Bachelor thesis
Information Science

RADBOUD UNIVERSITEIT

Smart Charging: A privacy and security analysis

Author:
Jory van Keulen
4038053

Main supervisor/assessor:
Prof. dr. M.C.J.D. van Eekelen
marko@cs.ru.nl

Second supervisor:
MSc. Carlos Montes Portela
Carlos.Montes-Portela@enexis.nl

Second assessor:
Dr. E.M.G.M. Hubbers
E.Hubbers@cs.ru.nl

July 14, 2014

Summary

Charging electric cars is becoming more and more important and the number of electric cars grows ever bigger. But charging all these cars can cause problems on the electricity grid, especially if all drivers charge their vehicles at the same moments. To deal with this, 'Smart Charging' was created. Smart Charging requires a lot of actors to work together and requires a lot of sensitive data to work.

In this research I will find out which privacy and security problems could occur when charging an electric vehicle using the Smart Charging architecture and which are the most dangerous for the Smart Charging process.

Contents

Preface

This thesis was written while I was performing an internship at Dutch energy grid operator Enexis. Enexis has designed their own Smart Charging architecture and has already done some research into privacy and security details of Smart Charging in collaboration with LaQuSo (an activity of Technische Universiteit Eindhoven and Radboud Universiteit Nijmegen). They have already designed several solutions to make the Smart Charging of an electric vehicle a privacy friendly process[1]. However, according to the preliminary study[8], it is not yet enough to serve as a basis for the final design, which is why I was asked to perform a risk analysis for their Smart Charging architecture, which could help them in their final design.

The assignment I was given by Enexis is to identify and assess the privacy and security needs for each of the actors involved in their Smart Charging architecture and perform a risk analysis. To do this, we will use the UML use case diagram and the system architecture they have developed as a starting point of this analysis (see Appendix 6.1), as this is the latest version of the use case and architecture they have designed about Smart Charging at the time this thesis was written.

This research is heavily based on the work and risk analysis Enexis has already performed, but goes into more detail on each of the actors involved in the process and looks at these from a different point of view.

There are also a few matters that will not be discussed in this research, as this would simply take too much time and I was told by Enexis not to waste time on them:

- Payment. Transferring money and payment data to the right parties as payment for the electricity used in charging an electric vehicle is not part of the scope of this research.
- The Electric Vehicle itself. An electric vehicle will have hardware, software and firmware required to charge it. These could be manipulated by attackers, but they are not a part of the scope of this research. It will be addressed solely as an input actor without issues of its own.

- Physical Security. It may of course be possible to tap the energy line in some way, or cut the line with an axe for example. Physical forms of security are not a part of the scope of this research.

Finally, I would like to thank Carlos Montes Portela, who has been my contact in Enexis, for his help and support while performing this analysis.

Chapter 1

Introduction: What is Smart Charging?

The concept of Smart Charging is rather new and a lot of research is still happening to get it going across the country. That does not mean it is an unimportant issue; the goal is to have between 15 and 20 thousand electric vehicles in The Netherlands by 2015. It is now 2014 and there are already over 15000 electric vehicles[5], so research into charging these vehicles without overloading the energy grid is becoming more and more important.

One of the aspects that is important to include in this research is to find out exactly what security and privacy aspects are involved in using the Smart Charging architecture. While an electric vehicle is being charged 'the smart way', many privacy and security related aspects are involved, such as the issue of identification. To turn Smart Charging into a successful way of delivering energy to electric vehicles, these aspects cannot be ignored. But to find these aspects, a basic knowledge of Smart Charging will first have to be established.

In a consumer point of view, Smart Charging should not be much more than plugging in an electric vehicle into the energy grid and expecting the vehicle to be charged the next time it is needed by the user. However, doing this will increase the amount of stress onto local parts the energy grid. One car is not a problem, but when hundreds or even thousands of vehicles are charging at the same time in the same area, the local energy lines will not be able to handle all the extra stress onto the network. And when this is happening in more than one area, problems will occur on the energy grid on an even larger scale, resulting in a serious problem for the energy grid provider. As shown in *figure 2.1*, local transformers and/or single feeders could be overloaded if there is more demand for electricity than it's capacity, and houses could face some voltage level issues because of the heavy loads

of charging electric vehicles[1, 3, 6].

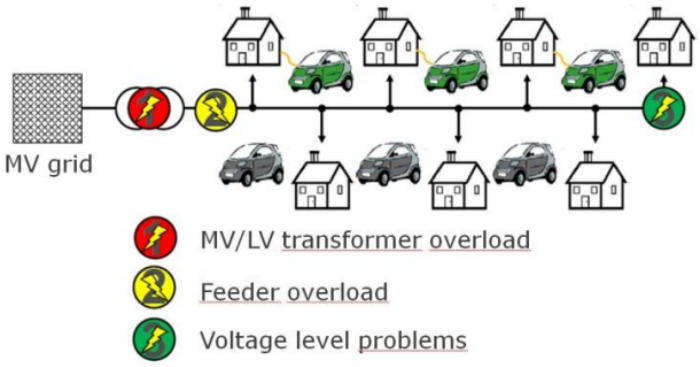

Figure 1.1: *Technical problems related to (large scale) uncontrolled EV charging*[6]

To preventing overloading the grid and still supplying the required energy to every electric vehicle, the term 'Smart Charging' was created by Eurelectric[3].

Enexis defines Smart Charging as the invention that makes it possible to charge electric vehicles for everyone by handling the network capacity in such a way, that the energy grid will never overload, even when many people connect their vehicles to the grid for charging at the same time[1]. This is done by controlling the charging process in such a way that the technical issues mentioned earlier can be avoided.

For obvious reasons, Smart Charging involves the energy grid operator. The energy grid operator, here after referred to as Distribution System Operator (DSO), needs to make sure their energy grid will not overload by handling the peaks in energy demand in an intelligent way. However, it also involves interactions and information exchanges between the DSO, the energy suppliers and charge spot operators, the actual charge spots and the electric vehicles plus their drivers. If there would be no security measures taken into this process, it could be possible to derive the locations of charging and possibly even the identity of an EV driver. There might even be issues that no one has even thought about before.

For these reasons, a risk analysis will be performed.

[1]http://www.smartcharging.nl/smart-charging/wat-is-smart-charging/

Chapter 2

Risk Analysis

2.1 Methodology

The methodology used in this risk analysis of Smart Charging is the same methodology that has been used to identify and assess risks for the Smart Meters in the Netherlands, as Smart Charging faces a fairly similar issue.

This Methodology was created after reaching a conclusion that there is no concrete example of a risk assessment methodology specific for the field of Smart Grid systems[1]. As a result, Netbeheer Nederland has chosen to use a methodology that is derived from the HMG IA Standard No. 1 (HMG IS1)[4], which is widely applied in UK government organizations and has suitable characteristics for use in the domain of smart energy systems. Because this domain includes Smart Charging, this specific methodology is also used in this research.

In this methodology, there are 6 basic steps to be taken[1]:

- Step 1: Identify Business Processes and define the assets

  The objective of the first step is to describe the system and derive the processes that happen when going through the basic course of events. This makes it possible to determine the assets that need protection against privacy and security threats. These are then categorized into the following classes:

  Informational Assets include the important data in the system.

  Functional Assets include system functions.

  System Assets refer to specific components or parts of the system.

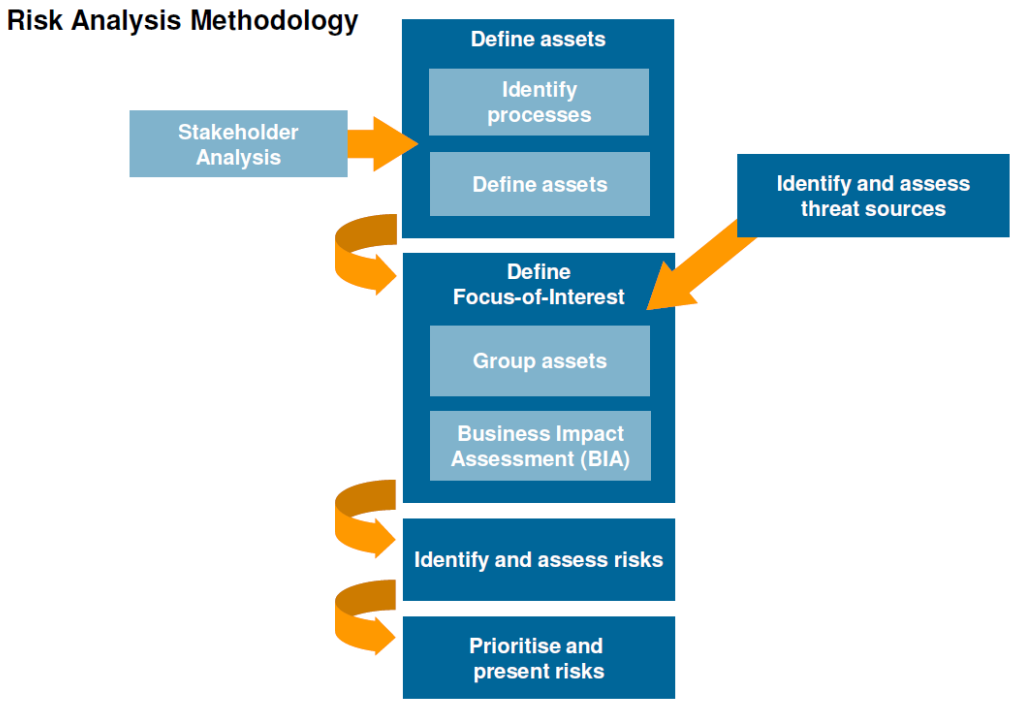

Figure 2.1: *Risk Analysis Methodology as created and used by Netbeheer Nederland to assess risks in Smart Meters.*[1]

- Step 2 and 4: Identify and Assess Threat Sources

  The objective of steps 2 and 4 is to determine who might deliberately attack the system, which external threat sources might be a danger to the system and how these are a threat.

- Step 3: Define the Focus of Interest (FoI)

  The goal of step 3 is to define specific groups of assets and processes to focus on in a particular risk assessment. If this is not done, every asset should be examined individually. This step also involves creating a Business Impact Assessment, which will be needed in step 5.

- Step 5: Identify the Specific Risks and Estimate Risk Levels

  Step 5 is the most important aspect of the risk analysis, as it results in a list of risks and corresponding risk levels. These risk levels are based on NIST 800-30[7]. This methodology focuses on two specifics to determine a risk level of high, medium or low: The likelihood that the vulnerability associated with that risk can be exploited for a successful attack and the severity of the consequence that can be achieved by a successful attack. A slightly adapted version of the NIST 800-30

classifications for risks and likelihood is used here (see Appendix 6.2 for these classifications).

- Step 6: Prioritize and Present the Risks

  The objective of the final step is to prioritize and present the risks in an easy format. In this analysis, step 5 and 6 will be presented together.

The impact and likelihood classifications used in this analysis of each separate actor are based on classifications that are already made by Enexis, in combination with questioning and personal research.

In order to analyze the risks for each of the actors involved in the Smart Charging system, each of these steps will be taken for each of the actor identified in the Smart Charging use case.

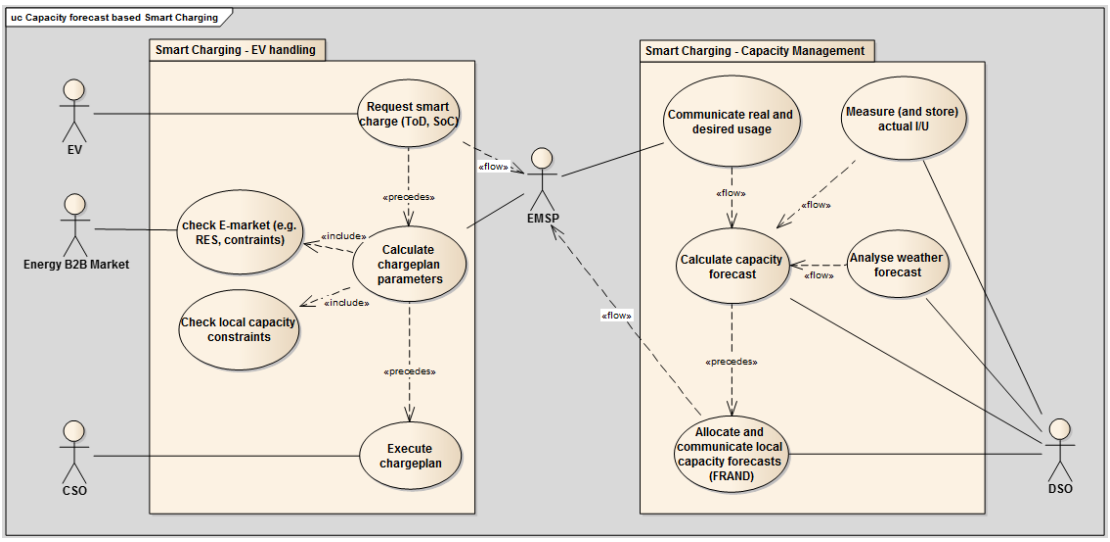

Figure 2.2: *UML Smart Charging Use Case diagram as developed by Enexis*

In this use case, 5 main actors in the Smart Charging architecture are identified[8]:

EV : Electric Vehicle. The vehicle that needs charging and its driver. The charging spot where the vehicle charges will only be handled as a medium for communication in the analysis of the electric vehicle.

