Cyber Security Assessment of Public Electric Vehicle Chargers in Amsterdam

Monica Eugenia Carranza Pasten
Intelligent Electrical Power Grid Section
CYBER SECURITY ASSESSMENT OF PUBLIC ELECTRIC VEHICLE CHARGING STATIONS IN AMSTERDAM

Thesis

to obtain the degree on Master in Science at Delft University of Technology, to defend in public on Friday 31st of August 2018 at 9:00 a.m.

by

Mónica Eugenia CARRANZA PASTEN

born in Mexico City, Mexico.
Technology, like art, is a soaring exercise of human imagination.

Daniel Bell
# CONTENTS

Abstract ix
Acknowledgements 1

1 Can a worm leave me in the darkness? 3
  1.1 Stuxnet: A new threat for society .................. 4
  1.2 Amsterdam: Place for opportunities and cradle for threats 7
  1.3 Scope of the research work .......................... 9

2 Important information that every hacker should know 11
  2.1 Introduction ........................................ 12
  2.2 Why? The motivation behind an attack ................ 12
  2.3 Where? Selecting the area of attack .................. 14
  2.4 When? The electrical demand & charging behaviour ........ 18
  2.5 What? The EV Charging Infrastructure ................ 20
    2.5.1 The EV Charging Communication Protocols ............ 22
    2.5.2 The EV Charging Communication Interfaces ............ 24
  2.6 Summary ........................................... 25

3 The Kill Chain 27
  3.1 Introduction to the Kill Chain ......................... 28
  3.2 Stage I: Cyber Intrusion, Preparation & Execution .......... 30
  3.3 Stage II: ICS Attack Development & Execution ............. 33
  3.4 ICS Attack Complexity and Objectives .................. 35
  3.5 The Attack Scenario .................................. 37
  3.6 ICS Cyber Kill Chain applied in the manipulation of Electric Vehicle Charging Stations .................................. 39

4 Thinking like a hacker: Stage I 41
  4.1 Introduction ........................................ 42
  4.2 Planning: Reconnaissance ............................. 42
    4.2.1 How does the system that controls the EV Charging Stations work? 44
    4.2.2 Planning: Information Technology .................. 49
    4.2.3 Planning: Operational Technology .................. 54
  4.3 Preparation: Weaponization ........................... 67
  4.4 Cyber Intrusion: Delivery, Exploit, Install ............... 71
    4.4.1 Delivery ......................................... 71
    4.4.2 Exploitation and Installation ...................... 72
  4.5 Management and Enablement: Command & Control ............ 73
5 Thinking like a hacker: Stage II
  5.1 Introduction .................................................. 76
  5.2 Attack Development & Tuning: Develop .................................. 77
  5.3 Testing Attack .................................................. 78
  5.4 ICS Attack Scenario ............................................. 80
    5.4.1 Most Vulnerable Zones ..................................... 80
    5.4.2 Present Scenario: From 0% to 100% of EV Manipulation ........ 83
    5.4.3 Future Scenario: From 110% to 200% of EV Manipulation ........ 92
    5.4.4 Future Scenario: 2025 Panorama .................................. 100
    5.4.5 Feeder Behaviour in the most vulnerable zone ...................... 102
  5.5 Assumptions .................................................. 106
  5.6 Sensitivity Analysis ........................................... 107

6 Conclusion .................................................. 109

7 Recommendation for future work .................................. 115

Appendix .................................................. 119

List of Figures ................................................. 129

List of Tables .................................................. 133
STUXNET marked the beginning of a new era. We are facing a new chapter where cyber security is not just a matter of safeguarding the Information Technology (IT), but Operational Technology (OT) became one of the major areas of concern. The attacker that used to control digital processes can now control physical ones. This can even now threat human lives. Moreover, innovation is growing, new technologies are emerging and countries are moving towards a sustainable future. A re-design of the infrastructure and communication paths is needed but also the concept of traditional cyber-security as we know it today. One example of this transition, is the newly adoption of Electric Vehicles. The city of Amsterdam became one of the development hubs, which is looking to achieve by 2025 a zero-emission target in the transportation sector. In order to achieve it, Amsterdam’s city council have established new measures which led the city to have today the highest density of Electric Vehicle Chargers in the world. This has raised the public concern if the Electrical Distribution Network is capable to withstand an exponential increase in the electrical demand. Research efforts have focused on finding ways to change the charging behaviour of the users. Nonetheless, there is a lack of understanding the consequences from a technical perspective. The objective of this thesis work is on one side, to understand the behaviour of the electrical grid’s components in presence of a cyber attack targeting the EV charging station’s infrastructure. And on the other side, to assess the likelihood and the steps of this potential attack. The selected methodology is the Industrial Control Systems (ICS) Cyber Kill Chain which structures the steps that a potential attacker is likely to follow when targeting an ICS.

When developing the attack, aspects such as the optimal geographical area to launch it, the electricity demand at peak hour, the charging behaviour of the users and the geographical position of the charging stations were taken into account. In order to test the attacks, the distribution grid of Amsterdam was reversed engineered using information from open sources and it was replicated in the Software Power Factory. The attack scenarios were tested for present and future scenarios. For the present scenario the behaviour of the parameters of the grid (cable, buses and feeders) were tested when having 10 %, 50 %, 80 % and 100 % of EV chargers manipulation. The results show that the characteristics of the components have enough capacity to withstand today an attack targeting 100 % of the EV Charging Stations. For the future scenario the parameters were tested for 110 %, 150 %, 180 %, 200 % and for the 2025 scenario where the zero-emission goal should be achieved. The results show that the capacity of elements is on the border limit to withstand the double of EV Charging Stations penetration. For the future scenario in 2025, the capacity of some of the elements that constitute the electrical grid of today are bypassed which means that this could lead to a potential electrical disruption. Finally, the impact on the most vulnerable zones was measured where there is a high electrical load together with a higher density of Electric Vehicle Charging Stations.
The feeder analysis of the most vulnerable zones shows the relation between the number of charging stations installed and the expected voltage drop. The voltage drop is compared to the standard for the operation of feeders in normal conditions (Range A) which allows a voltage drop of 7.5% and the standard for contingency scenarios (Range B) which allows 10.8% of voltage drop. Besides the OT valuation, an IT assessment was also elaborated with the aim of understanding the likelihood of the attack and the steps that an attacker would follow in order to intrude into the EV Charging Stations Control system. The results show that the information that can be obtained by passive and active reconnaissance techniques is enough to find the most suitable exploit to bypass the security of the system using the commercial tools that are available for pentesting purposes. Therefore, recommendations have been given to reduce the likelihood of an attack. It is expected that this research work can be a stepping stone towards a transition to an adequate planning for the cyber security of the EV charging infrastructure. Having adequate security measures and understanding the consequences can help to plan and design a new infrastructure that could welcome and facilitate the transition to a renewable future.
This master thesis has became the culmination of two hard years of hard work. It combines my passion for cyber-security, my two-year knowledge in power systems and my final life-goal to be a promoter of sustainability. This road would not have been possible to walk without the help of some very important people. First, I would like to thank Dr. Milos Cvetkovic for your guidance during this road, for all the brainstorming hours and all the support with the new ideas (and why not, also for the coffee). Prof. Dr. Peter Palensky for giving me all your support for the realization of this master thesis, for your feedback and also for all the advises that you have given me during my master studies. Dr. Stjepan Picek thank you for your advises and many thanks for accepting to be part of my committee. Definitely this work wouldn't have been possible without my dear parents, that have always been there supporting me with my non-conventional ideas since I was a kid. Many thanks to all my friends from TU Delft, that we have support each other with this crazy road that is called Master Thesis. And thanks to you reader, that has the time to take a dive into my thoughts.
Can a worm leave me in the darkness?

It takes 20 years to build a reputation
And few minutes of a cyber-incident to ruin it

Stephane Nappo

It was January 2010. Natanz in Iran was about to become witness of one of the most important events in history. After completing their routine inspection, investigators of the International Atomic Energy Agency realized that something in the Natanz’s Uranium Enrichment Plant was not correct. Thousands of centrifuges that were enriching Uranium inside the cascade rooms were not behaving as they should. Technicians were running in and out of the cascade rooms replacing the centrifuges one by one. The main question that remained in the air was: Why? The answer of this question became one of the major history changers in decades and its consequences remained latent until today [1].
1.1. **Stuxnet: A New Threat for Society**

Stuxnet became without any doubt the most complex malware ever written in history. Its structure was so impeccable that it was soon named the first cyber weapon ever built. The initial reason of why it was created was to stop Iranian President Mahmoud Ahmadinejad from building a potential nuclear weapon by sabotaging their Uranium Enrichment Program [1]. According to the report released by Symantec on February 2011, Stuxnet was the most large, complex piece of malware with many functionalities targeting, for the very first time in history, Industrial Control Systems [3].

![Figure 1.1: Part of Stuxnet’s Code that targets Step 7 projects and PLC manufactured by Siemens. [1]](image)

What makes Stuxnet different from any other malware ever seen, is its capacity to infringe physical damage to equipment [2]. Therefore, while traditional malware is a threat for digital assets - the so called Information Technology (IT) assets - Stuxnet goes one step beyond and opens a new branch for Cyber Security: Operational Technology (OT) Security. Now, Industrial Control Systems (ICS) became a vulnerable link in this new interconnected era. The lesson learned is that the smarter the systems are, the more vulnerable they become.

