Within 24hrs,N
Wireless Mesh		QoS	Used,N	Used,Y	Used,Y
SPD system			**69**	**79**	**62**

Note: The Configuration 3 is the Best Case configuration, because of only minimum values for criticalities are deployed.
For Scenario 3, the choice of Configuration 3 is justified because of for this scenario, requirements to preservation of the security objectives are put at highest level. This fact cuts off the other configuration choices.

For Scenario 4:

Having compared configurations 1,2, and 4, the researcher concluded that Configuration 4 is the best choice for this scenario.

Justification:

Table 4.16: Parameters comparison. Scenario 4 in focus.

			Conf. 1	**Conf.2**	**Conf.4**
Subsystem	**Component**	**Metric**	**Parameter**	**Parameter**	**Parameter**
Concentrator		BackUp	Provided,N	Provided,Y	Provided,Y
Link SM-HE		BackUp	Provided,N	Provided,Y	Provided,Y
Smart Meter	OS	Session	Session establishing,N	Session establishing,Y	Session establishing,N
Smart Meter	Interface A2	Node auth.	In use,Y	In use, Y	In use, N
Smart Meter	Phys.prot.	EM protect.	Applied,Y	Applied,Y	Applied,N
Smart Meter	Phys.prot.	Temperature	Applied,Y	Applied,Y	Applied,N
Smart Meter	Phys.prot.	Humidity	Applied,Y	Applied,Y	Applied,N
Head-End		Antivirus Update	Least once every 24hrs,Y	Least once every 24hrs,Y	Least once every 24hrs,N
Head-End		Patching	Within 24hrs,Y	Within 24hrs,Y	Within 24hrs,N
Wireless Mesh		QoS	Used,N	Used,N	Used,Y
SPD system			**60**	**69**	**62**

This scenario is considered to be a case when the entire wireless mesh network, to which the Smart Meter belongs, is under outage, thus every SM in the mesh start using battery power.

In this case the availability and minimum transmission delay of a message is paramount.

The other main point is that the battery power needs to be used rationally. The Configuration 4 supports these objectives. The physical protection options are almost totally switched off, except from tampering option. Antivirus updates and patching are not necessary under those circumstances. On the contrary, the QoS support and the

redundancy provision are essential features. For countering the absence of the secure session establishing and absence of traffic authentication, originating from an SM, the following solution is proposed. Each SM obtains a set of pre-calculated encrypted emergency messages from HE in advance, where the integrity and freshness are taken into account. The mandatory fields in those messages are the ID of an SM and type of the event.
Satisfying the requirements to preservation of the security attributes and keeping the wireless mesh network in operational state and in the same time is not trivial task. Additionally, the usage of resources in an SM must be kept low in order to extend the battery usage time.
For this reason, the Scenario 4, Outage Detection and Restoration, is being the most interesting case to evaluate.
Table 4.17 reviews the set of metrics and parameters for Configuration 4. The explanations of choosing certain configuration for a parameter are given.

Table 4.17: Set of parameters. Configuration 4.

index	Metric	Parameter	Reason
1	1. Secure Boot	Applied,Y	Cannot be modified, system design
2	2.Secure Memory	Applied,Y	Essential for all the scenarios
3	3. Antivirus SW	In use,Y	prevents intrusion of malware
4	5. Cryptography	112bits,Lower	May be compensated by using emergency messages
5	6. Logging	In use,Y	Logging feature is always on, requirement
6	1. Mesh Authentication	In use,Y	Prevention of fake node join
7	2. Node Authentication	In use,N	Not essential due to use of emergency msg.
8	3. Session	Session establishing,N	Save processing power
9	4. Jamming Detection	Implemented,Y	Prevention of an attack
10	5. DoS Prevention	Implemented,Y	Prevention of an attack
11	Interface A3	switched off	Not necessary to use under the outage
12			
13	1. Accessibility	Applied,Y	Prevention of malicious intrusion via A4
14	2. Equipment	Applied,Y	Prevention of malicious intrusion via A4
15	3.Crypto Protection	Applied,Y	Prevention of malicious intrusion via A4
16	1. EM Protection	Applied,N	Switched off, saving battery power
17	2. Temperature	Applied,N	Switched off, saving battery power
18	3. Humidity	Applied,N	Switched off, saving battery power
19	4. Tampering	Applied,Y	Prevention of malicious intrusion via opening
20	1. Antivirus Update	Least once every 24hrs,N	Reducing unnecessary in this event data traffic
21	2. Patching	Within 24hrs,N	Reducing unnecessary in this event data traffic
22	3. Compromisation	Greater than 72hrs,Y	Essential for AMM secure functioning
23	4. Intrusion	Applied,Y	Prevention of malicious intrusion
24	5.Access Control	Applied,Y	Essential for AMM secure functioning
25	1. BackUp	Provided,Y	Provision of redundant path to HE in this event is essential
26	2. Authentication Limit	Applied,Y	Essential to prevent malicious intrusion
27	3. Cryptography	112bits,Higher	Essential to prevent malicious intrusion
28	1. Path Cost	Simple	Cannot be modified, system design
29	2. QoS	Used,Y	Packet prioritization is essential in this event
30	1. BackUp	Provided,Y	Redundancy provision is essential in this event

For Configuration 4, a minor modification was made - switching completely off the interface A3. Usage of this interface is not essential in the event of outage. Recalculation the SPD system yield value *59* , what totally satisfies the SPD goal for Scenario 4.

General considerations

Evaluation of the retrieved configurations vs. SPD goal shows that in some cases better match can be obtained if the security level is decreased by changing parameters configuration.

Although, there are reasons for not to modify the configuration of some components to get security system's level decreased. Just to consider a case, when the entire wireless mesh is the subject of deliberate switching off of power, e.g. cutting the power line. If the configuration is changed to obtain the lower value for the security, the system might become vulnerable to malicious intrusion. Just to take as an example, metrics Mesh Authentication and DoS Prevention. Lowering security for components those metrics belong to, might give an intruder a chance to join a wireless mesh as a legitimate node. Change of configuration to a lower value for security for components described through metrics Accessibility and Equipment might give a chance for an intruder to install malicious software into SM. In this case, the SM can fall into a state where it might be configured and controlled by a malicious entity.