CSO : Charge Spot Operator. Responsible for operating and maintaining the charge spots. In light of these responsibilities, charge spots themselves will be incorporated into this actor.

EMSP : E-Mobility Service Provider. The EMSP is responsible for all contact with the EV users. This actor is also involved in communicating with the other actors.

DSO : Distribution System Operator. Responsible for operating and maintaining the electrical grid. The DSO actor also features a transformer which measures current and voltage levels on the energy grid.

Energy B2B Market : Energy supplier. Responsible for the energy used in the energy grid.

Note: it is very possible for the EMSP and CSO to be the same entity, even though the use case displays them as different entities. Because of this, they will be assessed as both a single entity and as separate entities. However, when addressing different actors that communicate with the EMSP or CSO, they will be kept separate.

2.2 The Electric Vehicle (EV)

Step 1: Identify Business Processes and define the assets

The electric vehicle is the actor where the process for executing the smart charging of a vehicle starts. The EV is connected to a charge spot (which is only handled as a medium for this actor) and its driver then identifies himself. Finally, a charge request is sent. This analysis is made from the point of view of the EV and its driver.

Analysis of the reference architecture (Appendix 6.1) shows that the EV is involved in the following processes:

- Connecting the electric vehicle to a charge spot to be charged.
- Identifying the owner/driver of the EV through means of an identity pass using Radio Frequency Identification (RFID)[2].
- Sending a Smart Charging request to the EMSP (E-Mobility Service Provider), including information such as the state of charge of battery, the amount of energy that is needed and when the EV is needed again and should be done charging.

The assets that can be derived from these business processes and the system characteristics for the EV are the following:

Table 2.1: Assets involved with the EV

Informational Assets	Functional Assets	System Assets
Driver Identity Data	**Connecting Function**	**Charge Spot**
Charge Request Data	**Identifying Function**	**EV & Driver**
	Requesting Function	**Identity Pass**
		Charge Request

Driver identity data: The data that indicates the identity of the EV and the owner/driver of the EV that is requesting Smart Charging.

Charge Request data: The data that indicates a Smart Charging request. This data includes data that will be needed by the EMSP to eventually set up a charging plan: battery state of charge, requested

amount of energy/kilometers, time of plug in and requested time of departure.

Connecting function: Connecting the EV to a charge spot and starting the Smart Charging process.

Identifying function: Identifying the vehicle and it's driver.

Requesting function: Sending a Smart Charging request to the EMSP.

Charge Spot: The specific Charge Spot where the EV is plugged into. *Note: It is assumed that the charging spot is a real one, eg. not a fake one made by thirdy parties to extract data from the EV. This is considered a physical form of security and is therefore out of the scope of this research. However, a malware program or anything of the sort placed on a 'real' charging spot, is taken into account.*

EV & Driver: The Electric Vehicle itself and it's driver.

Identity Pass: The pass that is used to identify the person requesting a Smart Charge.
Note: A physical identification pass could also be considered a form of physical security. However, since this is a rather big issue for privacy, this topic will still be addressed in this analysis.

Charge Request The part of the system that sends a charge request to the EMSP, including all the necessary data.

Step 2 and 4: Identify and Assess Threat Sources

Possible threat sources for the EV include but are not limited to:

- Disaffected or dishonest EV drivers: Dishonest EV drivers could find ways to manipulate their identification or send in wrong charge requests to the EMSP.
- Disaffected or dishonest EMSP employees: Dishonest employees of the EMSP could find ways to manipulate the requests received by EV drivers.
- Amateur or professional hackers/other third parties: Hackers could find ways to tap into the data that is sent by an EV driver and could potentially alter it. They could also potentially access the identity of the EV driver.
- Virus, malware and system bugs: Viruses and/or malware on the charging spot could potentially be a danger to the system by altering or tapping into specific parts of the identification and requesting

modules that make a charge request. Bugs, errors or wrong updates to the charging spot could also be a major problem to these specific parts of the system.

These threat sources could potentially be involved in the following threats:

Table 2.2: Possible threats and their sources for the EV

ID	sub	Threat	Asset
1		Driver Identity data is being read by unauthorized parties	Driver Identity Data
	a	Through manipulation of RFID	Driver Identity Data
	a	(reading pass without owner knowing it is being read)	
	b	Through maleficent software on the charging spot	Driver Identity Data
2		Driver Identity data does not match the driver	Driver Identity Data
	a	Through using someone else's pass	Driver Identity Data
	b	Through manipulation of RFID	Driver Identity Data
3		The data sent through Charge Spot is read by unauthorized parties	Charge Request Data
	a	Through maleficent software on the charging spot	Charge Request Data
	b	Through maleficent software at the receiving side (the EMSP)	Charge Request Data
	c	By a dishonest employee of the EMSP	Charge Request Data
	d	By a third party	Charge Request Data
4		Charge Spot is sending no data or incorrect data	Charge Request Data
	a	Because of a bug/error or an update on the charge spot	Charge Request Data
	b	Because it has been manipulated by a virus/malware	Charge Request Data
	c	Because it has been manipulated by a third party	Charge Request Data
5		The data received by the EMSP is being manipulated	Charge Request Data
	a	By an employee of the EMSP	Charge Request Data
	b	By a third party	Charge Request Data
	c	By a bug/error/virus/malware or an update in the system	Charge Request Data

Step 3: Define the Focus of Interest (FoI)

The assets that have been found in step 1 can be divided into three specific groups and are classified as shown on the next page. The kind of asset is also repeated (Informational Asset = IA, Functional Asset = FA, System Asset = SA). As the Connecting Focus of Interest is mostly physical, the other two groups will be mostly focused on in this research.

To assess the severity of the consequences a threat could have on the EV, a Business Impact Assessment (a classification based on NIST 800-30)

Table 2.3: Focus of Interest for EV

Focus of interest	**Involved Assets**	**Kind**
Identity	Driver Identity Data	IA
	Identifying Function	FA
	EV & Driver	SA
	Identity Pass	SA
Charge Request	Charge Request Data	IA
	Requesting Function	FA
	Charge Request	SA
	Charge Spot	SA
Connecting	Connection Function	FA
	Charge Spot	SA
	EV & Driver	SA

is made to classify the impact of a risk as high, medium or low. As the EMSP is the receiving party for the charge requests sent by the EV, there may also be risks for this actor and will thus also be partially incorporated in the Business Impact Assessment.

Table 2.4: Business Impact Assessment for EV

	Impact Categories		
	Low	Medium	High
Impact on EV (or EMSP)	Minor loss of integrity	Loss of integrity	Significant loss of integrity
	Minor loss of confidentiality	Loss of confidentiality	Significant loss of confidentiality
	Minor loss of reputation	Loss of reputation	Significant loss of reputation
	Minor monetary loss	Monetary loss	Significant monetary loss

The four major factors identified in this Business Impact Assessment in the point of view of the EV are losses of integrity, confidentiality, reputation and money. When data is read or changed by unauthorized parties, the confidentiality and/or integrity of the data sent by the EV is compromised. If this data is unimportant, the impact will be categorized as low. If the data is crucial to executing the charge plan, or contain crucial privacy details, the impact of breeching integrity or confidentiality will be high. If the EV or the EMSP loses a lot to a little amount of money because wrong data is sent, the impact for monetary loss will be categorized as high to low respectively. The reputation factor is mostly assigned to the EMSP. If things go very wrong, the EMSP will lose a lot of reputation in the eyes of the consumer.

Step 5 and 6: Identify the Specific Risks and Estimate Risk Levels and Prioritize

In these final 2 steps, the threats found in step 2 and 4 will be assessed by categorizing the impact using the Business Impact Assessment made in step 3 and the likelihood and risk tables in Appendix 6.2. They will then be displayed in order of most to least risky.

The likelihood and impact estimations used in this assessment are mostly based on the initial research by Enexis, as well as questioning and personal research.

After assessment of the security threats being faced by the EV, the following list of threats and their risks can be derived, prioritized from most to least risky. The CIA triad[1] is also used as much as possible. For a complete overview of the results including the different risk sources for the EV, see Appendix 6.3.1.

Table 2.5: Overview of analyzed threats and risk levels for EV

ID	Threat	Asset	AIC	Likelihood	Impact	Risk
1	Driver Identity data does not match the driver	Driver Identity Data	C/I	M	H	H
2	Charge Spot is sending no data or incorrect data	Charge Request Data	I/A	M	H	H
3	The data received by the EMSP is being manipulated	Charge Request Data	I	M	M	M
4	Driver Identity data is being read by unauthorized parties	Driver Identity Data	C	M	M	M
5	The data sent by a Charge Spot is being read by unauthorized parties	Charge Request Data	C	M	M	M

In conclusion, there are some rather high risks involved in this part of the smart charging process. There could be serious problems if the driver identity data or the charge request data are manipulated. Privacy can breeched if the driver's identity falls into the wrong hands and a non functional charge spot could ruin the entire charging process.

[1] http://www.techrepublic.com/blog/it-security/the-cia-triad/488/

2.3 The Charge Spot Operator(CSO)

Step 1: Identify Business Processes and define the assets

The charge spot operator is the actor that controls the charge spots in the smart charging architecture. It executes the charge plans established by the e-mobility service provider and operates on a central data storage system together with the EMSP. However, this central storage system is omitted in this actor and will be incorporated in the EMSP actor, as this is the actor dealing with the most important data. This analysis is made from the point of view of the CSO.

Analysis of the reference architecture (Appendix 6.1) shows that the CSO is involved in the following processes:

- Operating and maintaining of charge spots.
- Receiving a chargeplan from the EMSP.
- Executing the chargeplan received from EMSP by routing it to the charge spot.
- Measuring actual charge spot usage.
- Passing on charge spot usage data to the EMSP who then passes it on to the DSO.
- Communicating with the charge spots. When EV has finished charging, charge spot will show the amount of energy that was used. All communication between the CSO and the charge spot goes through the Open Charge Point Protocol (OCPP) created by E-laad in the Netherlands[2].

The assets that can be derived from these business processes and the system characteristics for the CSO are the following:

Charge Spot Usage Data: The data that is measured by the CSO about the actual usage of the charge spots.

Charge Plan Data: The data that is received by the CSO from the EMSP about the chargeplan that needs to be executed.

Operational Data: The data involved in the operating and maintaining of the charge spots, including the data sent to charge spot after the charging process is completed.

Operating Function: The operating and maintaining of charge spots.

Table 2.6: Assets involved with the CSO

Informational Assets	Functional Assets	System Assets
Charge Spot Usage Data	**Operating Function**	**Charge Spot**
Charge Plan Data	**Executing Function**	**Charge Plan**
Operational Data	**Measuring Function**	**Communication Module**
		Measurement Module

Executing Function: The receiving and executing of a charge plan.

Measuring Function: Measuring actual usage of charge spots.

Charge Spot: The charge spot that the EV is connected to and will receive a charge execution order.

Charge Plan: The charge plan that needs to be executed.

Communication Module: The part of the system that involved communication between EMSP and CSO, and communication between CSO and charge spot.

Measurement Module: The part of the system where actual usage of the charge spots is being measured.

Step 2 and 4: Identify and Assess Threat Sources

Possible threat sources for the CSO include but are not limited to:

- Disaffected or dishonest CSO employees: CSO employees could find ways to manipulate the execution of a chargeplan, the measuring of charge spot usage (including already measured data) or simply mess with the charge spot.
- (Disaffected or dishonest) EMSP employees: EMSP employees could find ways to manipulate the charge plan that is sent to the CSO, or send a wrong charge plan to be executed.
- Amateur or professional hackers/other third parties: Hackers could find ways to tap into the data sent between the EMSP and CSO as well as the CSO and charge spot, compromising confidentiality. They could find ways to alter this data, compromising integrity.

- Component failure, virus and malware: Component failure on the charge spot could potentially send in the wrong usage measurements, or execute charge plans incorrectly (or not at all).