Its meticulous infrastructure suggests that it took from five to ten core developers - according to Symantec - plus a team of experts that were in charge of evaluating the code quality and its management. It was discovered in July but it has been confirmed to have existed at least one year prior. Another element that played a significant role, was the detailed outline of its attack scenario. Both elements were crucial for the successful conclusion. The goal of Stuxnet was to access Field PGs: Windows computers used to program Programmable Logic Controllers (PLC), in order to modify the centrifuges activities that treated the Uranium. As it can be seen from Figure 1.1, Stuxnet targeted solely PLCs manufactured by Siemens, discarding any other. As Field PGs are unlikely to be connected to networks that have access to the internet and even to internal networks, Stuxnet had to find a way to perform host jumping until it got access to the its target [2].
We can identify the most important characteristics from a technical and an attack scenario standpoint that made Stuxnet a state-of-art Advance Persistent Threat (APT) [3]. These can be visualized in Figure 1.2:

**Figure 1.2: Characteristics of Stuxnet from a Technical and an Attack Scenario Perspective**

Stuxnet exploited four zero-day Microsoft vulnerabilities. Two were focused on self-replication while the other two on escalation of privileges. In order to get access to a Field PG, it spread first inside the Local Area Network (LAN) through a vulnerability in the Windows Print Spooler and also through the Server Message Block (SBM), a Microsoft protocol that allows printers and files sharing inside a local network. Moreover, it copied itself into Step 7 projects - a programming software for PLC - and auto-executed once it was loaded. As Stuxnet was not connected to internet, it updated itself through a peer-to-peer mechanism and the Command & Control instructions were embedded inside its binaries. It contained a Windows rootkit and the very first PLC rootkit in history [2].
Symantec speculated an attack scenario based on the characteristics that were found during Stuxnet’s investigation. The very first step was to gather the information that could reveal the characteristics of Natanz Plant’s schematics. It is highly likely, that the design documents of the ICS were stolen to develop Stuxnet code accordingly, as each feature was crafted solely for Natanz’s equipment. It has been also suspected, that Stuxnet was previously tested in a mirrored environment that included the targeted hardware. Moreover, Stuxnet binaries were digitally signed by two legitimate certification companies. Both companies were in close proximity to the city of Taiwan and it is presumed that a person got physical access to the building to steal them [3]. The big question that remains until today, is how the threat was infiltrated inside the plant. Symantec speculated about the presence of a willing third party such as a contractor that could had access to the facility and could have introduced the threat via a removable drive. According to the investigators, Stuxnet did not instantaneously execute actions but gathered information and recorded the normal operation data of the centrifuges for a determined period of time. Therefore, while performing the attack, it reproduced the normal operation data, so the operators could not realize instantaneously that something was wrong [2].

Why is Stuxnet valuable for this research work?
Stuxnet opened a door to a new field that scientists and experts never taught it could actually be possible. The concept that a digital element could infringe physical damage was speculated but never substantially proved. Stuxnet became the first piece of code that can be considered a weapon. The traditional IT security became not the only asset to safeguard and OT security became a new area of concern. After the latter incident, any Industrial Control System became a potential target. As the society aims to achieve a transition to a more interconnected and technological infrastructure, there is a correlation that signalizes a potential increase in the number of vulnerabilities. Therefore, new security measures should be implemented and the resilience of the systems should play an important role inside the ICS design and day-to-day operation.

The transition to a sustainable energy infrastructure, has lead the countries to adjust its policies to increase the share of renewable technologies. One of the most latent advances, is the inclusion of Electric Vehicles in the current mobility framework. It’s aim is to reduce the polluting emissions from the transportation sector. To achieve the latter, changes in the current cities infrastructure are needed, to provide the EV technology possibilities for its growth. From a technical perspective, this implies modifications in the city’s electrical network capacity that may reduce its reliability and availability [8]. To assure a secure transition, a detailed plan should be executed. Nonetheless due to the urgency for its implementation, many facilities do not account for resilience of the electrical network and do not give space for an adequate planning scheme.

Studies suggest that there is a lack of research effort to understand the technical consequences of the inclusion of EV chargers in the electrical infrastructure [8], [9]. It is already expected, that at least in the city of Amsterdam, an excessive use of the EV charging
stations could lead to an electrical disruption [9]. By itself, the latter is already an undeniable vulnerability. Therefore, it is important to understand the consequences from a technical perspective if a threat such as Stuxnet, exploits this vulnerability.

1.2. Amsterdam: Place for opportunities and cradle for threats

Amsterdam has today the highest density of Electric Vehicles worldwide. In the year 2006 it led the way with 2000 public stations. It has an extensive network of EV public charging stations that offer great possibilities to achieve its sustainability targets, not only from a transportation perspective but also as a potential source of electrical storage.

It was 2009 when Amsterdam introduced its first charging points as an initial step towards a mobility transition. As there was a scarce demand for Electric Vehicles, Amsterdam changed its strategy by increasing the number of public chargers with the aim of raising the confidence of potential drivers [4]. The experiment resulted in a positive outcome with an increase of 1,000 charging points by the year 2011. Today the number of charging points is higher than 4,000 and more than 50,000 charging sessions are registered per month [5].

One of the main keys for its success, is the so-called Dutch Approach. The core of the Dutch Approach is the interoperability of the charging stations: Every car can be charged in any public station with a standard plug, no matter the charger’s company and the subscription of the user [9]. Furthermore, Amsterdam municipality has set a maximum price for the suppliers, making electric driving affordable and attractive. This created a competitive advantage over fuel cars [4].

Approximately only 10 percent of the owners of Electric Vehicles in Amsterdam have access to a private EV charging station. Consequently, the municipality took responsibility and created public stations for those users that did not have one in the proximity of their surroundings. Together with the Distribution System Operator of Amsterdam: Liander, a civil engineering firma: Hijmans, the owner of the charging stations: Nuon and the municipality of Amsterdam, a very efficient process was created for the installation of charging points according to requests from drivers [4].
The process for requesting a charging station consists of ten simple steps which can be visualized in Figure 2.2:

1. **Electric driver makes a request online.**
2. **Nuon/Heijmans review if the requirements are fulfilled.**
3. **Amsterdam Council approves or rejects the installation.**
4. **Nuon/Heijmans create an installation plan.**
5. **Amsterdam council gives the formal permission for the installation.**
6. **The location and plan are published online.**
7. **Contractor requests permission for a grid connection.**
8. **Amsterdam Council instructs installation in that particular location.**
9. **Nuon/Heijmans start planning the work.**
10. **Contractor installs the station in a period of four hours.**

Figure 1.5: The ten-step process for requesting a charging station

The process starts when the user requests online a public charging station in its surroundings (Web Page: [https://www.nuon.nl/producten/elektrisch-rijden/laadpaal/openbaar/laadpaal-amsterdam/](https://www.nuon.nl/producten/elektrisch-rijden/laadpaal/openbaar/laadpaal-amsterdam/)). Nuon and Heijmans review the requirements which include the walking distance to the nearest charging station, the occupancy rate and if any previous request were turned down. Once the requirements are reviewed, Amsterdam city council decides if a new location should be installed and if the result is positive Noun, Heijmans and Liander start with the formulation of an installation plan. In this moment, Amsterdam Council concedes the formal permission to start the installation and the location of the planned charging station is published online. At this point, the contractor should request Liander a connection to the grid and after a soil survey Liander will allocate the connection and release it for installation. The final step is the installation of the charging point by the contractor and its availability is published online [4].

As the process visualized in Figure 2.2 reduces the time-to-installation significantly, it also gives rise to other issues that have already been brought to light by the academia and the municipality itself. Highlighted by studies of the Amsterdam University of Applied Sciences (AUAS), there is not enough research to estimate if the electrical grid has enough capacity to withstand the increasing demand due to the rise in numbers of charging sessions together with the conventional loads (residential, commercial, industrial, etc.) [5]. Efforts are now focusing on influencing the charging behaviour of the electrical drivers in order to reduce the use of charging sessions during peak hours [16].
Researchers from AUAS use data analysis to understand patterns and find solutions. It is already a fact that peaks in energy demand will present a real challenge for the city of Amsterdam and they are certain that the network will not be able to cope with it [9].

1.3. **SCOPE OF THE RESEARCH WORK**

The motivation behind this research work is in first place to understand if the capacity of the current electrical distribution grid is enough to withstand an attack of this magnitude and secondly, how a cyber attack to the EV Charging Infrastructure can be performed. This work will consider the present situation of the city of Amsterdam but will also focus on simulating future scenarios as is imperative for an adequate planning of the infrastructure of the city. It is expected that this research work will contribute to the future creation of a more resilient infrastructure and that it can be also used as a framework for other cities that also pursue a zero-emission target by the inclusion of EV.

Research efforts have been carried on analyzing potential attacks in solar panels where the attacker targets PV installations with the aim of causing a power outage [5]. Other research efforts have analyzed the possibility that a massive use of botnets can cause the instability of the grid in the frequency at the transmission level [6]. Moreover, most of the studies carried in the cyber security of smart grid technologies are targeting potential attacks in the SCADA system [7]. Nonetheless, as far as the author has knowledge, research studies have not been focusing yet on a cyber security assessment of the Electric Vehicle Charging Stations and its impact from a grid level. Therefore in this research work we are interested in answering the following questions:

- **How will Amsterdam’s Electrical Distribution Network and its components behave if an attacker compromises all the EV Charging Stations for the present and future scenarios?**

- **Which are the most vulnerable locations that could be compromised?**

- **Which are the potential steps than an attacker will likely follow to compromise the EV Charging Station Control System?**

The methodology that will be used to solve these research questions will cover the steps that a malicious willing third-party will likely follow to have a successful outcome. This methodology was previously applied in the military sector and Lockheed Martin used it as a framework modelling of a cyber attack scenario. This framework is named the *Kill Chain* and an adaptation of it to Industrial Control Systems (ICS), as described in [5], will be used in this research work. It consists of two stages and eight steps that describe the movements that a potential attacker will likely follow to perform an attack on an ICS. These steps were similar to those followed in the Stuxnet attack scenario. For this research work a similar approach will be used. The detailed explanation of the Industrial
Control System Kill Chain will be further elaborated in Chapter 3.