Additionally, there were detected that some of the parameters cannot be reconfigured rapidly. It applies in particular to the feature secure boot. This feature is inbuilt rigidly into the hardware of the MCU. However, there are no reasons to change its configuration. The second non-reconfigurable parameter is the routing table calculation scheme based on the number of hops. However, for making a transition to some other scheme for routing table calculation, a decision from the utility is needed, in making an investment first and then for upgrading.

Worst component

Worst component evaluation is done only for Subsystem SM, as Smart Meter is the main focus for the current research. Evaluation was executed through comparing the contribution of every SM component into overall security level for the SM. The formula (2), when used to calculate criticality value for a Subsystem SM, gives an expression (M indicating Multi Metrics analysis):

$$C = \sqrt{W_{OS}*(M_{OS})+W_{A2}*(M_{A2})+W_{A3}*(M_{A3})+W_{A4}*(M_{A4})+W_{PP}*(M_{PP})}\ ,$$

where W_i indicates a normalized weight for respectful component.

The expression above contains five elements, each of them corresponds to particular component in the SM. Thus, evaluation of the worst component for Subsystem SM were done by comparing the numerical values, obtained by executing the MM analysis on each component and multiplying the resulting value by normalized weight of corresponding component. The results of evaluation for every scenario reviews Figure 4.11 below (PP- Physical Protection).

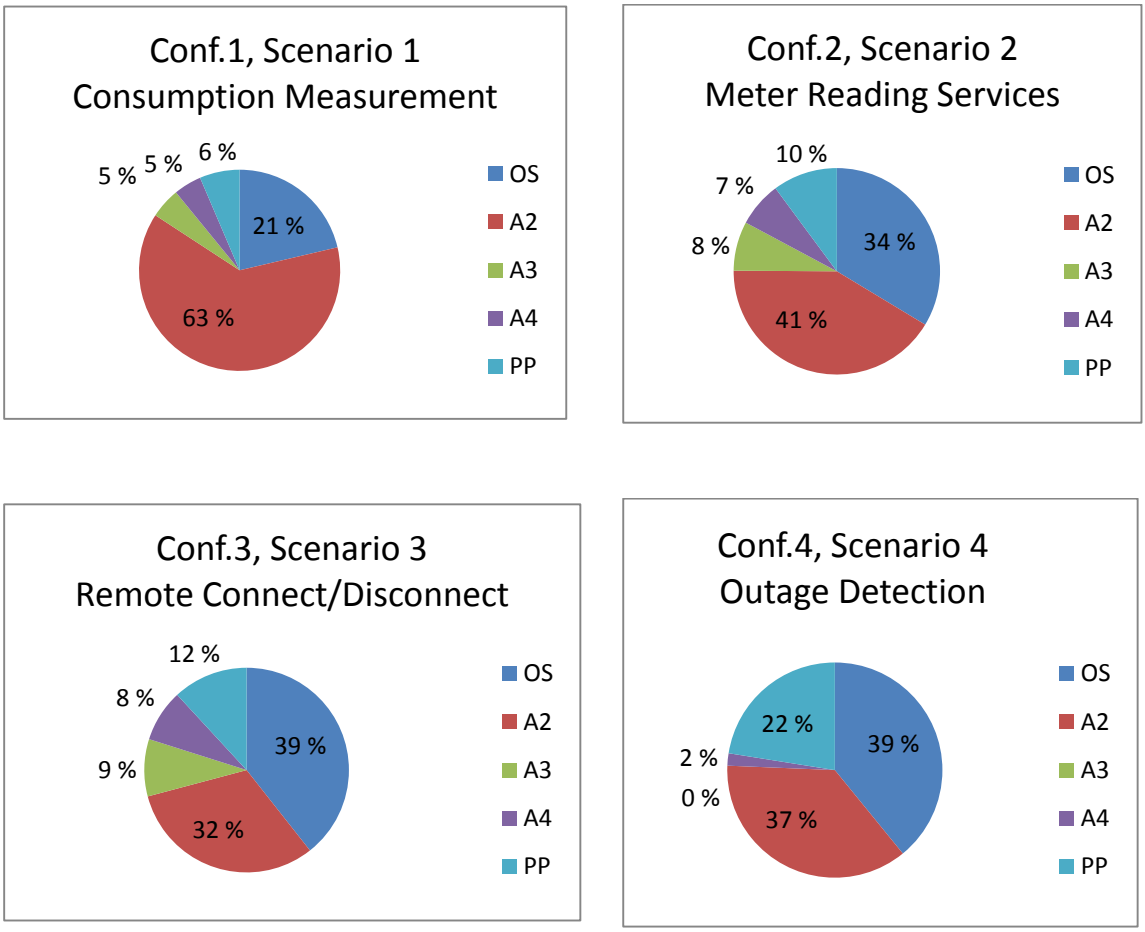


Figure 4.11: Contribution of components in Smart Meter.

Worst components of an SM might differ for various scenarios:

- Smallest contributors are components Interface A3 and A4
- Greatest contributors are components Interface A2 and OS
- Component Physical Protection contributes most for Outage Detection and Restoration scenario where lowering its security level is acceptable.

Regarding the Component OS, the configuration described by metric Cryptography is the greatest contributor in this component. The configuration of a parameter for this metric was made by choosing criticality value to be of the highest for Scenario 4, Outage Detection and Restoration.
Another greatest contributor for component Interface A2 is the configuration described by metric Session, which has worst configuration parameters for scenarios Remote Connect/Disconnect of Meter and Outage Detection and Restoration.
According to MM approach guidelines, the value of weight cannot be altered, thus if the interest lies in obtaining a lower value for criticality, the parameters in the underlying structure must be configured of having a lower value for criticality. However, there was made an observation that it is not always feasible to go for lowest level of criticality or vice versa, for highest level of security. Each scenario requires its own choice for configuration of parameters, thus having worse security level does not imply that chosen configuration is wrong, it is just works in that way.