These threat sources could potentially be involved in the following threats:

Table 2.7: Possible threats and their sources for the CSO

ID	sub	Threat	Asset
1		Charge Plan is manipulated	Charge Plan Data
	a	By CSO employees	Charge Plan Data
	b	By EMSP employees	Charge Plan Data
	c	By third parties	Charge Plan Data
2		Charge Plan is not executed properly	Charge Plan Data
	a	Because of component failure	Charge Plan Data
	b	Because of a incorrect charge plan	Charge Plan Data
3		Charge spot usage is not measured	Charge Spot Usage Data
	a	Because of component failure	Charge Spot Usage Data
	b	Because of a communication failure	Charge Spot Usage Data
4		Charge spot usage data is manipulated	Charge Spot Usage Data
	a	By CSO employees	Charge Spot Usage Data
	b	By EMSP employees	Charge Spot Usage Data
	c	By third parties	Charge Spot Usage Data
5		No data is sent between CSO and charge spot	Operational Data
	a	Because of component/communication failure	Operational Data
	b	Because of a CSO employee	Operational Data
6		Charge Spot firmware or configuration is manipulated	Operational Data
	a	Because of component failure	Operational Data
	b	By CSO employees	Operational Data
	c	By third parties	Operational Data

Step 3: Define the Focus of Interest (FoI)

The assets that have been found in step 1 can be divided into three specific groups and are classified as shown on the next page. The kind of asset is also repeated (Informational Asset = IA, Functional Asset = FA, System Asset = SA).

Table 2.8: Focus of Interest for CSO

Focus of interest	**Involved Assets**	**Kind**
FoI 1: CS Usage Measurement	Charge Spot Usage Data	IA
	Measurement function	FA
	Measurement module	SA
Fo1 2: Charge Plan Execution	Charge plan data	IA
	Executing function	FA
	Charge Spot	SA
	Charge Plan	SA
	Communication Module	SA
Foi 1: Charge Spot Operation	Operational Data	IA
	Operating Function	FA
	Charge Spot	SA
	Communication Module	SA

To assess the severity of the consequences a threat could have on the CSO, a Business Impact Assessment (a classification based on NIST 800-30) is made to classify the impact of a risk as high, medium or low.

Table 2.9: Business Impact Assessment for CSO

	Impact Categories		
	Low	Medium	High
Impact on CSO	Minor loss of integrity	Loss of integrity	Major loss of integrity
	Minor loss of confidentiality	Loss of confidentiality	Major loss of confidentiality
	Minor loss of reputation	Loss of reputation	Major loss of reputation
	Minor monetary loss	Monetary loss	Major monetary loss

The four major factors identified in this Business Impact Assessment in the point of view of the CSO are losses of integrity, confidentiality, reputation and money. If a charge plan is manipulated, integrity and/or confidentiality of data can be compromised. If the charge plan is not executed the way it should be executed, the CSO could take some serious blows to their reputation and lose a lot of money. If these are only minor incidents that will not affect them much, the impact will be categorized as low. Likewise, if the opposite is true, the impact shall be categorized as high. If the measurements that are made by the CSO about the charge spot usage are not correct or manipulated, a serious error in communication with the rest of the Smart Charging process will occur, most likely resulting in a lowered reputation and monetary losses for the CSO. And if the charge spot itself is not functioning properly or is manipulated, the impact to the CSO will be

the same.

Step 5 and 6: Identify the Specific Risks and Estimate Risk Levels and Prioritize

In these final 2 steps, the threats found in step 2 and 4 will be assessed by categorizing the impact using the Business Impact Assessment made in step 3 and the likelihood and risk tables in Appendix 6.2. They will then be displayed in order of most to least risky.

The likelihood and impact estimations used in this assessment are mostly based on the initial research by Enexis, as well as questioning and personal research.

After assessment of the security threats being faced by the CSO, the following list of threats and their risks can be derived, prioritized from most to least risky. The CIA triad is also used as much as possible. For a complete overview of the results including the different risk sources for the CSO, see Appendix 6.3.2.

Table 2.10: Overview of analysed threats and risk levels for CSO

ID	Threat	Asset	AIC	Likelihood	Impact	Risk
1	Charge spot firmware or configuration is manipulated	Operational Data	I/A	M	H	H
2	No data is sent between CSO and charge spot	Operational Data	I/A	M	M	M
3	Charge spot usage data is manipulated	Charge Spot Usage Data	I	L	M	L
4	Charge spot usage is not measured	Charge Spot Usage Data	A	L	M	L
5	Charge plan is manipulated	Charge Plan Data	I	L	L	L
6	Charge plan is not executed properly	Charge Plan Data	A	L	L	L

In conclusion, it is obvious that manipulation of a charge point is by far the most dangerous threat and is in definate need of protection. And if there is no proper communication between the charge spots and CSO, the CSO will not be able to operate the way they should, resulting in a risk that cannot be ignored. The actual usage of the charge spot is data that is needed by more than just the CSO, so not being able to deliver this will impact more than a single actor. However, the chance of this happening is rather low. And since charge plans are unique for each charge proces, the likelihood of an attacker or other threat affecting it is very low, as well as the impact.

2.4 The E-Mobility Service Provider (EMSP)

Step 1: Identify Business Processes and define the assets

The EMSP is more or less the central actor in the architecture this analysis is based upon. Because of this, some aspects of analysis for other actors will be repeated, albeit from the EMSP point of view. The EMSP (together with the CSO) operates with a central data storage system where both user details (for EV identification) and charge spot IDs are stored.

Analysis of the reference architecture (Appendix 6.1) shows that the EMSP is involved in the following processes:

- Communicating with the DSO about the energy capacity. This includes receiving capacity forecasts from the DSO and communication about actual and desired capacity usage. The Open Smart Charging Protocol (OSCP)[2] is used here to communicate.
- Forwarding the real usage of charge spots from the CSO to DSO.
- Receiving charge requests from the EV (the charge request will include a charge spot identification code, among other data).
- Handling the identity of the EV user, for administrative and service payment purposes.
- Checking local capacity constraints (the calculating and checking of capacity of local electricity lines).
- Checking the energy market (to find out if the energy needed can be supplied. Future use of this business process will include checking where the energy can be obtained the cheapest).
- Create a charging plan based upon the forecast made by the DSO and the charge request by the EV.
- Sending the charge plan to the CSO for execution.

The assets that can be derived from these business processes and the system characteristics for the EMSP are the following:

Capacity Data: The data involving communication with DSO about capacity including actual and desired capacity usage, and capacity forecasts.

Usage Data: The data involving the actual usage of charge spots that is received from the CSO and sent to the DSO.

[2]http://www.smartcharging.nl/smart-charging/open-smart-charging-protocol/

Table 2.11: Assets involved with the EMSP

Informational Assets	Functional Assets	System Assets
Capacity Data	**Request Receiving Function**	**Charge Request**
Usage Data	**Communication Function**	**Charge Plan**
Charge Request Data	**Checking Function**	**Checking Module**
Energy Market Data	**Plan Creation Function**	**CSO Communication Module**
Constraint Data		**DSO Communication Module**
Charge Plan Data		**Central Storage System**

Charge Request Data: The data received from the EV that indicates a charge request. For this analysis, user identification and charge spot identification will be part of the charge request data.

Energy Market Data : The data involving the energy supplier(s).

Constraint Data: The data involving the local capacity constraints.

Charge Plan Data: The data indicating chargeplan created by the EMSP.

Request Receiving Function: The receiving of a charge request.

Communication Function: Communication with the DSO and CSO.

Checking Function: Checking the energy market and local capacity constraints.

Plan Creation Function: Creating a charge request.

Charge Request: The charge request received from the EV.

Charge Plan: The charge plan that is created by the EMSP.

Checking Module: The part of the system where the EMSP checks the energy market and local capacity constraints.

CSO Communication Module: The part of the system where communication with the CSO takes place.

DSO Communication Module: The part of the system where communication with the DSO takes place through OSCP.

Central Storage System: The part of the system where user details, charge spot identification and more is stored.

Step 2 and 4: Identify and Assess Threat Sources

Possible threat sources for the EMSP include but are not limited to:

- Disaffected or dishonest CSO/DSO employees: CSO employees could find ways to manipulate charge spot usage data before they send it to the EMSP. DSO employees could find ways to manipulate the capacity forecasts before they are sent to the EMSP.
- Disaffected or dishonest EMSP employees: EMSP employees could find ways to manipulate the charge plan that is sent to the CSO, or send a wrong charge plan to be executed. They could create a disclosure of user data and charge spot identification, or manipulate other input that is needed for the creation of the charge plan and the Smart Charging process in general.
- Amateur or professional hackers/other third parties: Hackers could find ways to tap into and potentially alter the data sent between the several actors that the EMSP communicates with.
- Malware, viruses and system bugs: System bugs and viruses/malware could compromise the ability of the EMSP to create charge plans or handle sensitive data in a secure manner.

These threat sources could potentially be involved in a series of threats. See the next page for the list of these threats faced by the EMSP.

Step 3: Define the Focus of Interest (FoI)

The assets that have been found in step 1 can be divided into four specific groups and are classified as shown below. The kind of asset is also repeated (Informational Asset = IA, Functional Asset = FA, System Asset = SA). It is also worth mentioning that the final focus of interest, the creation of a charge plan, uses most of the other data assets as input to establish a charge plan as output.

Table 2.12: Possible threats and their sources for the EMSP

ID	sub	Threat	Asset
1		Real and desired capacity usage is manipulated	Capacity Data
	a	By a DSO employee	Capacity Data
	b	By an EMSP employee	Capacity Data
	c	By a third party	Capacity Data
2		Capacity forecasts from DSO are manipulated	Capacity Data
	a	By a DSO employee	Capacity Data
	b	By an EMSP employee	Capacity Data
	c	By a third party	Capacity Data
	d	Data incorrect because of virus/system bug	Capacity Data
3		Actual charge spot usage data is manipulated	Usage Data
	a	By a CSO employee	Usage Data
	b	By an EMSP employee	Usage Data
	c	By a DSO employee	Usage Data
	d	By a third party	Usage Data
	e	Data incorrect because of virus/system bug	Usage Data
4		The charge request is manipulated	Charge Request Data
	a	By an EMSP employee	Charge Request Data
	b	By a third party	Charge Request Data
	c	By a virus/system bug	Charge Request Data
5		EV user's identity is disclosed and/or manipulated	Charge Request Data
	a	Because of an EMSP employee	Charge Request Data
	b	By a third party	Charge Request Data
	c	Because of virus/system bug or malware	Charge Request Data
6		Charge spot Identity is disclosed and/or manipulated	Charge Request Data
	a	Because of an EMSP employee	Charge Request Data
	b	Because of a third party	Charge Request Data
	c	Because of virus/system bug or malware	Charge Request Data
7		Energy Market check data is incorrect	Energy Market Data
	a	Because of an EMSP employee	Energy Market Data
	c	Because of virus/system bug or malware	Energy Market Data
8		Capacity constraint data is incorrect	Constraint Data
	a	Because of an EMSP employee	Constraint Data
	c	Because of virus/system bug or malware	Constraint Data
9		The charge plan is incorrect	Charge Plan Data
	a	Because of wrong input	Charge Plan Data
	b	Because of an error from the EMSP	Charge Plan Data
	c	Data incorrect because of virus/system bug	Charge Plan Data
10		The charge plan is manipulated	Charge Plan Data
	a	By an EMSP employee	Charge Plan Data
	b	By a third party	Charge Plan Data

Table 2.13: Focus of Interest for EMSP

Focus of interest	**Involved Assets**	**Kind**
FoI 1: Charge Request Receiving	Charge Request Data	IA
	Request Receiving Function	FA
	Charge Request	SA
	Central Storage System	SA
FoI 2: Communication (with DSO and CSO)	Capacity Data	IA
	Usage Data	IA
	Communication Function	FA
	CSO Communication Module	SA
	DSO Communication Module	SA
FoI 3: Pre-Plan Creation Check	Energy Market Data	IA
	Constraint Data	IA
	Checking Function	FA
	Checking Module	SA
FoI 4: Charge Plan Creation	Charge Plan Data	IA
	Plan Creation Function	FA
	Charge Plan	SA

To assess the severity of the consequences a threat could have on the DSO, a Business Impact Assessment (a classification based on NIST 800-30) was made to classify the impact of a risk as high, medium or low:

Table 2.14: Business Impact Assessment for EMSP

	Impact Categories		
	Low	Medium	High
Impact on EMSP	Minor loss of integrity	Loss of integrity	Major loss of integrity
	Minor loss of confidentiality	Loss of confidentiality	Major loss of confidentiality
	Minor loss of reputation	Loss of reputation	Major loss of reputation
	Minor monetary loss	Monetary loss	Major monetary loss
	Minor safety issue	Safety issue	Major safety issue

Five impact factors have been identified in this Business Impact Assessment for the EMSP. They are losses of integrity, confidentiality, reputation, money and the occurrence of safety issues. Disclosure or manipulation of data would compromise confidentiality or integrity respectively. Should an attacker or error succeed in manipulating one of the EMSP's activities, the result will be a damaged reputation for the EMSP and monetary losses. If there are major errors with capacity checking and/or planning, there could

potentially be some safety issues. When these incidents are only of minor importance and would not affect the EMSP or Smart Charging system that much, the impact will be categorized as low. Should there be a very major impact after an incident, the impact will be categorized as high.