The next chapter will be focused on explaining the elements that a potential malicious adversary would need to understand, to perform a successful attack to the Electric Vehicle Charging Infrastructure in Amsterdam. These elements include the topology of the city, the electrical demand per hour and per season, the distribution, density and characteristics of the EV charging station infrastructure and the EV charging station’s communication framework. Moreover, other aspects such as the motivation behind an attack to an ICS and the development of a potential attack scenario will be also discussed.
It is a fact that we humans are animals that share the three main needs with other animals: food, sleep and shelter. What makes us different is the capacity to ask ‘Why?’ Curiosity is a unique characteristic that we humans possess. The capacity to create knowledge and learn is what makes us evolve and what leads to innovation. Asking ‘Why?’ is what makes a kid learn a language and it is also asking ‘Why?’ what makes a hacker compromise the whole electrical grid.
2.1. INTRODUCTION

In the last chapter, we have mentioned how Amsterdam is considered as one of the most important early adopters of electric mobility worldwide. Their aim for achieving a successful transition towards a sustainable future, has taken the city to establish attractive measures to encourage the use of electric vehicles [4]. The Dutch Approach has made this possible, and the ease and efficiency of any related process have accelerated this transition. As mentioned previously, few EV users have access to a private charger. To solve this problem, Amsterdam municipality established a simple process where the user can request online the construction of a public charging station [4]. As there is not enough research to understand if the electrical grid can withstand a simultaneous increase in the loads, a technical analysis will be developed.

Before performing any attack, four key questions need to be answered: Where? When? What? Why? This answers correspond to the background information that every hacker will need to know to perform a successful attack [10]. According to Doerr [10] the three key elements that are always present in an attack are: Means, Motives and Opportunity. Therefore, while answering the question When? and Where? the opportunity will be understood, the answer of the question What? will correspond to the means and the answer for Why? will make allusion to the motives. Each one of the following sections in this chapter will be focused on answering these questions.

2.2. WHY? THE MOTIVATION BEHIND AN ATTACK

One of the most important factors is the motivation behind every cyber-attack. Understanding the motivation can lead to know what a potential adversary is looking for and also can lead to establish adequate protection measures against them. The main difference between a conventional Information Technology (IT) attack and an attack to an Industrial Control System (ICS), is that an IT attack may be composed of conventional and publicly known attack techniques, where the attacker does not necessarily need to have a very specific knowledge of the system. On the other hand, an attack to an ICS is always a part of a campaign [11]. A campaign is categorized as an Advance Persistent Threat, where the attacker has a clear motivation and requires a higher level of knowledge regarding how the targeted Industrial Control System works. A campaign consists of a very structured attack where every step needs to be predefined which increases its complexity [11]. Attackers targeting ICS need to have high levels of expertise.

In an Advance Persistent Threat, having a clear understanding of the motivation behind the cyber attack can lead to generate adequate and more specific protection measures. According to Gandhi et al. (2011) [12], the motivations behind a cyber-attack can be classified in three main dimensions that can be visualized in Figure 2.1:
2.2. Why? The motivation behind an attack

Figure 2.1: Motivation behind Cyber Attacks by type: Socio-Cultural, Political and Economical

1. Socio-Cultural
The motivation behind these attacks is based on social or cultural factors that are present in the adversary’s surroundings. Social factors relate to entity behaviour as a part of a community and its interaction, while cultural factors are a set of norms and traditions that are transmitted through generations in an ethnic group or nation. Examples of socio-cultural motivations range from an unsatisfied employee or sabotage up to a cracker looking forward to enhance their reputation. Social-cultural factors also play a very important role contributing in hacktivism, terrorism or cyber-war [12].

2. Political
Political motivations are based on activities related with government polices or their administrative practices. Any political decision that results unfavourable to another party, can be a crucial motivation for starting a cyber attack. Examples of political attacks range from cyber-spionage by state actors up to hacktivism, cyber-war and terrorism. Political factors are one of the main concerns when analyzing the motivation behind ICS attacks.

3. Economical
Economical motivations imply a monetary or valuable reward by performing a successful attack. The rewards by accessing, manipulating or just by leaking information of the system can be very high. The size of the reward vary according to different factors such as the importance of the ICS and the complexity of the attack. Economical motives also play a very important role contributing to cyber-war, terrorism or industrial espionage.

For each one of these factors, different security and defense strategies should be considered when developing a safety plan. It is crucial to conduct an analysis to understand the likelihood of each motivation and generate a structured plan accordingly [10].
2.3. **WHERE? SELECTING THE AREA OF ATTACK**

In continuum mechanics a control area is defined as a mathematical abstraction that allows the definition of boundaries in order to perform a determined analysis [13]. Following, such definition, this section will be mainly focus on finding the most adequate control area for performing the attack. The control area selected in the region of Amsterdam is in function of the following variables:

\[ CA = f(Ta, Az, \delta_P, Ed, \delta_{CS}) \]

Where:

- \(Ta\) - Amsterdam’s City Topology
- \(Az\) - Main Activity (Commercial, Industrial, Residential)
- \(\delta_P\) - Population Density
- \(Ed\) - Electrical Demand
- \(\delta_{CS}\) - Electric Vehicle Chargers Density

The distribution of the population across the different zones of Amsterdam is highly related with the electricity demand per zone and also to the main activity developed. In this section it will be shown that the electrical vehicle chargers density has also a direct relation with the population density and the activity per zone. Understanding the city’s topology is fundamental to identify an adequate control zone and also to make an adequate sub-division in order to distribute the loads, EV chargers, sub-stations or any other element that could support to structure the model.

In the following paragraphs, each one of the variables will be defined together with their maps to understand graphically their behaviour in Amsterdam’s different zones. Finally, a relational analysis of these variables will be made to define the area of attack.

**1. Amsterdam Topology (Ta)**

The city of Amsterdam is divided in seven zones: North, Centre, East, West, New-West, South and South East. Their four-digit post codes division goes from 1000 up to 1108 and is expanded to a six-digit sub-division. It has 41 neighborhoods distributed across them [14]. Amsterdam’s topology and zone’s division can be visualized in Figure 2.2.

Figure 2.2 shows in red circles the seven Amsterdam’s zones. The lines in light blue indicate the borders between each zone and the line in dark blue marks the division of the borders of Amsterdam as a city. In the following paragraphs, the analysis of each one of the different variables will be made, following the 7-zone division showed in Figure 2.2.
2. Main Activity per zone (Az)

The main activity per zone includes the classification between residential, commercial and industrial activities [16]. These can be visualized in Figure 2.3a. The different colors signalize the type of activity: Blue stands for business and industrial activities, orange for commercial, green for residential and yellow is the mixture of residential and commercial. As it can be seen, most of the commercial activities are mainly in the center and East, while the industrial and businesses activities are located in Westpoort and partially in Amsterdam North. The residential sector is distributed along the city, with an exception of Westpoort which is mainly used for different types of Industrial Activities.

3. Population Density (Dp)

The population density has a direct correlation between the electrical demand, the main activity developed in the area, and consequently, the amount of electric vehicle chargers. As the population density increases per zone, it is evident that the electrical demand will also increase and so will the need for more charging stations. The population density can be visualized in Figure 2.3b. The highest population density is presented in dark blue and the color intensity decreases proportionally to the density. Five shades of blue can be identified in the map. The darkest blue section corresponds to densities higher than 2500 inhabitants per square kilometer, the second one goes from 750 to 2500, the third goes from 250 to 750, the fourth from 150 to 250 and finally the white section corresponds to a density lower than 150 inhabitants per square kilometer [17]. As it can be seen the highest population density is located in the Center, New-West, South, East and South-East, followed by a Amsterdam North. Westpoort has the lowest population density and this is due the aforementioned use of industrial activities [15].
4. **Electricity Demand** ($E_d$)

Figure 2.3c shows the average electricity demand per zone over a year period. The red color symbolizes the highest electricity demand with a yearly average electricity use of 6000 KWh/year. It is followed by the orange zone where the average demand goes from 5000 to 6000 KWh/year. In the yellow zone it ranges from 4000-5000 KWh/year. In the fourth place, the lemon-green zone has an average demand that ranges from 3000 to 4000 kWh/year. In the turquoise area it ranges from 2000 to 3000 kWh/year and finally the darkest green zone has a yearly average demand lower than 2000 kWh/year. As it is expected, the highest electrical demand is located in the area of Westpoort, due to the industrial activities. The central area also shows a high electrical demand due to the population density and the considerable presence of commercial and residential activities.

5. **Electric Vehicle Chargers Density** ($\delta_{CS}$)

Figure 2.3d displays the density of EV chargers. It can be appreciated that the EV density is proportional to the population density. The most dense zones are the Center, South, East and New-West. The Westpoort and North do not show a strong presence of Electric Vehicle chargers. This can be due the low population density that leads to lower requirement rates. An analysis on EV Chargers density will be further elaborated in Chapter 4.
Most Suitable Area for Performing the Attack

A vulnerable area has a high electrical demand together with a high density of charging stations. As previously mentioned, the highest density of charging stations is among the areas of the Center, South, East and New West, while the lowest density is in North and Wespoort. There is a positive relation between the population density and amount of charging stations, specially in the zones where the main activities are residential and commercial. Westpoort is an industrial area which makes it less likely to have charging stations as the population density and residential or commercial activities are very low.