Proposal for improvements

During considerations of an Aidon AMM system following insecure features were identified:

- Presence of routing traffic
- Usage of non-protected by crypto-means traffic originated at SM

Routing traffic for mesh installation cannot be eliminated completely. However, there are proposals to improve this situation. One way of doing this is to make a transition

from dynamical routing to a static routing scheme which would increase security level, but at the same time, it might downgrade the dependability level (manual work, maintenance, reliability). Another way is to configure and control routing from the Head End system. This solution requires additional research to evaluate capabilities of the AMM system to process an increased amount of interactions of SMs with the Head End. The creation of routing tables based on a hop count described by metric Path Cost can be changed to more complex evaluations, which takes into account e.g. bandwidth and latency. Such a solution requires additional research to evaluate the capabilities of SM to process an increased amount of data. The next proposal for a solution to increase security in case of usage routing protocols is the implementation of VM machines inside the SM, thus dividing processing of insecure routing traffic and secure routed/originated at SM traffic. This solution requires additional research to evaluate SM processing capabilities. More careful attention might be paid to designing the wireless mesh such that the number of hops to reach a concentrator is reduced as much as possible. The way of doing it might be a careful choice for placing of a concentrator e.g. in the center of a mesh installation.

There were considered only two ways of transmitting data traffic originating from SM, either by establishing secure e.g. SSL/TLS session or as plain data. The possible changes might be made by extending the option for metric Session, secure session vs. non-protection. It might be done by including the usage of lightweight cryptographic protocols. In this way, the number of configuration parameters for the metric Session (comp. OS, Subsystem 1, SM) might be extended as shown in Table 4.18.

Table 4.18: Extension of parameters for metric Session.

	Parameter			Parameter			
Metric	Secure session	Non-secure	→	Secure session	Lightweight Protocol 1	Lightweight Protocol 2	Non-secure
Session Cs	15	90		15	e.g. 40	e.g. 70	90

Such an extension requires that one considers the influence on processing time and battery power consumption. The plain message transmission was intended to be

used only in case of an emergency event, such as an outage. Another solution, mentioned previously, might be a use of encrypted emergency messages which are pre-calculated, and where integrity and freshness are taken into account. All mentioned solutions can be a subject for additional research.

Benefits for an owner of an AMI system or utility in using the MM approach

The owner of an AMI system or a vendor might use the MM approach to evaluate the security level of an entire system. The results for interactions between single SM and HE under specific deployed scenarios need to be scaled. The scaling will include multiple SM devices, multiple wireless mesh networks and other types of installations, such as those that are used for multi-story buildings and standalone houses. MM approach provides means for making such scalings.

The core of the MM approach is the set of metrics.

The proposal for defining a set of metrics, which will reflect the preservation of security objectives, is that it should be done by a board of experts in the field.

In this way, the resulting evaluations will to be unbiased by individual opinion.

The system's security level will be downgraded as time passes, as shown in Figure 4.12. This yields the necessity of making corrections for criticality values.

After recalculations the system's security level, the result is compared with the security goal.

If necessary, patching/updates/upgrades of software can be issued as indicated by blue errors. Thus, it can bring back the security to the required level.

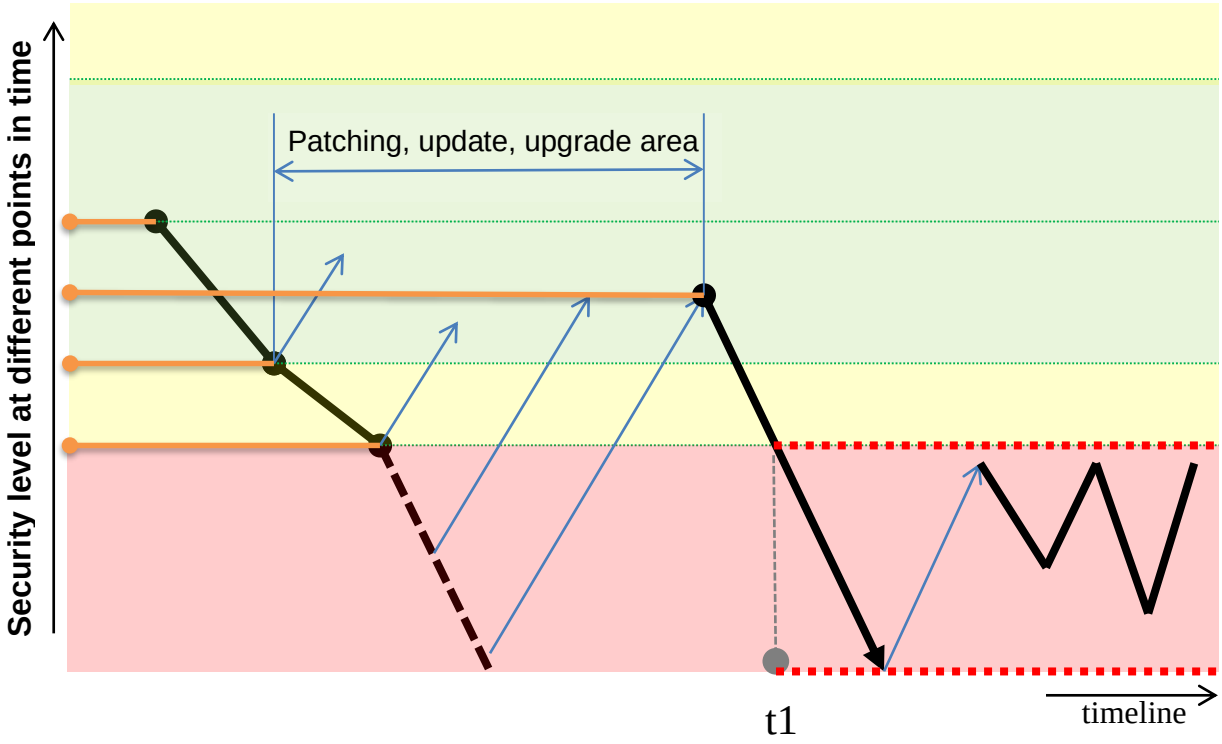


Figure 4.12: Timeline of security level. Green, Yellow and Red zones reflect MM approach's color representation.

Although, at some point in time, represented as *t1* in the figure above, those corrections would not provide a required security level, causing the security of the system to deviate in the red zone. At this time point, the decision to exchange/upgrade some of the hardware components or redesign a whole/part of a system should be made. On that account, the Multi Metrics approach shows itself to be a useful tool which assists in predictability analysis of an already deployed system.