Step 5 and 6: Identify the Specific Risks and Estimate Risk Levels and Prioritize

In these final 2 steps, the threats found in step 2 and 4 will be assessed by categorizing the impact using the Business Impact Assessment made in step 3 and the likelihood and risk tables in Appendix 6.2. They will then be displayed in order of most to least risky.

The likelihood and impact estimations used in this assessment are mostly based on the initial research by Enexis, as well as questioning and personal research.

After assessment of the security threats being faced by the EMSP, the following list of threats and their risks can be derived, prioritized from most to least risky. The CIA triad is also used as much as possible. For a complete overview of the results including the different risk sources for the EMSP, see Appendix 6.3.3.

Table 2.15: Overview of analyzed threats and risk levels for EMSP

ID	Threat	Asset	AIC	Likelihood	Impact	Risk
1	The charge request is manipulated	Charge Request Data	I	M	H	H
2	Real and desired capacity usage is manipulated	Capacity Data	I	M	M	M
3	Actual charge spot usage data is manipulated	Usage Data	I	M	M	M
4	EV user's identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
5	Charge spot identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
6	Capacity forecasts from DSO are manipulated	Capacity Data	I	L	M	L
7	Capacity constraint data is incorrect	Constraint Data	I/A	L	M	L
8	The charge plan is incorrect	Charge Plan Data	I	L	L	L
9	The charge plan is manipulated	Charge Plan Data	I	L	L	L
10	Energy Market check data is incorrect	Energy Market Data	I/A	L	L	L

In conclusion, for the EMSP, messing with the data coming from the charge spot itself is again the most important threat. If this is manipulated, capacity management, grid operation and customer satisfaction will be affected in a negative way. If the EMSP does not get good information about capacity (forecasts, capacity constraints etc), their capacity management can go wrong resulting in compromised management of capacity and could even create safety issues.

The most important privacy issues are also brought to light here: the EV's driver identity and location could be disclosed or manipulated, resulting in a serious breach of a customer's privacy.

And again, charge plans going wrong is a rather low risk incident, as the likelihood of that happening is low (assuming the input for creating one is correct) and the impact to the EMSP is not that great.

2.5 The EMSP and CSO as a single entity (the Operator)

Step 1: Identify Business Processes and define the assets

The EMSP and CSO are both separate actors in the Smart Charging architecture. However, is it very likely that these actors are actually the same entity; one business that fulfills both of these roles. For this reason, this analysis will combine the activities of both actors and treat them as a single actor. The difference between treating these actors as the same entity should be the fact that less communication between different actors is needed (namely the communication between EMSP and CSO), resulting in a smaller threat window for the overall Smart Charging process but a larger amount of threats for this combined actor (namely the threats of both CSO and EMSP).

For easy reference to this combined actor, this combination of EMSP and CSO will simply be called the operator. This analysis will be made from the point of view of the operator.

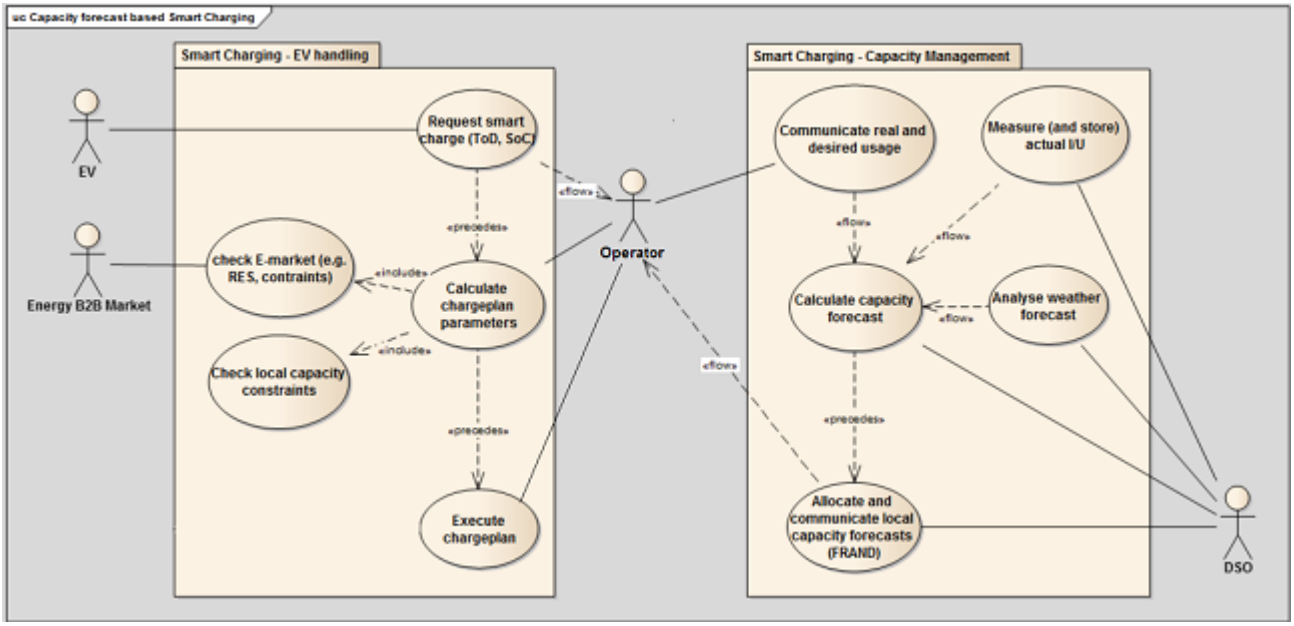

Figure 2.3: *Altered Smart Charging use case with combined EMSP and CSO as the Operator.*

Analysis of the reference architecture (Appendix 6.1), the altered use case (figure 2.3) and the separate analyses of the CSO and EMSP show that the operator is involved in the following processes:

- Receiving charging requests from the EV (The charge request will include a charge spot identification code, among other data).
- Handling the identity of EV user, for administrative and service payment purposes.
- Communicating with the DSO about the energy capacity. This includes receiving capacity forecasts from the DSO and communication about actual and desired capacity usage. The Open Smart Charging Protocol (OSCP)[3] is used here to communicate.
- Checking local capacity constraints (the calculating and checking of capacity of local electricity lines).
- Checking the energy market (to find out if the energy needed can be supplied. Future use of this business process will include checking there the energy can be obtained the cheapest).
- Creating a charging plan based upon the forecast made by the DSO and the charge request sent by the EV.
- Executing the chargeplan by routing it to the Charge Spot.
- Measuring actual charge spot usage.
- Sending the real usage of charge spots to DSO.
- Operating and maintaining of Charge Spots.
- Communicating with the charge spots. When EV has finished charging, charge spot will show the amount of energy that was used. All communication between the CSO and the charge spot goes through the Open Charge Point Protocol (OCPP) created by E-laad in the Netherlands[2].

[3]http://www.smartcharging.nl/smart-charging/open-smart-charging-protocol/

The assets that can be derived from these business processes and the system characteristics for the operator are the following:

Table 2.16: Assets involved with the operator

Informational Assets	Functional Assets	System Assets
Capacity Data	**Request Receiving Function**	**Charge Request**
Charge Spot Usage Data	**Communication Function**	**Charge Plan**
Charge Request Data	**Checking Function**	**Checking Module**
Energy Market Data	**Measuring Function**	**Communication Module**
Constraint Data	**Plan Creation Function**	**Central Storage System**
Charge Plan Data	**Executing Function**	**Charge Spot**
Operational Data	**Operating Function**	**Measurement Module**

Capacity Data: The data involving communication with DSO about capacity including actual and desired capacity usage, and capacity forecasts.

Charge Spot Usage Data: The data involving the actual usage of charge spots.

Charge Request Data: The data received from the EV that indicates a charge request. For this analysis, user identification and charge spot identification will be part of the charge request data.

Energy Market Data : The data involving the energy supplier(s).

Constraint Data: The data involving the local capacity constraints.

Charge Plan Data: The data indicating the chargeplan created and executed by the operator.

Operational Data: The data involved in the operating and maintaining of the charge spots, including the data sent to charge spot after the charging process is completed.

Request Receiving Function: The receiving of a charge request.

Communication Function: Communication with the DSO.

Checking Function: Checking the energy market and local capacity constraints.

Plan Creation Function: Creating a charge request.

Operating Function: The operating and maintaining of charge spots.

Executing Function: The executing of a charge plan.

Measuring Function: Measuring actual usage of charge spots.

Charge Request: The charge request received from the EV.

Charge Plan: The charge plan that is created and executed by the operator.

Checking Module: The part of the system where the EMSP checks the energy market and local capacity constraints.

Communication Module: The part of the system where communication with the DSO takes place through OSCP and communication with the charge spot takes places through OCPP.

Central Storage System: The part of the system where user details, charge spot identification and more is stored.

Charge Spot: The charge spot that the EV is connected to and will receive a charge execution order.

Measurement Module: The part of the system where actual usage of the charge spots is being measured.

Step 2 and 4: Identify and Assess Threat Sources

Possible threat sources for the operator include but are not limited to:

- Disaffected or dishonest employees: Employees could find ways to manipulate charge spot usage data before they send it to the DSO. DSO employees could find ways to manipulate the capacity forecasts before they are sent to the operator. Operator employees could find ways to manipulate the charge plan, or send a wrong charge plan to be executed. They could create a disclosure of user data and charge spot identification, or manipulate other input that is needed for the creation of the charge plan and the Smart Charging process in general.

- Amateur or professional hackers/other third parties: Hackers could find ways to tap into and potentially alter the data sent between the several actors that the operator communicates with.
- Component failure, malware, viruses and system bugs: System bugs and viruses/malware could compromise the ability of the operator to create charge plans or handle sensitive data in a secure manner. Component failure on the charge spot could potentially send in the wrong usage measurements, or execute charge plans incorrectly (or not at all).

These threat sources could potentially be involved in a series of threats. These threats and their sources are show below and continue on the next page:

Table 2.17: Possible threats and their sources for the operator (part 1)

ID	sub	Threat	Asset
1		Real and desired capacity usage is manipulated	Capacity Data
	a	By a DSO employee	Capacity Data
	b	By an operator employee	Capacity Data
	c	By a third party	Capacity Data
2		Capacity forecasts from DSO are manipulated	Capacity Data
	a	By a DSO employee	Capacity Data
	b	By an operator employee	Capacity Data
	c	By a third party	Capacity Data
	d	Data incorrect because of virus/system bug	Capacity Data
3		Actual charge spot usage data is manipulated	Charge Spot Usage Data
	a	By an operator employee	Charge Spot Usage Data
	b	By a DSO employee	Charge Spot Usage Data
	c	By a third party	Charge Spot Usage Data
	d	Data incorrect because of virus/system bug	Charge Spot Usage Data
4		The charge request is manipulated	Charge Request Data
	a	By an operator employee	Charge Request Data
	b	By a third party	Charge Request Data
	c	By a virus/system bug	Charge Request Data
5		EV user's identity is disclosed and/or manipulated	Charge Request Data
	a	Because of an operator employee	Charge Request Data
	b	By a third party	Charge Request Data
	c	Because of virus/system bug or malware	Charge Request Data

Table 2.18: Possible threats and their sources for the operator (part 2)

ID	sub	Threat	Asset
6		Charge spot Identity is disclosed and/or manipulated	Charge Request Data
	a	Because of an operator employee	Charge Request Data
	b	Because of a third party	Charge Request Data
	c	Because of virus/system bug or malware	Charge Request Data
7		Energy Market check data is incorrect	Energy Market Data
	a	Because of an operator employee	Energy Market Data
	cb	Because of virus/system bug or malware	Energy Market Data
8		Capacity constraint data is incorrect	Constraint Data
	a	Because of an operator employee	Constraint Data
	b	Because of virus/system bug or malware	Constraint Data
9		The charge plan is incorrect	Charge Plan Data
	a	Because of wrong input	Charge Plan Data
	b	Because of an error from the operator	Charge Plan Data
	c	Data incorrect because of virus/system bug	Charge Plan Data
10		The charge plan is manipulated	Charge Plan Data
	a	By an operator employee	Charge Plan Data
	b	By a third party	Charge Plan Data
11		Charge Plan is not executed properly	Charge Plan Data
	a	Because of component failure	Charge Plan Data
	b	Because of a incorrect charge plan	Charge Plan Data
12		Charge spot usage is not measured	Charge Spot Usage Data
	a	Because of component failure	Charge Spot Usage Data
	b	Because of a communication failure	Charge Spot Usage Data
13		Charge Spot firmware or configuration is manipulated	Operational Data
	a	Because of component failure	Operational Data
	b	By an operator employee	Operational Data
	c	By third parties	Operational Data
14		No data is sent between operator and charge spot	Operational Data
	a	Because of component/communication failure	Operational Data
	b	Because of an operator employee	Operational Data

Step 3: Define the Focus of Interest (FoI)

The assets that have been found in step 1 can be divided into seven specific groups and are classified as shown below. Some of the assets are needed in more than one focus of interest. The kind of asset is also repeated (Informational Asset = IA, Functional Asset = FA, System Asset = SA).