Regarding the electricity demand per zone, the highest yearly average demand is registered in the Center and in the Westpoort area. The latter is expected as the industrial processes require higher electrical demand than other activities. In the Center, it is due to the high population density and amount of residential and commercial activities.

By considering the aforementioned elements, the control area where the attack will be launched has been selected. Figure 2.4 shows the control area enclosed by a red circle. The most vulnerable zone is Amsterdam Centre as it has the highest electrical demand and the highest density of EV Chargers. The other regions, show a less extreme scenario where the electrical demand ranges from medium to high as well as the number of EV chargers. Nonetheless, considering these non-extreme cases is also important to make a proper valuation of the security of the city. The zones that were not considered in the attack scenario are Westpoort and a part of Amsterdam North as even if they have a high electrical demand, the amount of charging stations is very low. As a consequence an attack against these charging stations will not cause a considerable impact. South West will also not be considered due to the low density of charging stations.
2.4. WHEN? THE ELECTRICAL DEMAND & CHARGING BEHAVIOUR

The next aspect that should be carefully analyzed is the determination of the best moment to launch the attack. The moment is chosen taking into account two important elements: The charging behaviour of the EV users and the electricity demand fluctuation per hour in the previously defined region. Aspects such as seasonal variations were also taken into account as they increase or decrease the resilience of the network [25].

1. User’s behavioural analysis for EV Charging

Research carried by the Catalonia Institute of Technology [21], studied the European EV Charging behaviour by monitoring 2,762 charging points during a period of three years in seven different European Countries. They made a differentiation between municipality (public), private company and private user EV charging stations. Figure 2.5 shows the results of the research by these three sectors:

![Figure 2.5: Histogram of relative charging frequency by EV ownership Ref. [18]](image)

This research work will be only focused on public charging station. Therefore the results provided by the upper histogram are the ones that will be taken into account. For public charging stations, there are two blocks of peaks registered. Two in the morning at 10:00, 11:00 (working hours) and the other in the evening at 21:00 and 22:00 (after-working hours). Further research carried by Smith et. al (2011) [22] in battery optimization suggests that EVs are parked from 21:00 to 7:00 and at working hours from 9:00 to 15:00. Kelly et al. (2012) [23] suggests that the charging peak starts at 21:00 and finishes at 4:00. Taking into account these results, the most suitable time is considered at **21:00**.
2.4. **When? The Electrical Demand & Charging Behaviour**

**2. Electrical hourly demand in Amsterdam**

The electrical demand per hour in the city of Amsterdam has been analyzed using data provided by the Distribution System Operator in charge of this region: Liander [24]. The data has been processed with the software Tableau for visualization purposes. Figure 2.6 shows the average electrical demand for summer (June-September) and winter (December-February) per hour in a day. The data shows the aggregation of the demand over a year period (2015) of 10,000 customers. The figure on the left shows the summer demand behaviour while the figure on the right shows the demand on the winter period.

![Figure 2.6: Average summer and winter hourly electrical demand in Amsterdam per 10,000 customers in kWh/h](image)

The electrical demand on summer that is visualized in Figure 2.6a, shows a peak at 19:00 hours with an equivalent of 31.13 [kWh/h]. The second highest peak is detected at 21:00 hours with a value of 30.90 [kWh/h]. Moreover the lowest value during the day is at 3:00 with a value of 13.01 [kWh/h].

![a) Summer Hourly Electrical Demand](image)

The winter case is visualized in Figure 2.6b, where the highest demand peak is at 19:00 hours with an equivalent value of 36.53 [kW/h]. The value of the electrical demand at 21:00 is 30.93 [kWh/h].

Even though the electrical demand peak is higher in winter than in summer, the electrical distribution network infrastructure has a lower stability in summer period as the elements that compose the grid (cables, transformers, feeders) are more sensitive to an increase in the temperature [25]. Moreover, considering that the peak registered for EV charging is at 21:00, the electrical demand for summer and for winter at this hour is almost the same with a difference of 0.03 [kWh/h]. Furthermore, it is important to make emphasis that in summer period the second highest electricity peak is also registered at 21:00 hours. Consequently from an attacker perspective, it is reasonable to assume that the best moment to launch the attack would be at **21:00** hours of a summer period.
2.5. **What? The EV Charging Infrastructure**

In order to successfully supply electricity to an electric vehicle, multiple series of steps should be fulfilled in order to make it possible. From an attacker perspective, it is important to understand each step of the process before executing the attack, because targeting an ICS requires a high level of expertise of the process itself. Figure 2.7 shows the different steps together with the actors involved and the communication protocols used. A reliable communication between each one of these parties is imperative in order to assure correct operation.

![Figure 2.7: The EV Charging Station Infrastructure and communication protocols](image)

Figure 2.7 shows the different actors involved in the EV charging process (in black), together with their communication protocols inside the circles. The protocol in a red circle - the OCPP protocol - plays a fundamental role in the development of this research work and will be further explained at the end of this section. The role and description of each actor will be described in the following paragraphs:

1. **Charge Point**

   The charge point is the device that supplies electricity to the electric vehicle. There are three different types of charging levels. Type 1 provides 1 kW and the charging time ranges from 8 to 15 hours. Type 2 provides from 3 up to 20 kW and the charging time goes from 3 to 8 hours. Type 3 provides 50 kW and the charging time goes from 20 minutes to even 1 minute [27]. The element that connects the EV with the charger is named connector. There are two types of connectors, however to ensure the interoperability of charging stations, Europe has adapted the connector Type 2 (IEC 62196). The functions of the charging point are: Controlling the amount of energy transmitted to the EV (using the Electric Vehicle Supply Equipment), collecting the measurements of each charge level, identifying users and allowing or rejecting the charging sessions accordingly, and finally, executing remote commands from the CPO system using a local controller over a WAN interface [28]. The latter is crucial for this research work.
2. Charge Point Operator (CPO)

The Charge Point Operator (CPO) is the entity that is in charge of controlling the activities of all charging stations under its domain. The CPO is connected to the charging stations via a WAN interface and communicates with them via an open source protocol named OCPP (Open Charge Point Protocol). This protocol will be discussed at the end of this section. Activities carried on by the CPO include conceding permission to the user to effectuate a charging session, gathering the measurements given by each charging point, communicating with the Distribution System Operator (DSO) to exchange data and forecast values, and most importantly, establishing the energy limits to control the energy flow between the EV and the Charge Point. The establishment of these limits is achieved together with the DSO in order to safeguard the electrical infrastructure [27].

3. Distribution System Operator (DSO)

The Distribution System Operator (DSO) is the entity that is in charge of distributing the energy at intermediate and low voltage levels to end-customers. The medium voltage levels in The Netherlands according to the Dutch Energy Research Program, range from 3 to 30 KV and the low voltage levels range from 230 to 400 V [26]. The DSO network is directly connected to the Transmission System Operator (TSO) which is in charge of the transmission of electricity at a national level. The voltage levels from TSO to DSO are lowered using distribution transformers. The role of the DSO in the EV Charging Infrastructure is on one side to provide the electrical energy needed for the charging of the vehicle, and on the other side to forecast the EV voltage demand and exchange this information with the CPO to ensure the stability of the distribution grid [27].

4. Energy Supplier

The role of the Energy Supplier is to provide the electricity to the DSO going first from the Transmission System Operator (TSO) and then lowering its voltage levels. The DSO acts according to the exchange of information with the Energy Supplier and can ask, for example, the CPO to reduce its energy consumption levels [27].

5. E-mobility Service Provider (EMSP)

The E-mobility Service Provider (EMSP) is in charge of billing the user according to the amount of energy that has consumed during the EV charging session. In order to complete this task, it requests the necessary information about the CPO which it gets directly from the Charge Point [27]. Even though the EMSP has a fundamental role in the EV charging process, it will not be considered in the following research work.
2.5.1. The EV Charging Communication Protocols

The communication infrastructure is the platform that allows the transfer of information between the aforementioned partners. It consists of three main elements which are the protocols, the interfaces and the exchanged information [28]. As the attack will be focused on the communication between the CPO and the charging point, special emphasis will be made on explaining the OCPP protocol and the different commands that can be sent to the charging point. This section provides an overview on the protocols and the interfaces used by the process.

Communication Protocols

Figure 2.7 shows the different protocols that are being used for the communication by the different entities. The dutch company ElaadNL conducted a research study regarding the different protocols used on the EV communication process [8]. This study focuses on evaluating the different available protocols and the capabilities that they offer. Table 2.1 summarizes the communication protocols displayed in Figure 2.7 and gives an overview of their capabilities.

<table>
<thead>
<tr>
<th></th>
<th>OSCP</th>
<th>OCPP</th>
<th>OCHP</th>
<th>OICP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize Charging Session</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Billing</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>EV Charging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling Registration</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Grid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operate Charge Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide Charge Point Info</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reservation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roaming</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Charging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2.1: Protocols in the EV Charging Infrastructure with their functionalities

Each one of the different protocols displayed in Table 2.1 fulfills an specific task in different parts of the EV Charging Process. It is important to mention that besides these four, there are other protocols that were created with the goal to fulfill the same requirements. These are also covered in ElaadNL study. Nonetheless for this research work, only these four are considered as those are the ones that are being used today in The Netherlands.