5 Discussion and Conclusion

The purpose of the current research was to investigate an Aidon AMM by using an already developed Multi Metrics approach as a tool. The goal is to assess the security level of an AMM.

The researcher was also sought to determine how different operational scenarios put their requirements on security levels and how resilient the system was at adjusting its configuration to satisfy those requirements.

The main task before the researcher was to build up the set of metrics for components with the focus on a smart meter. This set of metrics had to be created such that it would reflect the preservation of a certain number of security objectives.

Usage scenarios have different requirements for the preservation of the following security objectives:

- Confidentiality
- Integrity
- Availability

Thus, the SPD goal for a system varies from scenario to another.
An attempt was made to adjust the configuration of the system to keep security level satisfying the SPD goal for the respective scenario. Such adjustments allow freeing resources and saving battery life, such as for Outage Report scenario. Another reason for adjustments was that if the security level is kept at unnecessarily high level, the dependability level is reduced. This happens because security and dependability are inversely proportional to each other. Thus, one more reason for choosing an SPD goal for Consumption Measurement as SPD = (50,p,d) is that it would keep both security and dependability at the highest possible level at the same time. This is imperative because for most of the time the system is supposed to be used under Consumption Measurement scenario.

On the other hand, the other security objectives:

- Authentication
- Accountability
- Repudiation

should be taken into account as well. The preservation of those objectives is mandatory in every usage scenario. This restricts the possibilities of adjustment of configuration for parameters. Thus, obtaining lower values of security cannot be done in the full scale. Those contradictions have been reviewed in the result analysis.

An interesting moment for discussion is the compromisation of a SM. Would it be possible to extract valuable information from it, for example by executing a side-channel attack. In this thesis, an assumption is made that it is necessary to evaluate this possibility. Thus, the metric Compromisation were introduces, which takes into account the timeframe between compromisation discovery of a smart meter and necessary measures taken. One of those measures can be a blacklisting of a private key, belonging to compromised device.

Another interesting point to discuss is the mechanism of acknowledgments.
All traffic between single SM and HE assumed to be between two endpoints which confirmed authenticity to each other, i.e. SM to HE as well as HE to SM. All data messages at application level, initiated at some endpoint are to be acknowledged, i.e. an ACK is sent confirming receiving of the message at an application level.

5.1 Limitations

Although the MM approach is used to define a security level of SuI which gives a coherent picture of what the current level of security is, there were several limitations to the study.

For internal interfaces such as A0 and A1, the full functioning and assessment of their influence on the whole security level of an SM were not conducted. It was assumed that those interfaces do not alter secure operations of an SM. The possibility of an intrusion for interface A0 from the side of power supply lines, by e.g. using high-frequency signal was not considered.
The possibility of reading light impulses from Energy Pulse LED, which shows current electricity usage, on the front side of Aidon SM with malicious intentions, was not considered.
There were no considerations of time synchronization aspect of SMs.
Accurate time synchronization is needed to:

- Ensure quality of error and event logs used for diagnosis;
- Accurately estimate the state of system based on its time stamped measurements;
- Develop control algorithms that can apply corrective action in a timely manner (Li-Baboud, 2012).

According to requirements of NVE, all the SMs have to be synchronized with Statnett NTP server. The greatest problem for time synchronization is that due to multipath propagation of a signal in the wireless mesh installations, the time synchronization message might arrive at different SMs with a different delay.
The operating system for a microcontroller unit was not investigated deeply or with respect to all of the aspects. A certification of the OS is usually done by an appropriate authority such as SERTIT (Norway), which defines the Evaluation Assurance Level (EAL) of the OS according to Common Criteria (CC) standard (ISO/IEC 15408).
There were no considerations of possible usage of the Hardware Security Module (HMS) for secure processing of crypto material. The HMS devices, specially built for use in concentrators do exist on the market. Consequently, the results validity might not be in line with reality.
Another limitation is that the possible values for parameters described through metrics were chosen out of constrained set. This set contains only two values. Such organization narrows the choice of possible configurations. Extending the number of values for metric's parameters, as shown in the result analysis, will yield more

accurate security evaluations and more flexible configurations. The next limitation is that underlying radio technology issues for the wireless mesh, which uses the wireless technologies such as ZigBee and Wi-Fi and the link between a concentrator and a Head End, which implemented using the mobile communications such as 2G, 3G, and 4G, were not taken into considerations. It is known, that wireless technology used in different IoT infrastructures can be of heterogeneous types, and it is a separate issue, to make them work smoothly together hand in hand. Especially it is related to a concentrator which is an intermediary device between the wireless mesh and the Head End.

Due to the limited scope of this thesis, there were no possibilities to consider key management issues for an AMI, to consider the layered protection of data exchanged between the SM and HE and another important feature of how the SM and HE notify each other about being up and running.

The above limitations affect the validity of the results. With better access to Aidon AMM documentation and more detailed description of SM functioning, the results may have more accurately reflected the assessed security level.

5.2 Recommendations for Future Research

Based on the results of the study, there are several recommendations for future research. First, some of the limitations outlined in this study may be minimized or eliminated by conducting a complex research on OS issues and the proposal is to make it as a dedicated study subject. An outcome of such research might be metrics which would allow assessing an OS in a more detailed way, thus leading to a more comprehensive analysis of an OS.

The next proposition for research is to determine if it is feasible to establish an SPD goal for components as well. This can follow to more accurate choice for establishing the set of metrics and parameters for components. It would follow to extension of original version of the MM approach.

Furthermore, the result analysis showed that there are dependencies between reducing processing power and saving battery lifetime and at the same time it is needed to keep whole wireless mesh in operational and secure state. Specially, it is highly related to Outage Detection and Restoration scenario. This thesis has come up with the proposal of sending a pre-calculated emergency message. Another option might be to enter a sleep/hibernate mode for SM, but such a solution is rather trivial. The subject of the future research can be to find solutions for breaking those dependencies without harming the security of a system and at the same time satisfying the requirements of the MM approach.

Another proposal for future research might be to find a methodology which does not require manual work to define the set of metrics for components, the criticality, and weight values. The subjectivity feature of the MM approach thus might be lowered.

5.3 Conclusion

Two major conclusions can be made based on the results of this study.
The MM approach was specially developed to allow assessment of security level for embedded systems. The general scheme for deployment of embedded systems in IoT is shown in Figure 5.1 below.