Table 2.19: Focus of Interest for operator

Focus of interest	**Involved Assets**	**Kind**
FoI 1: Charge Request Receiving	Charge Request Data	IA
	Request Receiving Function	FA
	Charge Request	SA
	Central Storage System	SA
FoI 2: Communication	Capacity Data	IA
	Charge Spot Usage Data	IA
	Communication Function	FA
	Communication Module	SA
FoI 3: Pre-Plan Creation Check	Energy Market Data	IA
	Constraint Data	IA
	Checking Function	FA
	Checking Module	SA
FoI 4: Charge Plan Creation	Charge Plan Data	IA
	Plan Creation Function	FA
	Charge Plan	SA
Fo1 5: Charge Plan Execution	Charge plan data	IA
	Executing function	FA
	Charge Spot	SA
	Charge Plan	SA
	Communication Module	SA
FoI 6: CS Usage Measurement	Charge Spot Usage Data	IA
	Measuring function	FA
	Measurement module	SA
Foi 7: Charge Spot Operation	Operational Data	IA
	Operating Function	FA
	Charge Spot	SA
	Communication Module	SA

To assess the severity of the consequences a threat could have on the operator, a Business Impact Assessment (a classification based on NIST 800-30) was made to classify the impact of a risk as high, medium or low:

Table 2.20: Business Impact Assessment for operator

	Impact Categories		
	Low	Medium	High
Impact on operator	Minor loss of integrity	Loss of integrity	Major loss of integrity
	Minor loss of confidentiality	Loss of confidentiality	Major loss of confidentiality
	Minor loss of reputation	Loss of reputation	Major loss of reputation
	Minor monetary loss	Monetary loss	Major monetary loss
	Minor safety issue	Safety issue	Major safety issue

Five impact factors have been identified in this Business Impact Assessment for the operator. They are losses of integrity, confidentiality, reputation, money and the occurrence of safety issues. Disclosure or manipulation of data would compromise confidentiality or integrity respectively. Should an attacker or error succeed in manipulating one of the operator's activities, the result will be a damaged reputation for the operator combined with monetary losses. If there are major errors with capacity checking and/or planning, there could potentially be some safety issues. If the charge plan is not executed the way it should be executed, the operator could take some serious blows to their reputation and lose a lot of money. If the measurements that are made by the operator about the charge spot usage are not correct or manipulated, a serious error in communication with the rest of the Smart Charging process will occur, most likely resulting in a lowered reputation and monetary losses for the operator. And if the charge spot itself is not functioning properly or is manipulated, the impact to the operator will be the same. If these are only minor incidents that will not affect them much, the impact will be categorized as low. Likewise, if the opposite is true, the impact shall be categorized as high.

Step 5 and 6: Identify the Specific Risks and Estimate Risk Levels and Prioritize

In these final 2 steps, the threats found in step 2 and 4 will be assessed by categorizing the impact using the Business Impact Assessment made in step 3 and the likelihood and risk tables in Appendix 6.2. They will then be displayed in order of most to least risky.

The likelihood and impact estimations used in this assessment are mostly based on the initial research by Enexis, as well as questioning and personal research.

After assessment of the security threats being faced by the operator, the following list of threats and their risks can be derived, prioritized from most to least risky. The CIA triad is also used as much as possible. For a complete overview of the results including the different risk sources for the operator, see Appendix 6.3.4.

Table 2.21: Overview of analyzed threats and risk levels for operator

ID	Threat	Asset	AIC	Likelihood	Impact	Risk
1	Charge Spot firmware or configuration is manipulated	Operational Data	I/A	M	H	H
2	The charge request is manipulated	Charge Request Data	I	M	H	H
3	No data is sent between operator and charge spot	Operational Data	I/A	M	M	M
4	Real and desired capacity usage is manipulated	Capacity Data	I	M	M	M
5	Actual charge spot usage data is manipulated	Usage Data	I	M	M	M
6	EV user's identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
7	Charge spot Identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
8	Capacity forecasts from DSO are manipulated	Capacity Data	I	L	M	L
9	Charge spot usage is not measured	Charge Spot Usage Data	A	L	M	L
10	Capacity constraint data is incorrect	Constraint Data	I/A	L	M	L
11	The charge plan is incorrect	Charge Plan Data	I	L	L	L
12	The charge plan is manipulated	Charge Plan Data	I	L	L	L
13	Charge Plan is not executed properly	Charge Plan Data	A	L	L	L
14	Energy Market check data is incorrect	Energy Market Data	I/A	L	L	L

In conclusion, combining the CSO and EMSP into a single actor does not change much about the process - the same threats and risks exist. However, as expected, the difference is that there are now more threats to a single actor, and less overall communication between actors since the CSO and EMSP are now a single entity. Messing with the charge spot or the data coming from the charge spot itself is again the most important threat. If this is manipulated, capacity management, grid operation and customer satisfaction will be affected in a negative way. If the operator does not get good information about capacity (forecasts, capacity constraints etc), their capacity management can go wrong resulting in compromised management of capacity and could even create safety issues. The EV's driver identity and location could be still disclosed or manipulated, resulting in a serious breach of a customer's privacy.

2.6 The Distributed System Operator (DSO)

Step 1: Identify Business Processes and define the assets

The distributed system operator is the actor that operates the energy grid. They provide current and voltage measurements as well as forecasts about the capacity that is going to be needed at any given time. The DSO communicates with the EMSP and makes sure the EMSP has what they need to build a good charge plan and has enough capacity to execute them. This analysis is made from the point of view of the DSO.

Analysis of the reference architecture shows that the DSO is involved in the following processes:

- Measuring and storing of the actual voltage and current levels on the energy grid.
- Capacity planning: analyzing weather forecasts using special algorithms and making capacity forecasts about the capacity of the energy grid that will be needed at specific locations and times.
- Communicating with the EMSP about the energy capacity that will be available to them and about the real and desired usage of the energy grid. The Open Smart Charging Protocol (OSCP)[4] is used for all communication between DSO and EMSP.
- Allocating capacity to the EMSP.

The assets defined for the DSO are the following:

Table 2.22: Assets involved with the DSO

Informational Assets	Functional Assets	System Assets
Measurement Data	**Forecasting Function**	**Transformer**
Monitoring Data	**Measuring Function**	**Forecasting Module**
Forecasting Data	**Monitoring Function**	**Communication Module**
	Communication Function	**Energy Grid**
	Capacity Allocation	

[4]http://www.smartcharging.nl/smart-charging/open-smart-charging-protocol/

Monitoring data: The data involved in the communication with the EMSP regarding actual and desired capacity usage.

Measurement data: The data involved in the measuring of the actual voltage and current levels on the energy grid.

Forecasting data: The data involved in making capacity forecasts.

Forecasting function: Making capacity forecasts.

Measuring function: Measuring and storing actual current and voltage levels on the energy grid using a transformer.

Monitoring function: Monitoring the capacity requests coming from the EMSP and analyzing weather forecasts.

Communication function: Communicating with the EMSP to determine real and desired capacity.

Capacity allocation: Making sure the EMSP is granted enough capacity based on requests and forecasts.

Transformer: The part of the system that measures current and voltage levels.

Forecasting module: The part of the system that contains the algorithms to compute capacity forecasts.

Energy grid: The energy grid that the DSO operates on.

Communication module: The part of the system where communications between DSO and EMSP take place through OSCP.

Step 2 and 4: Identify and Assess Threat Sources

Possible threat sources for the DSO include but are not limited to:

- Disaffected or dishonest employees: Dishonest employees of the DSO could find ways to manipulate forecasts, capacity and communication with the EMSP. Dishonest employees of the EMSP could find ways to manipulate communication with the DSO.
- Amateur or professional hackers/other third parties: Hackers could find ways to tap into the data that is being collected by the DSO and could potentially alter it.
- Virus and other malware: Viruses and/or malware could potentially be a danger to the system by altering or tapping into specific parts of the system.

- Component failure: System components could potentially measure wrong current and voltage levels, compromising the capacity management. This could happen by means of bugs, errors, faulty updates or broken components.

These threat sources could potentially be involved a series of threats. See next page for the list of these threats.

Step 3: Define the Focus of Interest (FoI)

The assets that have been found in step 1 can be divided into four specific groups and are classified as shown below. The kind of asset is also repeated (Informational Asset = IA, Functional Asset = FA, System Asset = SA).

Table 2.23: Focus of Interest for DSO

Focus of interest	**Involved Assets**	**Kind**
FoI 1: Transformer measurements	Measurement data	IA
	Measuring function	FA
	Transformer	SA
FoI 2: Communication	Monitoring data	IA
	Monitoring function	FA
	Communicating function	FA
	Communication module	SA
FoI 3: Forecasting	Forecasting data	IA
	Forecasting function	FA
	Forecasting module	SA
FoI 4: Allocation	Capacity allocation	FA
	Energy grid	SA

Table 2.24: Possible threats and their sources for the DSO

ID	sub	Threat	Asset
1		Monitoring data is manipulated	Monitoring data
	a	By an employee of either side	Monitoring data
	b	By a bug/error/virus/malware in the system	Monitoring data
	c	By a third party	Monitoring data
2		Wrong monitoring data is received	Monitoring data
	a	Through wrong readings from EMSP	Monitoring data
	b	Through reading error from DSO	Monitoring data
3		Transformer is not working properly: sending wrong or no data	Measurement data
4		Transformer readings are manipulated	Measurement data
	a	By an employee	Measurement data
	b	By a third party	Measurement data
	c	By a bug/error/virus/malware in the system	Measurement data
5		Weather forecast data is incorrect	Forecasting data
	a	Because of wrong readings	Forecasting data
	b	Because it has been altered by employee	Forecasting data
	c	Because it has been altered by third party	Forecasting data
	d	Because of a bug/error/virus/malware or an update in the system	Forecasting data
6		The forecasting algorithm is manipulated	Forecasting data
	a	By an employee	Forecasting data
	b	By a third party	Forecasting data
	c	By a bug/error/virus/malware or an update in the system	Forecasting data
7		The capacity forecast is manipulated (after the forecast is made)	Forecasting data
	a	By an employee	Forecasting data
	b	By a third party	Forecasting data
	c	By a bug/error/virus/malware or an update in the system	Forecasting data
8		Wrong capacity is allocated	Forecasting data
	a	Because of wrong input	Forecasting data
	b	By an employee	Forecasting data

To assess the severity of the consequences a threat could have on the DSO, a Business Impact Assessment (a classification based on NIST 800-30) was made to classify the impact of a risk as high, medium or low:

Table 2.25: Business Impact Assessment for DSO

	Impact categories		
	Low	Medium	High
Impact on DSO	Minor loss of integrity	Loss of integrity	Major loss of integrity
	Minor loss of confidentiality	Loss of confidentiality	Major loss of confidentiality
	Minor loss of reputation	Loss of reputation	Major loss of reputation
	Minor safety issue	Safety issue	Major safety issue
	Minor monetary loss	Monetary loss	Major monetary loss

The DSO has five impact factors to worry about. These are losses of integrity, confidentiality, reputation, money and the occurrence of safety issues. If data is changed or read without access, integrity and/or confidentiality is breeched. If this changes the process and activities are not executed properly, losses of reputation and money could occur for the DSO. If there are some serious issues with the measuring of the current and voltage levels, there could potentially be safety issues involved. If these factors are affected in a major manner and are of great importance to the process, the impact will be categorized as a high impact level. If there are only minor incidents that will not change the process and status of the DSO much, the impact will be categorized as low.

Step 5 and 6: Identify the Specific Risks and Estimate Risk Levels and Prioritize

In these final 2 steps, the threats found in step 2 and 4 will be assessed by categorizing the impact using the Business Impact Assessment made in step 3 and the likelihood and risk tables in Appendix 6.2. They will then be displayed in order of most to least risky.

The likelihood and impact estimations used in this assessment are mostly based on the initial research by Enexis, as well as questioning and personal research.

After assessment of the security threats being faced by the DSO, the following list of threats and their risks can be derived, prioritized from most to least risky. The CIA triad is also used as much as possible.For a complete overview of the results including the different risk sources for the DSO, see Appendix 6.3.5.