For the development of the attack scenario that will be covered in this research work, the most important protocol is the OCPP protocol. This is the one in charge of managing the communication between the Charging Station and the CPO. In the following paragraph an introduction to the OCPP protocol and its capabilities will be given.

OCPP stands for Open Charge Point Protocol. It has been designed to standardize the
communications between the EV charging point and the CPO system. This is an open source protocol and its main characteristic is the easiness to change from one network to another, without replacing the charging stations. The protocol has also the possibility to exchange information related with transactions, maintenance and even to be used to schedule EV charging sessions [29]. OCPP has become de facto open protocol for EV Charging-CPO communications in Europe and in some parts of the United States. As it can be displayed in Table 2.1 the cases that are supported by the OCPP are: Authorization of the charging session, billing, management of the grid, operation of the charge point, reservation of a charging session and smart charging. According to ElaadNL [27], the maturity of the protocol is categorized as high as well as its market adoption. OCPP is accessible to any entity and is publicly available from the website of Open Charge Alliance. Figure 2.8 shows a scheme of the cases supported by OCPP.

Figure 2.8 shows all the user cases from the CPO perspective that are supported by OCPP. OCPP supports sixteen different cases that are displayed on the green circles of Figure 2.8 [30]. The most important case for this research work is the Smart Charging Command that allows the CPO to manage remotely the power consumption of the charging point [29]. This is the command that allows the CPO to increase (or decrease) the amount of power consumed by the power station in a determined charging session [29]. The goal of the attack scenario in this research work will be to manage the charging stations using the Smart Charging Command increasing their power levels.
2.5.2. The EV Charging Communication Interfaces

An interface is defined as a shared path between two different components with the objective of exchanging information. There are several types of interfaces according to the technical and security requirements of the established communication [28]. In an EV Infrastructure the most important interfaces are:

1. **WAN Interfaces**
   WAN stands for Wide Area Network and is the interface that connects the Charge Point to the CPO system. This communication is set either by a network operator or by the CPO. Usually the connections are GPRS, CDMA, glass fiber or DSL based. There are two communication paths that run in the WAN interface. The first one is the Information Communication which makes use of the OCPP. The second is the Remote Configuration and Maintenance which, as its name suggest, allows engineers to send updates, setting adjustments or any other type of maintenance activities [28]. The WAN interface is the most important in this research work as the attack will be performed through this channel. It is important to mention that attacks on the Remote Configuration and Maintenance are also possible. Nonetheless, they will not be a part of the scope in this research work.

2. **Local Network Interface**
   The Local Network Interface is the platform that connects the Local Controller through the Electric Vehicle Supply Equipment (EVSE) and other devices inside the Charge Point. Therefore, it allows the communication inside all the elements contained in the charging station. The communication in this interface is mainly based with on the RS232 protocol [25]. Attacks at this interface level have been studied in research and are considered highly important. Nonetheless, they will not be considered as a part of this research work.

3. **DSO to CPO Interface**
   This is the interface that assures a reliable communication between the DSO and the Charging Point Operator. Similar to the WAN interface, the DSO to CPO interface can be hosted either by the CPO or by an intercommunication operator. The protocol used is the OSCP protocol and is TCP/IP based [28]. This interface will not play an important role for the attack scenario in the following thesis work but is also prone to be attacked.

4. **Other Interfaces**
   Other interfaces that are also part of the EV communication infrastructure are: The Authentication Terminal Interface, the User Authentication Interface, the power switch interface, the plug interface, the electric vehicle interface and the meter interface [28]. All of the above also play a very important role for the operation of the charging stations. This research work will not consider the vulnerabilities that may be found in these interfaces. Nonetheless, security measures at this level are also important to be considered.
2.6. Summary

The objective of this chapter is to provide the reader with the background information that every potential attacker would need to know in order to structure an attack against the Electric Vehicle Charging Station Infrastructure in Amsterdam. The structure of this chapter follows the answers of the questions that are needed to be answered by any potential adversary: What?, When?, Where? and Why? which at the same time disclose the elements that are always present in any attack: means, motive and opportunity.

The chapter starts by answering the question Why? which is related to the motives of a cyber attack. According to Gandhi R. A. et al., the motivation of any cyber-attack can be classified in three main dimensions: Socio-cultural, political and economical. Examples that can be common drivers for targeting ICS range from terrorism, cyber-war, reputation, hacktivism, economical gain, among others.

The second part of the chapter answers the questions Where? and When? that are related to the opportunity of the adversary. The answer to the question Where? focuses on finding the most suitable control zone to perform the attack. This control zone is in function of different variables such as: Amsterdam's city topology division, population density, main activity per area (residential, commercial or industrial) and electric vehicle chargers density. As there is a correlation between the aforementioned elements the most vulnerable zone is identified as the one with the highest average electrical demand and the highest EV chargers density. This is considered as the most sensitive scenario. Other less sensitive zones are also considered because they are non-extreme cases that are also important to understand. The answer to the question When? formulates the best time to perform the attack. For this section, two elements are taken into account: The EV charging users’ behaviour and the hourly peak electrical demand in Amsterdam per season. After performing an analysis on both elements, the reasonable assumption for performing the attack at 21:00 hour in a summer period is selected.

Finally, the third part of the chapter answers the question What? that is related with the means of the attacker. In this chapter the EV charging infrastructure is analyzed together with the main actors and the communication paths. Understanding the infrastructure of the Industrial Control System is the mean to perform the attack. This chapter starts by explaining the series of steps and the actors that are involved in the EV charging process together with their communication protocols. A brief explanation on the activity of each protocol is given with special emphasis to the OCPP as this will be the mean to perform the attack. Finally, the last part of this chapter focuses on the communication interfaces present in the EV charging architecture and their importance for launching an attack.

In the next chapter the methodology that will be used in this research work will be explained followed by the proposed attack scenario. It is important to mention that the attack scenario may vary depending on the adversary. Nonetheless, several elements should be taken into account in order to propose an initial defense plan that could improve the resilience of the ICS system.
Figure 2.8: OCPP Protocol communication scenarios. The red circle indicates the Smart Charging Command Ref. [26]
A chain is not stronger than its weakest link,
And life is after all a chain
William James

"Cyberattacks aren't new, but the stakes at every level are higher than ever. Adversaries are more sophisticated, well-resourced, trained, and adept at launching skillfully planned intrusion campaigns called Advanced Persistent Threats (APT). Our nation's security and prosperity depend on critical infrastructure. Protecting these assets requires a clear understanding of our adversaries, their motivations and strategies. Adversaries are intent on the compromise and extraction of data for economic, political and national security advancement. Even worse, adversaries have demonstrated their willingness to conduct destructive attacks. Their tools and techniques have the ability to defeat most common computer network defense mechanisms."

Lockheed Marteen
3.1. **Introduction to the Kill Chain**

The Kill Chain is a methodology developed by Lockheed Martin that was originally used for military purposes. It shows the structure of an attack from an information security perspective, when modelling the intrusion of a host or network. The military model consists of six different phases: Find (the target), Fix (their location), Track (their movements), Target (with an appropriate weapon), Engage (apply the weapon) and Assess (Evaluate the effects of the attack) [32]. This model is also known as F2T2EA, which are the initials of the six steps. The term "chain" makes allusion to the fact that a potential interruption disrupts the whole process [10]. So the strength of the whole chain, depends on the strength of its weakest link.

From an information technology perspective, the scientists of Lockheed Martin adopted the F2T2EA and created a kill chain focused on the potential steps that an attacker will follow to achieve a cyber attack or intrusion to a host or network. The kill chain does not just focus on how to attack but also on how to defend. This framework is a part of the Intelligence Driven Defense, which is a philosophy of the company that focuses on stopping offensive maneuvers during an attack while having a defensive posture [29]. As mentioned previously, if the defender knows how to interrupt the chain at any step it will prevent the attack to develop further. Moreover, understanding how the attacker could compromise each step, can help the defender to interpret the security level and breaches of the systems. As every attack have different nuances and can be developed from different perspectives, the literature suggests that variations in this methodology are valid [30]. Figure 3.1 shows the steps of the Cyber Kill Chain by Lockheed Martin:

![Figure 3.1: Cyber Kill Chain Methodology by Lockheed Martin](image)

The main difference between IT attacks and Industrial Control System (ICS) attacks is that in the latter, all the components are designed in unique ways depending on the application [33]. Therefore, the Kill Chain from Lockheed Martin has been adapted by Michael J. Assamte and Robert M. Lee creating the Industrial Control System Cyber Kill Chain where the conventional Kill Chain is used as a foundation.
An ICS attack requires in first place, that the adversaries are aware of the type of processes that are automated and have knowledge of the engineering decisions and the design of the Industrial Control and Safety systems. Another difference between them is the nature of the objective. Most of the ICS attacks registered have as final goal, the physical damage to equipment rather than espionage or theft of information. Moreover, an attacker targeting an ICS have a deeper level of knowledge regarding the system operation, as most of the ICS are tailor made according to its application [33]. In a later stage of this chapter, the classification of the attacker objectives will also be discussed together with the characteristics of the attack scenario in this research work.