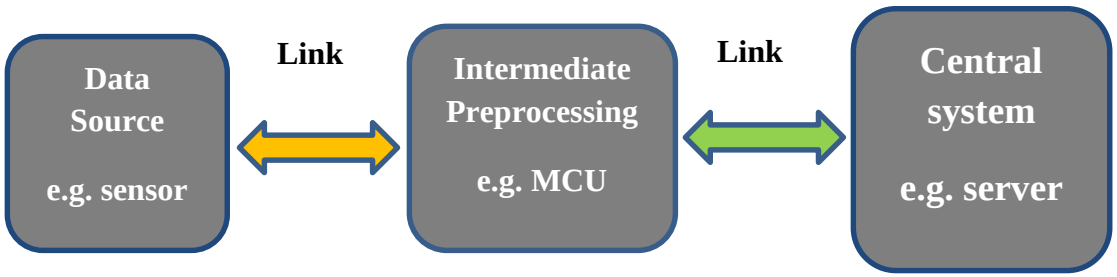


Figure 5.1: Deployment of embedded system in IoT.

The main point in the picture above is that it yields that different links can be built on various heterogeneous networking technologies.
As for the first conclusion, the work done in current research confirmed its full applicability in the assessment of the security level of a given SuI, the Aidon AMM by:

- Easiness of subsystems and components identification
- Easiness of scenarios recognition
- Easiness of executing calculations
- Moderate difficulty of SPD goal establishing
- Moderate difficulty of metrics establishing

The special features of the MM approach were highlighted and a proposal was made for a possible extension.
Three main features of the MM approach:

- Highly subjective
  - ✓ Possible alternative is to set up the board of experts that

would identify metrics and values for criticality and weighs thus making it more objective

- Highly skeptical to obtaining values of absolute security (100) or absolute weight (100)
  - ✓ The positive feature, the security level always has a trend of being downgraded during the time. Requires regular re-evaluations of the results

- Highly scalable and agile
  - ✓ Allows adding/removing subsystems and components

The second conclusion is that the Aidon AMM system is showed to be flexible system when it comes to possibility of its reconfigurations and be a very secure during operations.

The Aidon AMM system was analyzed with a focus on Smart Meter, and a proposal for a set of metrics for components has been made with some limitations. The security level of an Aidon AMM system was calculated for specific configurations. It was shown that there are configurations that satisfy the requirements of the SPD goal for considered scenarios. There were made justifications of why one configuration should be given priority over other configurations in the case if multiple configurations satisfy the established SPD goal. There were shown how and why the set of defined metrics is used to cover the requirements of security attributes. There were made justifications why different scenarios have various relations with those attributes in specific scenarios. The major finding of work achieved in this thesis was that it outlined the ways of thinking, any researcher or user may adopt when he has a reach choice of configurations for a usage scenario, but when one is obliged to choose that very configuration which would not put in jeopardy the operations of an AMI.

References

Administration, U. S. E. I. (2016, 19.12.2016). Electricity Explained. Retrieved from https://www.eia.gov/Energyexplained/index.cfm?page=electricity_delivery

Aidon. (2017a, 2017). Aidon Efficient Communications. Retrieved from http://www.aidon.com/our-solutions/efficient_communication/

Aidon. (2017b, 2017). Head-End System - Aidon. Retrieved from https://www.aidon.com/our-solutions/head-end-system/

Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine, 3*(5), 34-41.

AMS for Smart Strøm Østafjells. ([s.n]). *Bilag 1 Kundens kravspesifikasjon*. [s.l]: Smart Strøm Østafjells.

Ashraf, U. (2010). *Quality of service and routing in wireless mesh networks.* INSA de Toulouse.

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing, 1*(1), 11-33.

Balmert, D., Grote, D., & Petrov, K. (2012). Development of best practice recommendations for smart meters rollout in the energy community. *KEMA*.

Barker, E. (2016). NIST Special Publication 800-57 Part 1 Revision 4—Recommendation for Key Management (Part 1: General): National Institute of Standards and Technology, US Department of Commerce.

Benioef, M. R., & Lazowska, E. D. (2005). *Cyber Security: A Crisis of Prioritization: Report to the President: President's Information Technology Advisory Committee*: Diane Publishing Company.

Boyer, W., & McQueen, M. (2007). *Ideal based cyber security technical metrics for control systems.* Paper presented at the International Workshop on Critical Information Infrastructures Security.

Buchla, D. M., International Organization for, S., & International Electrotechnical, C. (2012). *IT-sikkerhet : et av utvalg standarder i NS-ISO/IEC 27000-serien*. Lysaker: Standard Online.

Cisco. (2015, 2015). Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/iot-system-security-wp.pdf

Dhanjani, N. (2015). *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*: O'Reilly Media, Incorporated.

Fayyad, S., & Noll, J. (2015). Components Interconnection Consideration In Multi Metrics Approach.

Frantti, T., Hietalahti, H., & Savola, R. (2013). A Risk-Driven Security Analysis and Metrics Development for WSN-MCN Router. *2013 International Conference on Ict Convergence (Ictc 2013): Future Creative Convergence Technologies for New Ict Ecosystems*, 342-347.

Garitano, I., Fayyad, S., & Noll, J. (2015). Multi-metrics approach for security, privacy and dependability in embedded systems. *Wireless Personal Communications, 81*(4), 1359-1376.