Table 2.26: Overview of analyzed threats and risk levels for DSO

ID	Threat	Asset	CIA	Likelihood	Impact	Risk
1	Manipulation of capacity distribution	Forecasting data	I	M	H	H
2	Monitoring data is manipulated	Monitoring data	I	M	M	M
3	Transformer readings are manipulated	Measurement data	I	M	M	M
4	Transformer is not working properly: sending wrong or no data	Measurement data	A	M	M	M
5	Wrong monitoring data is received	Monitoring data	A	L	M	L
6	Weather forecast data is incorrect	Forecasting data	I/A	L	M	L
7	The forecasting algorithm is manipulated	Forecasting data	I	L	M	L
8	The capacity forecast is manipulated (after the forecast is made)	Forecasting data	I	L	M	L

In conclusion, the risks posed by the DSO could each have a serious impact on security. However, some of them are more likely to happen than others. The main threat to the DSO is the distribution of capacity being manipulated or going wrong. This would have serious impact on the DSO and the Smart Charging process in general. All of the threats that have been found are closely related to the ability of predicting the capacity that is needed and the distribution of it.

2.7 The Energy Supplier

Step 1: Identify Business Processes and define the assets

The energy supplier only has a small role in the Smart Charging picture, namely supplying energy to the energy grid for electric vehicles to charge. Energy cannot be seen as a flow of information, as it is simply generated and put onto the energy grid, where it is used where needed/agreed and so it cannot be said that the energy supplier is providing energy for just a single actor in the architecture. This analysis is made from the point of view of the energy supplier.

Analysis of the reference architecture shows that the energy supplier (named Energy B2B Market in the system characteristics, appendix 6.1) is involved in only two processes:

- Supplying the right amount of energy on the energy grid for the CSO to execute the chargeplan created by the EMSP.
- Communicating with the EMSP about the amount of energy provided (mainly for administrative and payment purposes).

The assets that can be derived from these business processes and the system characteristics for the Energy Supplier are the following:

Table 2.27: Assets involved with the energy supplier

Informational Assets	Functional Assets	System Assets
Administrative Data	**Energy Supplying Function**	**Energy**
	Communication Function	

Administrative Data Data data sent back and forth with the EMSP about the amount of energy that is used on the energy grid, provided by that particular energy supplier. This data is mainly used for administration and payment to the energy supplier for the energy used.

Energy Supplying Function Supplying sufficient energy onto the energy grid to make smart charging possible.

Communication Function Communication with EMSP about the amount of energy that is used on the energy grid, provided by that particular energy supplier.

Energy The energy that is generated and supplied by the energy supplier.

Step 2 and 4: Identify and Assess Threat Sources

Possible threat sources for the energy supplier include but are not limited to:

- Disaffected or dishonest employees: Dishonest employees of either side could find ways to manipulate administrative data.
- Amateur or professional hackers/other third parties: Hackers could find ways to tap into the administrative data and could potentially alter it.
- Administrative errors: It could be possible for the administrative data to be wrong or slightly off because of an administrative error on either side.
- Component failure: There could potentially be insufficient energy supplied if the energy supplier is facing some serious component failure[5]. It could also occur that wrong values are being measured by component failure, detailing a higher or lower amount of energy supplied than is actually the case.

These threat sources could potentially be involved in the following threats:

Table 2.28: Possible threats and their sources for the energy supplier

ID	sub	Threat	Asset
1		Administrative data is manipulated	Administrative data
	a	By an employee of either side	Administrative data
	b	By a third party	Administrative data
2		Administrative data is wrong	Administrative data
	a	Because of component failure at the energy supplier	Administrative data
	b	Because of an administrative error on either side	Administrative data
3		Not enough energy is supplied	Administrative data
	a	Because of component failure at the energy supplier	Administrative data

[5]As of the time this thesis was written, an EMSP cannot simply just go to another (cheaper) energy supplier whenever they please. However, this is expected to change in the future.

Step 3: Define the Focus of Interest (FoI)

The assets that have been found in step 1 can now be divided into 2 specific groups and are classified as shown below. The kind of asset is also repeated (Informational Asset = IA, Functional Asset = FA, System Asset = SA).

Table 2.29: Focus of Interest for Energy Supplier

Focus of interest	**Involved Assets**	**Kind**
FoI 1: Energy Supplying	Energy Supplying Function	FA
	Energy	SA
FoI 2: Communication	Administrative Data	IA
	Communication Function	FA

Now that a number of threats are identified and focus of interests have been defined, it is possible to start assessing each of these threats to see what risk they pose. The second part of step 3 is to make a Business Impact Assessment (BIA, a classification based on NIST 800-30) which will be used to assess the severity of the consequences a threat could have on the Energy Supplier. This Impact Assessment will help classify the impact of a threat as high, medium or low:

Table 2.30: Business Impact Assessment for Energy Supplier

Impact Categories		
Low	Medium	High
Minor loss of Reputation	Loss of Reputation	Major Loss of Reputation
Minor Monetary Loss	Monetary Loss	Major Monetary Loss

The two factors identified in this Business Impact Assessment in the point of view of the energy supplier are losses of reputation and money. Wrong or altered data or energy values could lead to loss of image of the energy supplier, or could potentially cost them lots of money (for example by supplying energy no one has paid for). If this is only a small error and doesn't cost much, the risk will be classified as low. However, if a huge error occurs that would cost the energy supplier hundreds of thousands of euros and would be a huge blow to their reputation, they could lose clients to competitors, resulting in a serious risk which will be classified as high.

Step 5 and 6: Identify the Specific Risks and Estimate Risk Levels and Prioritize

In these final 2 steps, the threats found in step 2 and 4 will be assessed by categorizing the impact using the Business Impact Assessment established in step 3 and the likelihood and risk tables in Appendix 6.2. They will then be displayed in order of most to least risky.

The likelihood and impact estimations used in this assessment are mostly based on the initial research by Enexis, as well as questioning and personal research.

After assessment of the security threats being faced by the energy supplier, the following list of threats and their risks can be derived, prioritized from most to least risky. The CIA triad is also used as much as possible. For a complete overview of the results including the different risk sources for the energy supplier, see Appendix 6.3.6.

Table 2.31: Overview of analyzed threats and risk levels for energy supplier

ID	Threat	Asset	CIA	Likelihood	Impact	Risk
1	Not enough energy is supplied	Administrative data	A	L	H	M
2	Administrative data is manipulated	Administrative data	I	L	M	L
3	Administrative data is wrong	Administrative data	A/I	L	L	L

In conclusion, the risks faced by the energy supplier seem to be exactly that - threats only to the energy supplier. These risks pose no grave threat to the smart charging process, as there will always be different energy suppliers on the energy market when one of them cannot provide the appropriate amount of energy. But, for the energy supplier, there could be some serious monetary losses if these threats are not taken into account.

2.8 Interesting Results

Now that each actor has been analyzed, it is safe to say that there are definitely a lot of threats involved on different parts of the Smart Charging architecture. The analysis of the EMSP and CSO as separate and single entities show that the more actors are involved in the process, the more communication is needed and the more threats arise.

A very interesting result of this analysis is the fact that in almost every actor, the problem of manipulation of the charge spot is present and poses the most serious threat. If a charge spot is manipulated, does not send the right data or the EV simply does not use the spot properly, the entire Smart Charging process is affected in a very negative way. Another interesting result, especially concerning privacy, is that an EV driver's identity, location and charge details could potentially fall into the wrong hands. An EV driver's identity could even be stolen by manipulation of their RFID identity pass.

Other serious threats to the Smart Charging process seem to be coming from the DSO side. If the net capacity distribution does not go the way it is supposed to go, either by manipulation or error, serious issues on the energy grid could occur and could potentially paralyze Smart Charging in entire areas. The input data received by the DSO and the data calculated by their algorithms is also quite important and could have a big impact on the process if they are not correct.

On the other hand, when smaller things go wrong, such as the execution of a single charge plan, it is obvious that it does not affect the process much and the impact and likelihood of it happening is very low. Another interesting point is the fact that the energy supplier only plays a rather small role in the process, and could (especially in the future) easily be replaced by others.

In short, according to this analysis, it is safe to assume that the most interesting parts of the Smart Charging process in regards to security and privacy, and will need the most attention and protection, are located at both the horizontal and vertical ends of the smart charging process: the charge spot and the DSO.

Chapter 3

Methodology Analysis

In this chapter, I will reflect on the methodology that was used to analyze Smart Charging.

First off, I think the methodology has been a great help in analyzing the architecture that was provided to me. As there was no other concrete example of a risk assessment methodology that was specific for the field of Smart Grid systems, this methodology was a perfect fit for Smart Charging, as it was designed for a similar issue, namely the Smart Meter issue in the Netherlands. It proved to be very applicable to the field of Smart Charging as well.

One thing that was a big plus for me was the fact that the NIST 800-30 classifications for risks and likelihood were used in this methodology, as the research provided by Enexis has also used these classifications, which provided me with a lot of likelihood and impact classifications to use and compare with. It is also a rather simple way of showing which threats are dangerous and which are not, and it helped me a great deal in depicting the results that were found in my analysis in an easy format.

However, there are a few remarks that will have to be made about this particular methodology. The most notable issue with this methodology for me, was the fact that step 2 and 4 (the identifying and assessing of threat sources) were more or less pulled together and that step 3 (defining the focus-of-interests) was not made before these two. During the analysis, I often found myself grouping the assets and business processes I found in step 1 (identify business processes and define the assets) before I would start to think about what could possibly have an impact on them. Doing this would help me divide the entire process of a single actor into several activities which could each have their own privacy and security issues and then analyze these activities independently.

Another thing I found rather strange is that the Business Impact Assessment is part of the third step in this methodology, while it would not be used until step 5 (identify and assess risks), so why not include it in this fifth step? In my earlier versions of this thesis, even the people that had read them had trouble understanding the order of the steps and the motive behind it.

So in short, I am very happy I have used this particular methodology in my research and think it is a very applicable methodology for the Smart Charging architecture, but I do think the order of some of the steps could have been changed somewhat.

Chapter 4

Conclusion

After using this very applicable methodology for analyzing each of the actors in the Smart Charging architecture, it is safe to say that there are a lot of threats involved on different parts of the Smart Charging architecture. The more actors involved in the process, the more communication is needed and the more threats arise. The most important threat that appears in almost each of the actors that have been analyzed is manipulation of the charge spot or the data sent by the EV through the charge spot. Another problem that came back (albeit in different forms) in almost every analysis is threats that jeopardize the capacity distribution. For the customer's privacy, the identity and location are actually in danger of being disclosed or falling into the wrong hands. Smart Charging definitely has weaknesses in it's architecture that are in need of protection.

Chapter 5

Reflection

This thesis is focused on a very specific system architecture and it is worth mentioning that several aspects of this architecture are omitted from this research and could be subjects for new research. The most important of these subjects are the flow of payment for all the services done. This is a very important aspect of Smart Charging and will require a research of it's own. Another aspect that is not looked at in this research is the software/hardware/firmware inside the electric vehicle itself. It could also be interesting to spend time analyzing the threats that come with physical forms of security which are not part of the scope of this research. Each of these aspects could be looked at in follow-up research.

5.1 Validation

Smart Charging is a relatively new concept and much research into this subject is still happening. New breakthroughs and changes to the Smart Charging process can still happen in the future. The architecture that was provided to me by Enexis is only one of many, and even for Enexis this architecture might still change in the future.

The results of this research are very much based on a particular architecture of Smart Charging and a particular methodology. A different company could be using a different architecture, or the one made by Enexis could change over time. This could mean that a similar research in a different timespan or location could produce different results. However, the actors inside every version of a Smart Charging system will more or less be the same. Older versions of this architecture by Enexis had the same actors in them, albeit under different names. There is no Smart Charging without a charging spot to charge at, or a service company to have contact with the customer, or someone to operate on the charge spots, and so on. Depending on the architecture and the way these actors communicate, different results

could be found in a similar analysis. Some of the findings of this research could be rendered invalid when compared to a new architecture, but there will also be core similarities.

The same applies to methodologies. If a different methodology is used to analyze security and privacy threats, different outcomes could occur. However, if the objective is the same (finding and assessing these threats), the goal of the research should be the same and similar results will be found.

The methodology that was used for this research is a valid methodology for Smart Charging as it was created by taking a well established and accepted standard for risk analysis[4], and adapting it into the domain of Smart Grid systems. Smart Charging is technically a part of this domain, but the methodology was intended for use in the Smart Meter architectures. There will of course be differences between Smart Meters and Smart Charging. But the actors involved show several similarities, and there are even some similar outcomes[1].

5.2 What to do with these results?

The results that have been found in this research could be used as input for developing a secure and privacy friendly Smart Charging architecture. Enexis could analyze them, compare them to their own or other research and draw conclusions of their own.

This research could also be used as a starting point or reference for new research. One could focus more on the way payment is done for each of the services done in the Smart Charging architecture, or analyze a new version of the architecture and compare it with this research. It could even be possible to expand this research and add more aspects such as the electric vehicle itself (hardware, software and firmware).