The authors M. Lee and Assamte segregated the ICS cyber Kill Chain in a double stage process where the first part is called *Cyber Intrusion, Preparation and Execution* and follows a similar logic to the one of the traditional Lockheed Martin’s Cyber Kill Chain. The second one is called *ICS Attack Development and Execution* and focuses solely on the attack at the Industrial Control System level. Both stages combined have a total of eight steps. In Stage I, the goal is to gather information and access the IT systems as a previous step to accessing the ICS. In Stage II, the information acquired during Stage I is used to develop and test a potential attack against an ICS [33]. In the following paragraphs the steps of each one of the two stages will be explained in detail and the application of the ICS Cyber Kill Chain on this thesis work will be discussed.
3.2. **Stage 1: Cyber Intrusion, Preparation & Execution**

As previously mentioned, the ICS Cyber Kill Chain consist of two stages. Stage I covers the activities that would allow the attacker to intrude into the IT systems. The steps on this stage are similar to the ones followed in the traditional Cyber Kill Chain. The objective of Stage I is to gain the necessary information and access in order to launch the attack against the targeted Industrial Control System in Stage II [33]. Figure 3.2 introduces the five steps of Stage I:
1. Planning

Planning is the first step of Stage I. The objective is gathering as much information as possible using any available means. This is known in the traditional Cyber Kill Chain as *Reconnaissance*. The type of information that can be gathered during this stage ranges from social, technical (network, host, protocol-type) up to policies, processes and procedures [35]. The process for gathering information can be passive, also called footprinting, or active. Passive reconnaissance means that the attacker does not interact directly with the victim, while active reconnaissance implies a certain level of contact [13]. Several commercial tools available online can be also used for helping to gather information such as *nmap, nslookup, whois*, etc, as well as the use of search engines. Social Engineering is also a widely known approach to obtain valuable information [34]. The output of the reconnaissance step is the acquisition of sufficient information to achieve a successful attack and the identification of vulnerabilities that could be exploited in later stages.

2. Preparation

The second step of Stage I, the preparation phase, includes two parts that are not compulsory dependant one of the other: Weaponization and Targeting. Weaponization is the procedure of finding an adequate tool which can bypass any vulnerability found on step 1 (Planning, reconnaissance). An example of weaponization is the use of malware hidden in harmless files that could lead to the exploitation of a determined vulnerability [33]. On the other hand, targeting is the procedure of identifying potential victims or vulnerabilities in order to select the most suitable “weapon”. The perfect target has an appropriate balance between the effort required, the time needed, the likelihood of success and the risk of being detected [34]. As mentioned before, targeting is not compulsory followed by weaponization. An example of the latter is by obtaining the credentials of the selected target and therefore, the weaponization step can be avoided. The preparation phase is needed in order to proceed to the next step: The intrusion.

3. Cyber Intrusion

Cyber Intrusion is the third step of Stage I. It includes three important sub-steps: Delivery, Exploitation and Installation or Modification. The cyber intrusion phase can be also sub divided into two major phases: Attempt and Success, where the delivery remains in the Attempt phase, exploitation in both and installation in the Success phase [32].

*Delivery* stands for the channel that the attacker selects for "delivering" the exploit to the victim. The delivery method can range from emails with attached malicious links or files, scripts up to USBs or any other device that contains the selected weapon. *Exploitation* is the process where the weapon chosen, takes advantage of the vulnerability and intrude into the system. Finally this will lead to the *installation* of the necessary tools that the adversary could use to launch the attack. The installed tools range from backdoors, key loggers and most importantly, remote shells to control remotely the targeted system [34]. This leads to next step which is the Management and Enablement.
4. Management & Enablement

Management & Enablement is the fourth step of Stage I. Due to the installation of the remote shells, the attacker establishes a command and control path to the targeted system. Some attacks even use more than one command and control connection to avoid losing connectivity. The communication exchanged between the targeted host and the adversary can be hidden between the normal inbound or outbound traffic where the adversaries tend to select the busiest time in the network traffic to remain hidden [33].

5. Sustainment, entrechment, development and execution

This is the fifth and last step of Stage I. The adversary acts and achieve the first set of actions according to its pre-established goal. The actions can vary from discovering new systems or hosts, getting users credentials, collecting desired data, manipulating systems, among others. In this stage, the attacker can also take the necessary measures to avoid being detected. These measures can range from erasing any trace of its activity up to replicating normal system's data to trick the operators into believing that everything works fine [33].

As mentioned before, the output of Stage I is crucial for planning and executing Stage II which will be discussed in the next section. The reason why the ICS Cyber Kill Chain is divided into two Stages is because most of the Industrial Control Systems do not have a direct connectivity to the internet and not even to the company's internal network. Due to such architecture, compromising these systems require an extensive and more tailored knowledge in comparison with the traditional IT systems. Therefore, it is necessary to first infiltrate into the company's network (Stage I) to obtain the necessary resources. This can lead to accessing the ICS network (Stage II) or to performing host jumping until a successful intrusion is achieved. However, some ICS do have a direct connection to the internet as this facilitates the communication between parties, but also lowers the security level. It has been reported that two thirds of the Black Energy campaigns are targeting specifically ICS-Internet facing systems [33]. This is the case for the EV Charging Stations Infrastructure, as the control system is cloud-based which lowers the complexity from an attacker perspective. Understanding the steps in Stage I as a defender, is crucial to design the most adequate security measures. Also, understanding how far in the kill chain the attacker was capable to go, can give a very good indication of the system's vulnerability.

The next section will be focused on explaining Stage II. It is already expected that by this stage, the attacker already possesses the necessary information to access the Industrial Control System. The steps that will be described are an addition to the traditional Kill Chain developed by Lockheed Martin.
3.3. **Stage II: ICS Attack Development & Execution**

The Stage II describes the steps that an attacker could potentially follow when targeting a desired Industrial Control System. The attacker must use the knowledge that was gained during Stage I as input. As every ICS is tailored to a certain application, an attack to an ICS is not of random nature and implies a clear intention from the adversary. These complex campaigns can take years to develop, as acquiring the specific information and know-how of the ICS requires a high level of expertise. The information needed can range from the type of hardware used, its manufacturer, the ICS’s operational processes, normal operation data, system policies, among other elements [7]. Figure 3.3 shows the three steps that compose the ICS Attack Development and Execution Stage.

![Figure 3.3: Three steps of the ICS Cyber Kill Chain Stage II](image)

**1. Attack development & tuning**

This is the first step of Stage II. In this stage the attacker has already the necessary information to understand the vulnerabilities of the targeted ICS and to develop a tailored made attack for the specific target. The attack scenario is in function of the objective/goal of the adversary, the characteristics of the ICS and the attacker’s expertise. There are many different ways on how the attack scenario can be structured. In this research work, an attack scenario based on common registered techniques will be made. Most of the ICS attacks that have been registered imply the manipulation and physical damage of the control systems [33].
2. Validation

This is the second step of Stage II. In this step the attacker must test the already defined ICS attack in a duplicated environment. The information acquired during the reconnaissance stage can lead to select the adequate ICS hardware and software to make this replicated system as similar as the real one. This level of testing is vital in order to assure the potential success of the attack. Testing the attack can also lead to making the necessary modifications if needed. Once the attack is already successfully validated in the duplicated environment, the attack advances to the next step which is delivering it to the victim and executing it in the real environment [33]. This step was also present in the Stuxnet attack scenario as is highly likely that a mirrored environment was developed years before delivering the threat to the victim [7].

3. ICS Attack

This is the third step of Stage II. The development of the ICS attack involve three vital steps that are also present in Stage I: Delivery, Installation or Modification and Execution. As mentioned in the previous section, delivery is the process where the attacker selects the most suitable channel to send the ICS exploit. As most of the ICS are not connected to the internet, most of the delivery techniques range from host-jumping to USB or any other external device infection. Installation or Modification implies the Establishment of necessary elements that lead the attacker to control the system such as the Command and Control Shell and even the use of back-doors. The final step is executing the attack, where the system is already successfully controlled by the adversary and the attack launched [33]. This marks the final step of the Kill Chain.

The outcome of the attack can vary depending on the initial goal of the attacker. This can range from manipulation of processes or equipment, manipulation of data (bad data injection), loss of view, loss of control, etc. Complex attacks also include the know-how on the system’s behaviour in normal conditions and are capable of tricking the operator to think that everything operates in normal conditions while performing the attack. In the next section, two vital elements that define the structure of the Kill Chain will be addressed: The Attack Complexity and the Objective. These two elements should be previously defined by the attacker in order to develop the threat accordingly.
3.4. ICS Attack Complexity and Objectives

Defining the attack complexity and the objectives is the first step that the attacker should fulfill. Both elements will determine the structure of the Kill Chain and also the resources that will be needed. Depending on the goal of the attacker, the complexity to successfully execute it may vary accordingly as well as the resources and effort needed. The following paragraphs will be focused on explaining both elements in detail:

1. Complexity
The complexity of an attack refers to the amount of resources that are needed in order to assure a successful outcome and the level of knowledge that is needed to perform the attack. An Industrial Control System depends on different elements such as the operational processes, policies, security systems, the available data of the system operation, hardware and software used, etc. The complexity of developing the attack depends on the goal of the attacker. According to M. Lee and J. Assante [30], the complexity of an attack an ICS follows the behaviour as expressed in Figure 3.4.

![Figure 3.4: Levels of complexity of an ICS Attack](image)

The authors suggest that the activity that requires less effort is compromising the ICS security as this only implies having potential access to the system without causing any physical damage. The most difficult task is performing the pre-established attack successfully (damaging the availability, integrity or confidentiality of the system) while having an option open for re-attack in the future. Other activities that can be performed by the attacker can be visualized in Figure 3.4 together with their level of complexity.
2. Objectives

The objective of an attack is the most important element, as the development of the Kill Chain will be defined according to it. According to [10], the three main elements that should be safeguarded in any system are: Confidentiality, Availability and Integrity (No Repudiation has been also considered as the fourth element). Depending on the objective of the attack, some of these three elements are violated. The objective of any ICS attack can be classified in three different categories as visualized in Figure 3.5.