Grid, N. S. (2010). Introduction to NISTIR 7628 guidelines for smart grid cyber security. *Guideline, Sep*.
Hahn, A., & Govindarasu, M. (2011). Cyber attack exposure evaluation framework for the smart grid. *Ieee Transactions on Smart Grid, 2*(4), 835-843.
Hjelmgaard, K. (2016, 2017). 'Internet of Threats': Q&A with Eugene Kaspersky - USA Today Retrieved from http://usa.kaspersky.com/about-us/press-center/in-the-news/2014/internet-threats-qa-eugene-kaspersky-usa-today
its-wiki.no. (2017, n.d.). IoTSec:Smart Meter Connectivity Retrieved from http://its-wiki.no/wiki/IoTSec:Smart_Meter_Connectivity
Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks, 20*(8), 2481-2501.
Li-Baboud, Y.-S. (2012, 08.2016). Precision Timing for Smart Grid Systems Retrieved from https://www.nist.gov/programs-projects/precision-timing-smart-grid-systems
Liu, V., Tesfamicael, A. D., Caelli, W., Sahama, T., & Ieee. (2015). Network Security Metrics and Performance for Healthcare Systems Management. *2015 17th International Conference on E-Health Networking, Application & Services (Healthcom)*, 189-194.
LLC, L. R. (2013, November 2013). An Introduction to the Internet of Things (IoT). Retrieved from http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
Lovdata. (2017, February 03,2017). Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. Retrieved from https://lovdata.no/dokument/SF/forskrift/1999-03-11-301/KAPITTEL_4#KAPITTEL_4
Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-driven risk analysis: the CORAS approach*: Springer Science & Business Media.
Nicol, D. M. (2005). Modeling and simulation in security evaluation. *IEEE security & privacy, 3*(5), 71-74.
Noll, J., Garitano, I., Fayyad, S., & Abie, H. (2014). Measurable security, privacy and dependability in smart grids. *Journal of Cyber Security and Mobility, 3*(4), 371-398.
NVE. (2011, 06.05.2011). **Avancerte måle- og styringssystemer**. Retrieved from http://webfileservice.nve.no/API/PublishedFiles/Download/200701944/418378
NVE. (2015, 02.03.2017). Smarte Strømmålere (AMS). Retrieved from https://www.nve.no/Media/5403/du-bestemmer-hvem-som-skal-f%C3%A5r-data-fra-smarte-str%C3%B8mm%C3%A5lere.pdf
Sen, S. K., Dey, S., & Saha, I. (2014). An Innovative Approach to Devise Security Matrix to Measure Impact of Attack Vectors in Cloud Networks. *International Journal, 2*(4).
Strategy, N. M. G. (2008). Advanced metering infrastructure. *US Department of Energy Office of Electricity and Energy Reliability*.
SynapseIndia. (2017, n.d.). Internet of Things (IoT) – Unlocking the Infinite Possibilities. Retrieved from https://www.synapseindia.com/internet-of-things.html
U.S. Department of Energy. (2008, 2008). The Smart Grid: an Introduction. Retrieved from https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf
Varaiya, P. P., Wu, F. F., & Bialek, J. W. (2011). Smart operation of smart grid: Risk-limiting dispatch. *Proceedings of the IEEE, 99*(1), 40-57.
Vasilevskaya, M., & Nadjm-Tehrani, S. (2015). *Quantifying risks to data assets using formal metrics in embedded system design.* Paper presented at the International Conference on Computer Safety, Reliability, and Security.

Wang, L. Y., Singhal, A., & Jajodia, S. (2007). Toward Measuring Network Security Using Attack Graphs. *Qop'07: Proceedings of the 2007 Acm Workshop on Quality of Protection*, 49-54.

Wermann, A. G., Bortolozzo, M. C., da Silva, E. G., Schaeffer-Filho, A., Gaspary, L. P., & Barcellos, M. (2016). *ASTORIA: A framework for attack simulation and evaluation in smart grids.* Paper presented at the Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP.

Whitehouse, O. (2014). Security of Things: An Implementers' Guide to Cyber-security for Internet of Things Devices and Beyond. *NCC Group*.

Wiki, I. o. T. (2016). Understanding Internet of Things. Retrieved from http://internetofthingswiki.com/internet-of-things-definition/

Wikipedia. (2015, June 02,2017). December 2015 Ukraine power grid cyber attack. Retrieved from https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyber_attack

Wikipedia. (2017, 09.02.2017). Privacy. Retrieved from https://en.wikipedia.org/wiki/Privacy

Appendixes

Appendix A

NVE requirements for AMI

Excerpt from (AMS for Smart Strøm Østafjells, [s.n])

Functional requirements

Section 3.0 on enforcement of AMM system must:

- register and store measurement with the frequency between 1 and 4 times per hour,
- communicate with external equipment via standard interfaces,
- do not lose measurements in case of the outage,
- send and receive information about tariff, price, and errors,
- be secured against misuse,
- be able to measure energy in 4 quadrants,
- be able to forward measurements to Distribution Service Operator (DSO) and the end consumer.

Section 3.1 on enforcement of Measurement, it must:

- have a certain label, containing ID of Metering device, ID of location, type of energy, unit of measure,
- be automatically forwarded,
- functionality in AMM system to forward measurements from several ESDs,
- be automatically repeated in case of lost transmission.,
- be temporarily stored at Head-End System,
- be manually or automatically deleted from Head-End System upon acknowledgment from DSO,
- have the functionality of automatically forwarding data between Head-End System and DSO.

Section 3.2 on enforcement to Power Quality have to:

- register outages,
- register deviation from nominal values of delivered electrical energy.

Section 3.3 on enforcement to Network (Smart Grid) and consumer service:

- to be able to switch ON/OFF the ESD controlled facility from DSO
- to be able to limit electrical energy use at the facility controlled by ESD,
- to be able to register residual current error,
- to be able to register and to forward to Head-End events such as short circuit, open door, internal water overflow, internal high temperature and so on,
- to be able to counter "jamming" of Head-End System.

Section 3.3 on enforcement to Network (Smart Grid) and consumer service:

- to be able to switch ON/OFF the ESD controlled facility from DSO,
- to be able to limit electrical energy use at the facility controlled by ESD,
- to be able to register residual current error,
- to be able to register and to forward to Head-End events such as short circuit, open door, internal water overflow, internal high temperature,
- to be able to counter "jamming" of Head-End System.

Section 3.4 on enforcement of Facilitation of value-added services:

- to have the functionality of connection extra equipment to ESD,
- to have the functionality of routing data from Head-End and ESD to extra equipment.

Technical requirements

Section 4.1 on enforcement to ESD to have:

- unique identity number and bar code,
- the functionality of self-diagnosing inbuilt in ESD,
- the functionality of switching ON/OFF all or one of the phasor.

Section 4.2 on enforcement to Interface:

- to have an internal serial interface A1.

System requirements

Section 5.1 on general rules for AMM:

- to the lifecycle of components of minimum 18 years,
- not to require the exchange of software for Head-End System during 18 years, but still, have the functionality to update software,
- to have most of “intelligence” in Head-End System.