[1] http://docbox.etsi.org/workshop/2013/201301_securityworkshop/04_m2mandsmartsecurity/alliander_rambi.pdf

Chapter 6

Appendix

6.1 System Characterization by Enexis

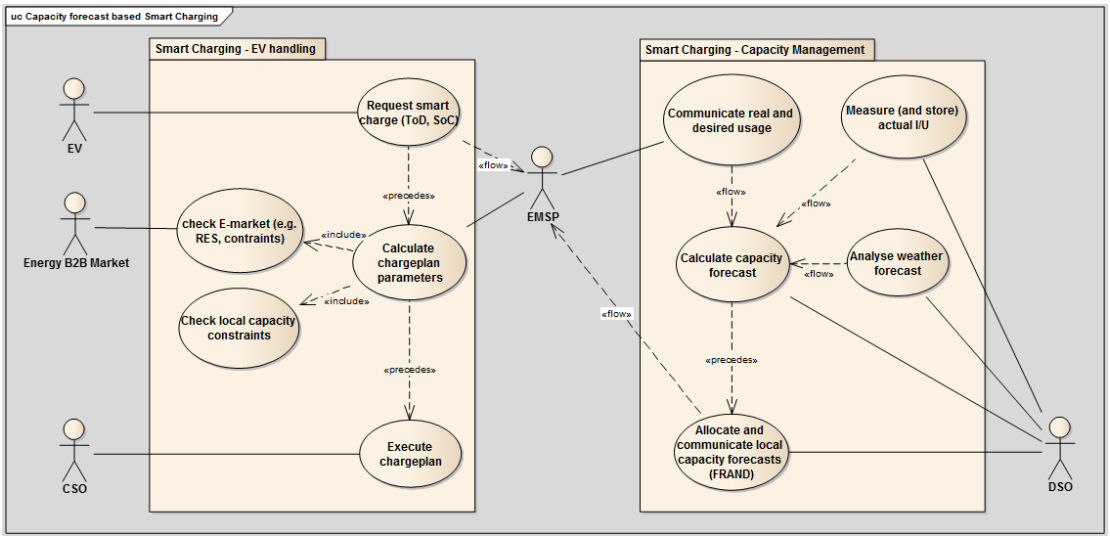

Figure 6.1: *Smart Charging Use Case as developed by Enexis in 2013*

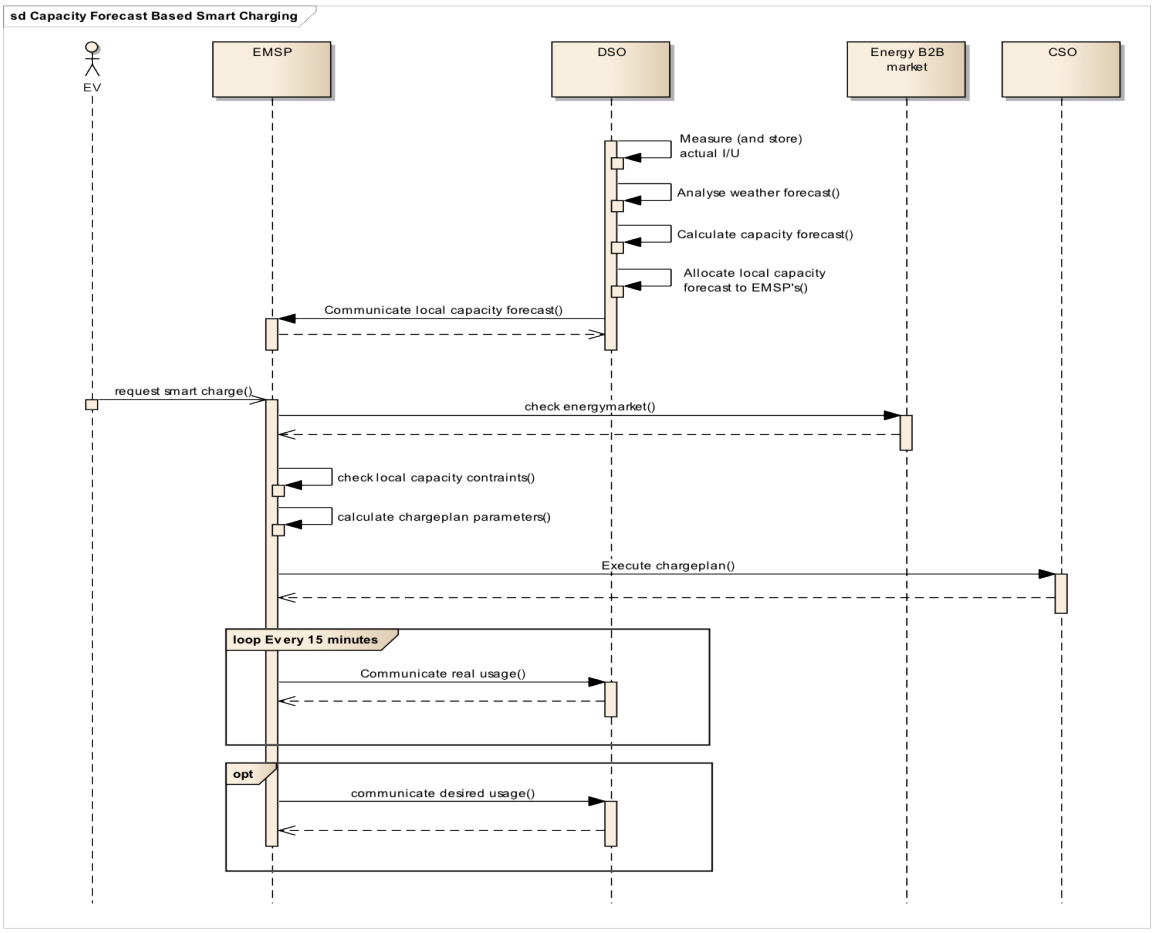

Figure 6.2: *Data flow diagram describing the data flow in the smart charging system as developed by Enexis in 2013.*

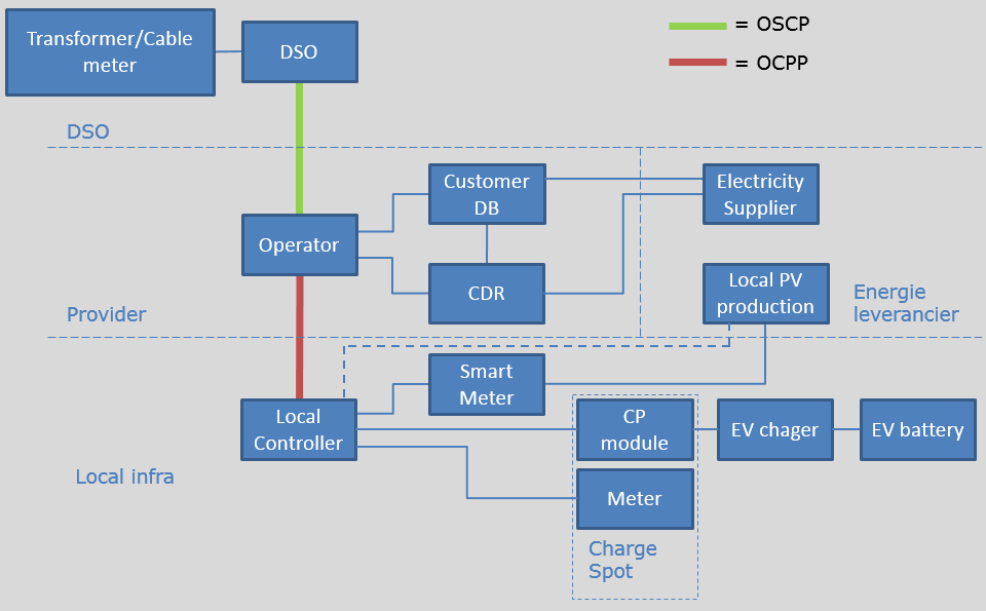

Figure 6.3: *The reference architecture of all the roles and components involved in Smart Charging using OSCP and OCPP. It is a visual representation of the different components.*

6.2 NIST 800-30 Classifications

	Likelihood Categories		
	High	Medium	Low
Occurance in time	Monthly-Daily More than 10 times in a year	Annual Once a year to 10 times in a year	Possible Once in a century to once in a year

Figure 6.4: *A slightly altered version of the NIST 800-30 classifications of likelihood used in this Risk Analysis of Smart Charging.*

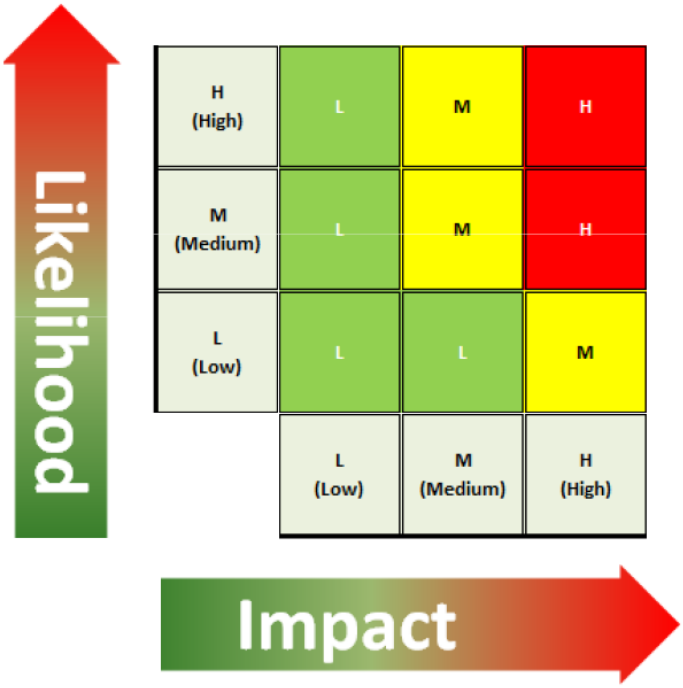

Figure 6.5: *The NIST 800-30 classifications of risk, which is a combination of Impact and Likelihood. These Classifications are also used in this risk analysis of Smart Charging.*

6.3 Complete results of the Risk Analysis

The following results are compied from the author's own research files.

6.3.1 Analysis results: Electric Vehicle (EV)

ID	sub	Threat	Asset	AIC	Likelihood	Impact	Risk
1		Driver Identity data does not match the driver	Driver Identity Data	C/I	M	H	H
	a	Through using someone else's pass	Driver Identity Data	C/I	M	H	H
	b	Through manipulation of RFID	Driver Identity Data	I	L	H	M
2		Charge Spot is sending no data or incorrect data	Charge Request Data	I/A	M	H	H
	a	Because of a bug/error or an update on the charge spot	Charge Request Data	A	M	H	H
	b	Because it has been manipulated by a virus/malware	Charge Request Data	I	L	H	M
	c	Because it has been manipulated by a third party	Charge Request Data	I	L	H	M
3		The data received by the EMSP is being manipulated	Charge Request Data	I	M	M	M
	a	By an employee of the EMSP	Charge Request Data	I	M	M	M
	b	By a third party	Charge Request Data	I	M	M	M
	c	By a bug/error/virus/malware or an update in the system	Charge Request Data	I	M	M	M
4		Driver Identity data is being read by unauthorised parties	Driver Identity Data	C	M	M	M
	a	Through manipulation of RFID	Driver Identity Data	C	M	M	M
	a	(reading pass without owner knowing it is being read)					
	b	Through malificent software on the charging spot	Driver Identity Data	C	L	M	L
5		The data sent by a Charge Spot is being read by unauthorised parties	Charge Request Data	C	M	M	M
	a	Through malificent software on the charging spot	Charge Request Data	C	L	M	L
	b	Through malificent software at the receiving side (the EMSP)	Charge Request Data	C	M	M	M
	c	By a dishonest employee of the EMSP	Charge Request Data	C	M	M	M
	d	By a third party	Charge Request Data	C	M	M	M