The three categories in Figure 3.5: Manipulation, Denial and Loss, also differ in the level of complexity. The most complex is *Manipulation*, as several security layers should be bypassed in order to achieve the manipulation of any system. The attacker can manipulate either the view, the control systems, the safety systems and even the sensors or instruments. The consequences of a successful manipulation attack can range from damage to equipment up to threat for a human life, as the most complex and dangerous one. Manipulation attacks can violate the Integrity, Confidentially and potentially the availability of the systems [33].

A *Denial* Attack implies that the attacker has the access to the control system and can cause the operators to fail to perform certain actions. These can be denial of control of the Industrial Control System, of view of the processes or access the safety systems. This can be the equivalent of a Denial of Service Attack. This also implies a high level of complexity as the attacker should already have access to the ICS network. Nonetheless, according to the authors it is still less complex than a Manipulation Attack. This objective violates the availability and potentially the confidentiality of the system [33].

A *Loss* Attack implies that the attacker has already obtained access to the control system and can cause the operators to lose either view or control of the Industrial Control System. The loss attack violates the availability of the system.
3.5. The Attack Scenario

An Attack Scenario is defined as the series of steps that the adversary will follow to perform the attack. Every attack scenario is unique and depends on the creativity, preferences, knowledge and experience of the attacker and also on the victim's characteristics. Once the attack scenario is defined, the kill chain can be used to structure the attack in a more organized manner. For achieving a determined objective, several attack scenarios can be created and the attacker can decide to pursue the one that has the highest probability of success. For this research work the attack scenario in Figure 3.6 has been proposed. It is important to mention that in a real scenario, variations of the proposed attack are possible.
The proposed attack scenario in Figure 3.6 is divided into two main steps. The objective of the first step is to gather information about the victim and the ICS. Questions such as: How does the system work?, Who are the players? are fundamental for the development of the attack. Furthermore, obtaining information from an IT level is essential. Questions such as Which is the type of the server?, What is the Operational System?, Which are the relevant IPs? are also part of the scope.

Once this information has been successfully obtained, the attacker advances to the next step which is gaining access to the system. In this section two potential paths can be followed by the attacker. As we already know that the EV charging station control system is cloud based, the first scenario focuses on compromising the server that contains the credentials information. The second scenario focuses on targeting the working station of the person in charge of managing the EV charging stations and getting access to his/hers credentials. Even tough, both scenarios lead to the control of the charging stations, the first one can have a major impact as several credentials or other relevant information can be stolen. Nonetheless the second one has a lower level of complexity.

Figure 3.6 structures the answer of the third research question: Which are the potential steps than an attacker will likely follow to compromise the EV Charging Station Control System? The next chapter will be focused on structuring the proposed attack scenario in the ICS Cyber Kill Chain methodology previously explained. As mentioned before, diverse attack scenarios can be developed for achieving the same goal, therefore variations to the latter scenario are plausible.
3.6. ICS Cyber Kill Chain applied in the manipulation of Electric Vehicle Charging Stations

The rapid transition of Amsterdam to become a zero emission city in terms of transportation, have lead to ease the process for adopting electrical mobility. As a consequence, the number of charging stations in the last years have increased exponentially and will keep increasing until achieving the zero emissions goal. The question that has been risen by the academia and the municipality itself is if the electrical grid is capable to withstand this increment as there is a notably lack of research from a technical perspective.

Since the discovery of Stuxnet, ICS attacks have become one of the major concerns and safeguarding the electrical infrastructure is now a matter of National Security. As the uncontrolled increase of Electric Vehicle chargers is a clear vulnerability of the electrical distribution network, it can also be exploited. Therefore, in order to evaluate this potential attack, the methodology of the Kill Chain will be adopted to the previously discussed attack scenario to structure the steps that will be followed in this research work.

Objectives and Complexity of the Attack

As mentioned in the last section, prior the development of the Kill Chain, the objectives need to be clearly defined as well as the complexity of the attack to understand the resources that will be required. The objectives of the attack scenario in this research work (which are also addressed in the research questions from Chapter I) are:

1. Access the system that controls the EV Charging Stations in Amsterdam.
2. Manipulate all the charging stations at peak electricity demand hour.
3. Evaluate the potential damage in the components of the distribution grid.
4. Evaluate the previous objectives for a future scenario with double number of the charging stations of today and for the 2025 panorama.

The complexity of this attack scenario, according to [33] is catalogued as high. The reason for this is that it involves two important steps: the intrusion to the systems and the manipulation of the Industrial Control System.
Therefore, when applying the ICS Cyber Kill Chain to the attack scenario that has been covered in the last section, we can obtain the structure of the attack and the steps that will be carried on in the following research work:

Figure 3.7: ICS Cyber Kill Chain Stage I: Applying the attack scenario of this research work

Figure 3.8: ICS Cyber Kill Chain Stage II: Applying the attack scenario of this research work

Figure 3.7 shows the Kill Chain for Stage I while 3.8 for Stage II. Chapter 4 will be focused on elaborating the steps for Stage I, while Chapter 5 for Stage II.
THINKING LIKE A HACKER: STAGE I

*Invincibility lies in the defence,*  
*The possibility of victory in the attack*  
Sun Tzu

"A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

-That company is still totally Vulnerable-

*Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches*

-Those individuals are still completely vulnerable.-"

Kevin Mitnick
4.1. **INTRODUCTION**

In this section the five steps of Stage I will be developed following the attack scenario that has been proposed in the last chapter. The objective of replicating the attack, is to understand the potential security breaches that the system may occur in order to propose solutions. This test can also help to assess the likelihood of the attack and to give the reader an idea on how an attacker operates. The chapter is divided into sections corresponding to each one of the steps and concludes with a summary of the results.

4.2. **PLANNING: RECONNAISSANCE**

Reconnaissance is the step where the attacker is focused on gathering any type of valuable information in order to find vulnerabilities in the system that can be exploited in order to launch the attack. This step is also referred as Planning because the adversary defines the structure of the attack based on the information found. For the following thesis work, active and passive methods of information gathering were applied in order to assure that all the important elements were covered. For this stage, reconnaissance of the systems was done at three levels that can be visualized in Figure 4.1:

![Figure 4.1: Three Levels covered in the Planning (Reconnaissance) stage](image-url)
Figure 4.1 shows the three main elements that should be known by the attacker before the execution of the attack. These elements are: The operation of the system that controls the EV Charging Station, the characteristics of its IT infrastructure and finally the characteristics of the distribution grid and the physical location of the EV Charging Stations (OT).

For each one of the three steps, sub-questions were defined in order to structure the information that is required. To understand how the system that controls the EV Charging station works, the first element is to find out who are the parties involved and the responsible CPO. Important information regarding the internal organization and key people who work in the company is also necessary as this makes the targeting activities easier. Moreover, understanding how the system works, what activities the operator is responsible of, how does the platform look like, among other elements, are key factors for this stage.

On the other hand, understanding the IT characteristics of the targeted system is necessary to be able to compromise it. The most important elements that need to be understood are the topology and the characteristics of the victim's network and the discovery and identification of hosts that are relevant for gaining access to the ICS. Moreover, in order to achieve a successful intrusion, the vulnerabilities of the host should be identified (open ports or vulnerabilities in the OS) that could consequently lead to the selection of the most suitable weapon.

For launching this attack, having a clear idea of the topology and characteristics of the distribution grid of Amsterdam and the physical location of the charging points is crucial. Being familiar with the Operational Technology aspects of the system is vital to guarantee the success of the attack. This implies identifying the type of cables, voltage levels of the grid, location of substations, feeders, transformers, among all the elements that constitute the grid. Moreover, understanding the electricity demand behaviour is necessary to identify the most suitable moment to launch the attack together with the location of the most vulnerable zones.

The next section covers the information gathered for the three aforementioned elements and an explanation of the procedure of how it was carried on. It is important to mention that only publicly available data was used in this research work.
4.2.1. **How does the system that controls the EV Charging Stations work?**

The first element is to understand how the system that controls the charging stations works. In order to structure this information, three sub questions have been proposed that will facilitate the reconnaissance activities: *Who manages the EV Charging Infrastructure?*, *Who are the key people that work in the company?* and *How does the EV Charging Control system work?* In this section, each question will be answered and the output will conclude with the first section of the Planning stage.

1. **Who manages the EV Charging Infrastructure?**

As discussed in the last chapter, the role of the CPO is to manage and assure the correct operation of the EV charging stations. Amsterdam has a network of six CPOs that operate independently. These are displayed in Table 4.1. From information obtained from the municipality of Amsterdam, the city has today a total of 4084 public EV charging points. Table 4.1 shows the name of the operators, the percentage of occupancy that they have in the city, the number of charging stations that they operate, the type of the station based on their power limits and the accumulated kW installed per CPO:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Coverage %</th>
<th>Num. Stations</th>
<th>Station Type kW</th>
<th>Total kW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alfen</td>
<td>0.33</td>
<td>16</td>
<td>11.5</td>
<td>184</td>
</tr>
<tr>
<td>Ecotap</td>
<td>1.03</td>
<td>42</td>
<td>22.1</td>
<td>928.2</td>
</tr>
<tr>
<td>EV-box</td>
<td>4.51</td>
<td>184</td>
<td>11.5</td>
<td>2116</td>
</tr>
<tr>
<td>New Motion</td>
<td>3.28</td>
<td>134</td>
<td>11.5</td>
<td>1541</td>
</tr>
<tr>
<td>Allego</td>
<td>1.47</td>
<td>60</td>
<td>43.5/25.2</td>
<td>1786.1</td>
</tr>
<tr>
<td>Nuon</td>
<td>89.32</td>
<td>3648</td>
<td>11.5</td>
<td>41952</td>
</tr>
</tbody>
</table>

Table 4.1: CPOs operating today in Amsterdam

From Table 4.1, it can be seen that the CPO that has the highest amount of Charging Stations is Nuon with a total of 3648 charging points (city coverage of 89.32 %), adding up a total of 41,952 kW. The second with the highest number of stations is EV-box with a total of 184 (coverage of 4.51 %) and 2,116 accumulated kW. It is important to mention that Allego works with stations that provide fast charging. Therefore, even if they cover only 1.47 % of the city, the total amount of kW installed is relatively high. The others operators do not have a large presence in the city nor have high amount of kW.