Section 5.2 on enforcement to System stability:

- to be able to detect communication problems between Head-End and ESD,
- to have automatic upstart of a component after downtime, no data loss allowed,
- to have mechanism for detection of faults in communications,
- to have the functionality of exposing attempts and generating an alarm in case of misuse from inside and outside AMM.

Section 5.4 on enforcement of Time function:

- to have synchronization of time inside AMM system devices with Statnett NTP servers.

Section 5.5 on enforcement of Response time:

- to provide technical solutions for keeping latency inside of AMM systems's communications, limited to certain values.

Section 5.6 on enforcement to Head-End System:

- to have mandatory logging of operations related to security as write, read, change of access rights.

Section 5.10 on enforcement to Security for processing of information and user registration:

- not allowing for manual data exchange inside of AMM system,
- to have the functionality of alarm rising in the case of data manipulations.

Section 5.11 on enforcement to the Remote control of parameters and software upgrade:

- to support of remote update of software for ESD from Head-End.

Section 5.12 on Scalability:

- to allow scaling AMM system up to 200.000 consumers.

Requirement to cost effective operations and maintenance

Section 7.2 on enforcement of Requirements to future changes and scalability:

- to have the functionality of changing mobile operator without changing a SIM card.

Requirements for security

Section 8.1 on enforcement to Privacy:

- Head-End System must keep personal information protected.

Section 8.2 on enforcement to Authentication:

- to have authentication and authorization mechanisms for every unit inside of AMM and for extra equipment implemented in advance,
- to have implemented access control as:

    - ✓ Identity-Based Access Control
    - ✓ Role Based Access Control
    - ✓ Organization Based Access Control

- to not allowing new unit connection to AMM without being authenticated and authorized,
- to keep the principle of least privilege,
- to allow of usage passwords of a certain strength,

- to provide access to the measurements in ESD only upon authorized request,
- to have authentication and authorization mechanisms for external equipment,
- to allow handheld equipment (field equipment) access to ESD only after it has been authorized by AMM (Head-End) and after the user has been authenticated and authorized,
- to control of Security Certificate (SA) each time external equipment unit connects to AMM,
- to limit the functionality of external equipment unit to a certain set of tasks
- to have the functionality of removing authentication and authorization of external equipment unit from Head-End System,
- to have the functionality of controlling and detection of changes in software and data by performing integrity checks of AMM system. Performing integrity check of software is done upon each start, update, execution,
- to provide physical and logical securing of the unit against unauthorized update and alternation of software,
- to approve and test changes in software,
- to provide alarm rising in the case of integrity check failure,
- to provide functionality for units in AMM in checking of all requests and commands for validity. The requirement to commands is to have correct format and authenticated and authorized source,
- to use SA for verifying command execution.

Section 8.3 on enforcement to Robustness against malware and intrusion:

- to mandatory usage of protection and recognition of malicious software systems.

Section 8.4 on enforcement to Encryption:

- to mandatory usage of encryption,
- to encrypt keys and passwords,
- to keep passwords and keys inside of AMM system only in encrypted form,
- to not allowing of obtaining a key or password from AMM system,
- to keep all communication between ESDs, Head-End system inside of AMM in a safe way,
- to not allowing sniffing, tampering with data and so on,
- to implement encryption mechanisms to ensure end-to-end encryption, i.e. encryption and decryption must occur only in communicating end points.

Section 8.5 on enforcement of General requirements to security:

- to ensure that failure of a single component must not influence the security functionality of AMM,
- to ensure that deactivated functionality does not influence the security functionality of AMM,
- to ensure that AMM has the functionality of being upgraded with new upcoming security mechanisms,

- to ensure that AMM is ready to counter malicious attempts at any time,
- to oblige the supplier of AMM to warn DSO in the case of new vulnerability discovery,
- to ensure that security updating conducted as soon as possible after vulnerability discovery,
- to ensure that security cannot be manipulated by use of extra equipment connected to ESD via any of its interfaces,
- to make sure that security is not affected in case of overtaking the AMM system ownership by some third party.

Requirements for logging in Head-End System:

- provide secure logging of all components in AMM. Logging level depends on the security the level of that component,
- changes, errors, normal and abnormal functionality and security events must be logged,
- logs must be safe and controlled in Head-End System for the possibility of figuring out what was the reason for an event.

➢ Logs at ESD only in case of absence of communication with Head-End System

➢ Logs must be ensured against malicious tampering.

Section 8.6 on enforcement on Protection against Electromagnetic Interferences (EMI):

- to make sure that all components of AMM are being protected against external electromagnetic fields. In turn, AMM components must not influence the external components by their electromagnetic fields.

Section 8.7 on enforcement on Protection against Electromagnetic Pulse (EMP):

- to ensure that all the elements of AMM are being protected against EMP,
- to ensure that EMP cannot cause loss of data or change in software.

Additional requirements

Section 7 prescribes usage of both IPv4 and IPv6 for communication links, usage of IP VPN for communication between ESD master node and Head-End System and ensuring the existence of backup for Head-End System.

Appendix B

Configurations and Parameters

			index	Metric	Configuration Worst Case	
					Parameter configuration	Criticality
Subsystem 1, Smart Meter	OS		1	1. Secure boot	Applied,N	80
			2	2.Secure Memory	Applied,N	70
			3	3. Antivirus SW	In use,N	60
			4	5. Cryptography	112bits,Lower	90
			5	6. Logging	In use,N	70
	Interface	A2	6	1. Mesh authentication	In use,N	80
			7	2. Node authentication	In use,N	80
			8	3. Session	Session establishin,N	90
			9	4. Jamming Detection	Implemented,N	70
			10	5. DoS Prevention	Implemented,N	60
		A3	11	1. Crypto	Applied,N	60
			12	2. Authentication	Applied,N	70
		A4	13	1. Accessibility	Applied,N	95
			14	2. Equipment	Applied,N	95
			15	3.Crypto Protection	Applied,N	90
	Physical Protection		16	1. EM Protection	Applied,N	70
			17	2. Temp.	Applied,N	60
			18	3. Humidity	Applied,N	60
			19	4. Tampering	Applied,N	80
Subsystem 2, Head - End			20	1. Antivirus Update	Least once every 24hrs,N	80
			21	2. Patching	Within 24hrs,N	80
			22	3. Compromisation	Greater than 72hrs,Y	60
			23	4. Intrusion	Applied,N	85
			24	5.Access Control	Applied,N	90
Subsystem 3, Concentrator			25	1. BackUp	Provided,N	60
			26	2. Authentication Limit	Applied,N	80
			27	3. Cryptography	112bits,Lower	90
Subsystem 4, Wireless Mesh			28	1. Path Cost	Simple	60
			29	2. QoS	Used,N	
Subsystem 5, Link Concentrator-HE			30	1. BackUp	Provided,N	
Resulting SPD criticality						76