6.3.2 Analysis results: Charge Spot Operator (CSO)

ID	sub	Threat	Asset	AIC	Likelihood	Impact	Risk
1		Charge Spot firmware or configuration is manipulated	Operational Data	I/A	M	H	H
	a	Because of component failure	Operational Data	A	M	H	H
	b	By CSO employees	Operational Data	I	M	H	H
	c	By third parties	Operational Data	I	M	H	H
2		No data is sent between CSO and charge spot	Operational Data	I/A	M	M	M
	a	Because of component/communication failure	Operational Data	A	M	M	M
	b	Because of a CSO employee	Operational Data	I	L	M	L
3		Charge spot usage is not measured	Charge Spot Usage Data	A	L	M	L
	a	Because of component failure	Charge Spot Usage Data	A	L	M	L
	b	Because of a communication failure	Charge Spot Usage Data	A	L	M	L
4		Charge spot usage data is manipulated	Charge Spot Usage Data	I	L	M	L
	a	By CSO employees	Charge Spot Usage Data	I	L	M	L
	b	By EMSP employees	Charge Spot Usage Data	I	L	M	L
	c	By third parties	Charge Spot Usage Data	I	L	M	L
5		Charge Plan is manipulated	Charge Plan Data	I	L	L	L
	a	By CSO employees	Charge Plan Data	I	L	L	L
	b	By EMSP employees	Charge Plan Data	I	L	L	L
	c	By third parties	Charge Plan Data	I	L	L	L
6		Charge Plan is not executed properly	Charge Plan Data	A	L	L	L
	a	Because of component failure	Charge Plan Data	A	L	L	L
	b	Because of a incorrect charge plan	Charge Plan Data	A	L	L	L

6.3.3 Analysis results: E-Mobility Service Provider (EMSP)

ID	sub	Threat	Asset	AIC	Likelihood	Impact	Risk
1		The charge request is manipulated	Charge Request Data	I	M	H	H
	a	By an EMSP employee	Charge Request Data	I	M	H	H
	b	By a third party	Charge Request Data	I	M	H	H
	c	By a virus/system bug	Charge Request Data	A	M	H	H
2		Real and desired capacity usage is manipulated	Capacity Data	I	M	M	M
	a	By a DSO employee	Capacity Data	I	M	M	M
	b	By an EMSP employee	Capacity Data	I	M	M	M
	c	By a third party	Capacity Data	I	M	M	M
3		Actual charge spot usage data is manipulated	Usage Data	I	M	M	M
	a	By a CSO employee	Usage Data	I	M	M	M
	b	By an EMSP employee	Usage Data	I	M	M	M
	c	By a DSO employee	Usage Data	I	M	M	M
	d	By a third party	Usage Data	I	M	M	M
	e	Data incorrect because of virus/system bug	Usage Data	A	M	M	M
4		EV user's identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
	a	Because of an EMSP employee	Charge Request Data	C/I	M	M	M
	b	By a third party	Charge Request Data	C/I	M	M	M
	c	Because of virus/system bug or malware	Charge Request Data	C/I	M	M	M
5		Charge spot Identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
	a	Because of an EMSP employee	Charge Request Data	C/I	M	M	M
	b	Because of a third party	Charge Request Data	C/I	M	M	M
	c	Because of virus/system bug or malware	Charge Request Data	C/I	M	M	M
6		Capacity forecasts from DSO are manipulated	Capacity Data	I	L	M	L
	a	By a DSO employee	Capacity Data	I	L	M	L
	b	By an EMSP employee	Capacity Data	I	L	M	L
	c	By a third party	Capacity Data	I	L	M	L
	d	Data incorrect because of virus/system bug	Capacity Data	A	L	M	L
7		Capacity constraint data is incorrect	Constraint Data	I/A	L	M	L
	a	Because of an EMSP employee	Constraint Data	I	L	M	L
	c	Because of virus/system bug or malware	Constraint Data	A	L	M	L
8		The charge plan is incorrect	Charge Plan Data	I	L	L	L
	a	Because of wrong input	Charge Plan Data	I	L	L	L
	b	Because of an error from the EMSP	Charge Plan Data	I	L	L	L
	c	Data incorrect because of virus/system bug	Charge Plan Data	I/A	L	L	L
9		The charge plan is manipulated	Charge Plan Data	I	L	L	L
	a	By an EMSP employee	Charge Plan Data	I	L	L	L
	b	By a third party	Charge Plan Data	I	L	L	L
10		Energy Market check data is incorrect	Energy Market Data	I/A	L	L	L
	a	Because of an EMSP employee	Energy Market Data	I	L	L	L
	c	Because of virus/system bug or malware	Energy Market Data	A	L	L	L

6.3.4 Analysis results: EMSP and CSO as a single entity

ID	sub	Threat	Asset	AIC	Likelihood	Impact	Risk
1		Charge Spot firmware or configuration is manipulated	Operational Data	I/A	M	H	H
	a	Because of component failure	Operational Data	A	M	H	H
	b	By an operator employee	Operational Data	I	M	H	H
	c	By third parties	Operational Data	I	M	H	H
2		The charge request is manipulated	Charge Request Data	I	M	H	H
	a	By an EMSP employee	Charge Request Data	I	M	H	H
	b	By a third party	Charge Request Data	I	M	H	H
	c	By a virus/system bug	Charge Request Data	A	M	H	H
3		No data is sent between operator and charge spot	Operational Data	I/A	M	M	M
	a	Because of component/communication failure	Operational Data	A	M	M	M
	b	Because of an operator employee	Operational Data	I	L	M	L
4		Real and desired capacity usage is manipulated	Capacity Data	I	M	M	M
	a	By a DSO employee	Capacity Data	I	M	M	M
	b	By an EMSP employee	Capacity Data	I	M	M	M
	c	By a third party	Capacity Data	I	M	M	M
5		Actual charge spot usage data is manipulated	Usage Data	I	M	M	M
	a	By a CSO employee	Usage Data	I	M	M	M
	b	By an EMSP employee	Usage Data	I	M	M	M
	c	By a DSO employee	Usage Data	I	M	M	M
	d	By a third party	Usage Data	I	M	M	M
	e	Data incorrect because of virus/system bug	Usage Data	A	M	M	M
6		EV user's identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
	a	Because of an EMSP employee	Charge Request Data	C/I	M	M	M
	b	By a third party	Charge Request Data	C/I	M	M	M
	c	Because of virus/system bug or malware	Charge Request Data	C/I	M	M	M
7		Charge spot Identity is disclosed and/or manipulated	Charge Request Data	C/I	M	M	M
	a	Because of an EMSP employee	Charge Request Data	C/I	M	M	M
	b	Because of a third party	Charge Request Data	C/I	M	M	M
	c	Because of virus/system bug or malware	Charge Request Data	C/I	M	M	M

8		Capacity forecasts from DSO are manipulated	Capacity Data	I	L	M	L
	a	By a DSO employee	Capacity Data	I	L	M	L
	b	By an EMSP employee	Capacity Data	I	L	M	L
	c	By a third party	Capacity Data	I	L	M	L
	d	Data incorrect because of virus/system bug	Capacity Data	A	L	M	L
9		Charge spot usage is not measured	Charge Spot Usage Data	A	L	M	L
	a	Because of component failure	Charge Spot Usage Data	A	L	M	L
	b	Because of a communication failure	Charge Spot Usage Data	A	L	M	L
10		Capacity constraint data is incorrect	Constraint Data	I/A	L	M	L
	a	Because of an EMSP employee	Constraint Data	I	L	M	L
	c	Because of virus/system bug or malware	Constraint Data	A	L	M	L
11		The charge plan is incorrect	Charge Plan Data	I	L	L	L
	a	Because of wrong input	Charge Plan Data	I	L	L	L
	b	Because of an error from the EMSP	Charge Plan Data	I	L	L	L
	c	Data incorrect because of virus/system bug	Charge Plan Data	I/A	L	L	L
12		The charge plan is manipulated	Charge Plan Data	I	L	L	L
	a	By an EMSP employee	Charge Plan Data	I	L	L	L
	b	By a third party	Charge Plan Data	I	L	L	L
13		Charge Plan is not executed properly	Charge Plan Data	A	L	L	L
	a	Because of component failure	Charge Plan Data	A	L	L	L
	b	Because of a incorrect charge plan	Charge Plan Data	A	L	L	L
14		Energy Market check data is incorrect	Energy Market Data	I/A	L	L	L
	a	Because of an EMSP employee	Energy Market Data	I	L	L	L
	c	Because of virus/system bug or malware	Energy Market Data	A	L	L	L

6.3.5 Analysis results: Distributed System Operator (DSO)

ID	sub	Threat	Asset	CIA	Likelihood	Impact	Risk
1		Manipulation of capacity distribution	Forecasting data	I	M	H	H
1	a	Because of wrong input	Forecasting data		M	H	H
1	b	By an employee	Forecasting data	I	M	H	H
2		Monitoring data is manipulated	Monitoring data	I	M	M	M
2	a	By an employee of either side	Monitoring data	I	M	M	M
2	b	By a bug/error/virus/malware in the system	Monitoring data	I/A	M	M	M
2	c	By a third party	Monitoring data	I	M	M	M
3		Transformer is not working properly: sending wrong or no data	Measurement data	A	M	M	M
4		Transformer readings are manipulated	Measurement data	I	M	M	M
5	a	By an employee	Measurement data	I	M	M	M
5	b	By a third party	Measurement data	I	M	M	M
5	c	By a bug/error/virus/malware in the system	Measurement data	I/A	M	M	M
5		Wrong monitoring data is received	Monitoring data	A	L	M	L
3	a	Through wrong readings from EMSP	Monitoring data	A	L	M	L
3	b	Through reading error from DSO	Monitoring data	A	L	M	L
6		Weather forecast data is incorrect	Forecasting data	I/A	L	M	L
6	a	Because of wrong readings	Forecasting data	A	L	M	L
6	b	Because it has been altered by employee	Forecasting data	I	L	M	L
6	c	Because it has been altered by third party	Forecasting data	I	L	M	L
6	d	Because of a bug/error/virus/malware/update in the system	Forecasting data	I/A	L	M	L
7		The forecasting algorithm is manipulated	Forecasting data	I	L	M	L
7	a	By an employee	Forecasting data	I	L	M	L
7	b	By a third party	Forecasting data	I	L	M	L
7	c	By a bug/error/virus/malware or an update in the system	Forecasting data	I/A	L	M	L
8		The capacity forecast is manipulated (after the forecast is made)	Forecasting data	I	L	M	L
8	a	By an employee	Forecasting data	I	L	M	L
8	b	By a third party	Forecasting data	I	L	M	L
8	c	By a bug/error/virus/malware or an update in the system	Forecasting data	I/A	L	M	L

6.3.6 Analysis results: Energy Supplier (B2B Market)

ID	sub	Threat	Asset	CIA	Likelihood	Impact	Risk
1		Not enough energy is supplied	Administrative data	A	L	H	M
1	a	Because of component failure at the Energy Supplier	Administrative data	A	L	H	M
2		Administrative data is manipulated	Administrative data	I	L	M	L
2	a	By an employee of either side	Administrative data	I	L	M	L
2	b	By a third party	Administrative data	I	L	M	L
3		Administrative data is wrong	Administrative data	A/I	L	L	L
3	a	Because of component failure at the Energy Supplier	Administrative data	A	L	L	L
3	b	Because of an administrative error on either side	Administrative data	A/I	L	L	L

Academic Documents

[1] Carlos Montes Portela, Danny Geldtmeijer, Han Slootweg and Marko van Eekelen. A Flexible and privacy friendly ICT architecture for smart charging of EVs, *22nd International Conference on Electricity Distribution*, CIRED Session IV, Paper 0199, june 2013

[2] Want, R. An introduction to RFID technology, *Pervasive Computing, IEEE*, Volume 5, Issue 1, 2006

[3] J. A. Peças Lopes, F. J. Soares and P. M. Almeida and M. Moreira da Silva. Smart Charging Strategies for Electric Vehicles: Enhancing Grid Performance and Maximizing the Use of Variable Renewable Energy Resources, *EVS24 International Battery, Hybrid and Fuel Cell Electric Vehicle Symposium*, May 13-16, 2009

Technical Documents

[1] Sandro Bologna, Himanshu Khurana, Zoltan Precsenyi, Johan Rambi, Hani Banayoti, and Ralph Eckmaier. High level risk assessment methodology for relevant assets: Expert group on the security and resilience of communication networks and information systems for smart grids. (Work Package 1.4, draft 0.9), 27 march 2012.

[2] E-laad.nl. OCPP v1.5: A functional description. (Final version 2.0).

[3] Eurelectric. European electricity industry views on charging electronic behicles, a eurelectric proposition paper. 2011.

[4] CESG: The National Technical Authority for Information Assurance. HMG IA Standard No. 1: Technical risk assessment. Issue: 3.51, October 2009.

[5] RDW. Gegevensmodel op basis van aandrijflijn- en brandstofconcept. *Technical report, Rijksdienst voor het wegverkeer*, 2013.

[6] Christian Rehtanz and Christian Wietfeld. Presentation interoperabilität als schlüssel zur intergration der elektromobilität in die netzsysteme der zukunft. Technical report, Technische Universität Dortmund and IKT.

[7] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk management guide for information technology systems: Recommendations of the national institue of standards and technology. *National Institute of Standards and Technology Special Publication 800-30*, July 2002.

[8] Marko van Eekelen, Erik Poll, Engelbert Hubbers, Barbara Vieira, and Fabian van den Broek. Security of the OSCP protocol: Preliminary study. December 20, 2013.