Table.Appendix B 1: Set of parameters. Configuration Worst Case.

			index	Metric	Configuration 1		Configuration 2	
					Parameter configuration	Criticality	Parameter configuration	Criticality
Subsystem 1, Smart Meter	OS		1	1. Secure boot	Applied,Y	20	Applied,Y	20
			2	2.Secure Memory	Applied,Y	30	Applied,Y	30
			3	3. Antivirus SW	In use,Y	30	In use,Y	30
			4	4. Cryptography	112bits,Higher	10	112bits,Higher	10
			5	5. Logging	In use,Y	30	In use,Y	30
	Interface	A2	6	1. Mesh authentication	In use,Y	20	In use,Y	20
			7	2. Node authentication	In use,Y	20	In use,Y	20
			8	3. Session	Session establishing,N	90	Session establishin,Y	15
			9	4. Jamming Detection	Implemented,Y	30	Implemented,Y	30
			10	5. DoS Prevention	Implemented,Y	40	Implemented,Y	40
		A3	11	1. Crypto	Applied,Y	20	Applied,Y	20
			12	2. Authentication	Applied,Y	15	Applied,Y	15
		A4	13	1. Accessibility	Applied,Y	20	Applied,Y	20
			14	2. Equipment	Applied,Y	20	Applied,Y	20
			15	3.Crypto Protection	Applied,Y	10	Applied,Y	10
	Physical Protection		16	1. EM Protection	Applied,Y	15	Applied,Y	15
			17	2. Temp.	Applied,Y	20	Applied,Y	20
			18	3. Humidity	Applied,Y	20	Applied,Y	20
			19	4. Tampering	Applied,Y	15	Applied,Y	15
Subsystem 2, Head - End			20	1. Antivirus Update	Least once every 24hrs,Y	30	Least once every 24hrs,Y	30
			21	2. Patching	Within 24hrs,Y	20	Within 24hrs,Y	20
			22	3. Compromisation	Greater than 72hrs,N	20	Greater than 72hrs,N	20
			23	4. Intrusion	Applied,Y	20	Applied,Y	20
			24	5.Access Control	Applied,Y	20	Applied,Y	20
Subsystem 3, Concentrator			25	1. BackUp	Provided,N	60	Provided,Y	20
			26	2. Authentication Limit	Applied,Y	15	Applied,Y	15
			27	3. Cryptography	112bits,Higher	10	112bits,Higher	10
Subsystem 4, Wireless Mesh			28	1. Path Cost	Simple	60	Simple	60
			29	2. QoS	Used,N	70	Used,N	70
Subsystem 5, Link Concentrator-HE			30	1. BackUp	Provided,N	70	Provided,Y	20
Resulting SPD criticality						**44**		**31**

Table.Appendix B 2: Set of parameters. Configuration 1 and 2.

			index	Metric	Configuration 3		Configuration 4	
					Parameter configuration	Criticality	Parameter configuration	Criticality
Subsystem 1, Smart Meter	OS		1	1. Secure boot	Applied,Y	20	Applied,Y	20
			2	2.Secure Memory	Applied,Y	30	Applied,Y	30
			3	3. Antivirus SW	In use,Y	30	In use,Y	30
			4	4. Cryptography	112bits,Higher	10	112bits,Lower	90
			5	5. Logging	In use,Y	30	In use,Y	30
	Interface	A2	6	1. Mesh authentication	In use,Y	20	In use,Y	20
			7	2. Node authentication	In use,Y	20	In use,N	80
			8	3. Session	Session establishing,N	90	Session establishin,N	90
			9	4. Jamming Detection	Implemented,Y	30	Implemented,Y	30
			10	5. DoS Prevention	Implemented,Y	40	Implemented,Y	40
		A3	11	1. Crypto	Applied,Y	20	Applied,Y	20
			12	2. Authentication	Applied,Y	15	Applied,Y	15
		A4	13	1. Accessibility	Applied,Y	20	Applied,Y	20
			14	2. Equipment	Applied,Y	20	Applied,Y	20
			15	3.Crypto Protection	Applied,Y	10	Applied,Y	10
	Physical Protection		16	1. EM Protection	Applied,Y	15	Applied,N	70
			17	2. Temp.	Applied,Y	20	Applied,N	60
			18	3. Humidity	Applied,Y	20	Applied,N	60
			19	4. Tampering	Applied,Y	15	Applied,Y	15
Subsystem 2, Head - End			20	1. Antivirus Update	Least once every 24hrs,Y	30	Least once every 24hrs,N	80
			21	2. Patching	Within 24hrs,Y	20	Within 24hrs,N	80
			22	3. Compromisation	Greater than 72hrs,N	20	Greater than 72hrs,N	20
			23	4. Intrusion	Applied,Y	20	Applied,Y	20
			24	5.Access Control	Applied,Y	20	Applied,Y	20
Subsystem 3, Concentrator			25	1. BackUp	Provided,Y	20	Provided,Y	20
			26	2. Authentication Limit	Applied,Y	15	Applied,Y	15
			27	3. Cryptography	112bits,Higher	10	112bits,Higher	10
Subsystem 4, Wireless Mesh			28	1. Path Cost	Simple	60	Simple	60
			29	2. Quds	Used,Y	20	Used,Y	20
Subsystem 5, Link Concentrator-HE			30	1. BackUp	Provided,Y	20	Provided,Y	20
Resulting SPD criticality						**21**		**38**

Table.Appendix B 3: Set of parameters. Configuration 3 and 4.

Appendix C

The Excel file

The executable file SPD_criticality.xlsx can be found on:

https://github.com/gagarin525125/Master_Thesis_2017