As attacking all the CPOs’ systems will require a high level of effort and resources, the best strategy is to focus on the most suitable target. The most suitable target is the one with the highest accumulated kW and the highest distribution of Charging Points along the city. From the results obtained from Table 4.1, Nuon is the one that objectively fulfills these requirements. The latter was expected as Nuon works together with the municipality of Amsterdam to be the major provider of EV public charging points.
2. Identifying key people in the targeted company

One of the main factors that is necessary to understand prior to the execution of any attack, is identify the key people working in the targeted company. These are the people who the attacker may deliver the malware, steal their credentials, or have a deep knowledge regarding the process that the attacker wants to have access to. The means to gather this information range from search engines, social media channels (LinkedIn has been proved to be a useful tool) or social engineering techniques [35].

The importance of identifying the key people in this research work has two purposes. In first place these people have the targeted hosts that the attacker may be interested to deliver the threat. Secondly, their credentials can be vital for accessing the system that controls the charging stations. Therefore, an inspection and analysis of these key people is carried out. Names or other personal information will not be written in this research work, nonetheless the type of information that was possible to gather will be highlighted.

LinkedIn offers a very good platform for acquiring information. From a search in this platform the names, the role, the experience and the location of key people working in the targeted company was found. From a research on social engines, the emails, phone numbers, social media profiles and address of their work place were found. Moreover, from the targeted company's web page, the vacancy/job section provides valuable information regarding the key activities that people working with the EV charging stations perform, information regarding the operation and logistics of the company and also about the presence of third parties that perform certain activities such as the maintenance of the Web server.

Output: Name of the key people working in the EV charging station's department, role and detailed description of their activities and responsibilities, phone numbers of the office place, company's email addresses, company's physical address, social media personal profiles, basic understanding of the logistics and operation of the EV Charging Station Department.
3. Understanding the EV charging station’s control system

Most of the CPO’s systems that control the charging stations are cloud based in order to facilitate the connectivity and to manage the activities of the charging stations. All the commercial CPOs’ software available in the market have in their specification sheet this characteristic. After calling the targeted company, this information has been confirmed and the DNS domain that allows the access via user name and password has been obtained. As it has been discussed in Chapter 2, the communication between the CPO system and the charging stations in the European zone is based on the OCPP protocol and a WAN interface.

The second element that is important to understand is how the software that controls the charging station works. This information was not possible to be obtained directly from the targeted company. Therefore, it has been reconstructed using passive methods. Figure 4.2 shows the overview of the web interface that is used by the targeted company for controlling and administrating the charging stations:

![Figure 4.2: Overview of the interface that manages the EC Charging Stations of the targeted company](image)

In Figure 4.2 the Status, Charge Point ID, the address, description and the details of the different charging stations administrated by the targeted company are displayed. Moreover, a link to the remote maintenance and control actions is given per each one of the charging stations. This gives an initial idea on how the targeted system could look like. As this is just a snapshot of its operation, other sources were consulted to enforce this knowledge.
ANWB, which stands for Algemene Nederlandse Wielrijdersbond (Royal Dutch Touring Club) is a Dutch association that supports infrastructure and assistance activities related to the traffic in The Netherlands. They designed a tutorial which is available online to train operators to use the software that controls the EV Charging Stations [36]. The interface shown in this tutorial is similar to the one used by the targeted company. ANWB’s platform is also cloud based and the level of access/privileges depends as well on the user’s credentials. This tutorial is divided into three user-levels of the platform: The charging station administrator, the charging station manager and the charging station sessions. Figure 4.3 shows the administration interface together with its capabilities.

Figure 4.3: EV Charging Station’s Administrator Interface [36]

Figure 4.3 shows the administrator capabilities in the system. It has access to the Contract ID, the Charging station ID, the roaming activity, the place, the date it was last used and an option to see all the transactions per charging station.

Figure 4.4 shows the interface for managing the Charging Stations. This is the one that allows the operator to control the charging stations. The information displayed is the Charging station ID, the start date of the last charging session, the stop date of this charging session, the number of times that it has been used, the status (available or unavailable), the address, city, connector ID, the load and the temperature. It is important to highlight that from the ID-link the manager is able to manipulate remotely the charging point.

The last element explained in the tutorial are the transactions of the charging points that can be visualized in Figure 4.5. A transaction is equivalent to a charging session. Relevant information can be acquired from this functionality such as the charging station ID, the start and ending date of the transaction, the status of the charging station, the physical address and place of installation, its load and its temperature. This can provide information of the system status while performing the attack.
The objective of this step was to understand how the web interface for remotely controlling the charging stations works, in order to know what to expect when accessing the system. The next section will focus on understanding the characteristics of the victim’s network and hosts from an IT level.

**Output:** The system is cloud-based, overview of the system’s interface, capabilities from the managers and operators, facilities that the software offers, potential attack vectors.
4.2.2. PLANNING: INFORMATION TECHNOLOGY

Reconnaissance in Information Technology (IT) is the research of all the characteristics of the target’s network, hosts and elements that compose its infrastructure. Gathering this information will allow the intruder to access the targeted system. In literature on pentesting examinations and real attacks scenarios, several tools are used to gather this data. The most common tools will be used in this research work. The type of information that can be obtained, range from the type of operational system that the target’s servers or hosts are running, the open ports, the IPs of the servers or hosts, among other characteristics. There is not a universal methodology to perform information gathering from an IT level, but it depends on the strategy and expertise of the attacker. Figure 4.6 gives a snapshot of the steps that will be followed in this work:

To achieve successfully each one of the three steps displayed in Figure 4.6, five different tools will be used. These are the most common ones for gathering information in traditional attack scenarios. The following subsections will be named after the tool and a summary of the information obtained will be given. As the information obtained from each tool may contain sensitive data, the output values have been omitted but the type of data that has been discovered is highlighted.
1. NSLookup

As the size of the World Wide Web increased, special attention had to be placed on the management of IP addresses. In order to avoid duplication and its correct management, the Internet Assigned Numbers Authority (IANA) was created that manages IP addresses worldwide. IP addresses are assigned in a hierarchical fashion where IANA delegates blocks of IP addresses to the Regional Internet Registries (RIR). The RIR allocates them in a regional level and creates sub-blocks that are given to the different Internet Service Providers that provide them to their customers. This hierarchical architecture facilitates the communication between hosts. Furthermore, as remembering an IP from a human perspective is a complicated task, the Domain names systems (DNS) were created to make easier the process of reaching any web service. IANA is also responsible to manage the DNS [10]. NSlookup, that stands for “Name Server Lookup”, is a network administrator command-line tool that is widely used to convert DNS names to IP.

As mentioned in the previous subsection, the DNS of the web service that allows the CPO administrator to log in was obtained. The next step is to retrieve the value of the IP from that web service. The tool NSlookup has been selected and two variations of it, were used. The first one is `nslookup -type=any example.com` to find all the available DNS records of the domain and the second one is `nslookup -query=mx example.com` which provides the access to the Mail Exchange (MX) IP Records. The output of this commands can be visualized in Figure 4.7. The values obtained are the name of all the related servers, their IP addresses and also the one of the Mail Exchange Server.

![NSLookup output](image)

**Figure 4.7: NSLookup results: The IP addresses of important servers**

As mentioned in the previous subsection, the DNS of the web service that allows the CPO administrator to log in was obtained. The next step is to retrieve the value of the IP from that web service. The tool NSlookup has been selected and two variations of it, were used. The first one is `nslookup -type=any example.com` to find all the available DNS records of the domain and the second one is `nslookup -query=mx example.com` which provides the access to the Mail Exchange (MX) IP Records. The output of this commands can be visualized in Figure 4.7. The values obtained are the name of all the related servers, their IP addresses and also the one of the Mail Exchange Server.

**OUTPUT:** Main Server name and IP, Related Servers names and IPs, MX Server name
2. Whois

The IPs can provide valuable information that can be retrieved with the help from other tools. *Whois* is a tool used for querying databases with information of internet registered users. Initially it was used to inform the responsible parties about any issue with their domain. The information obtained from this command ranges from data about the owners of the domain, email addresses, phone numbers and physical addresses. Therefore, *whois* has been used in many hacking attempts to different organizations. The results from applying *Whois* to the IP obtained in the last section are shown on Figure 4.8. The values are omitted due to privacy purposes, nonetheless the fields reveal the information that can be retrieved by an attacker.

![Whois command output example](image)

Figure 4.8: Information obtained by the use of the command *Whois*

Figure 4.8 displays the available information to any entity that uses command *Whois* to the targeted IP. The information obtained is divided in four sections. The first section contains the data of the server including the name of the mother-organization, the country, routing information of the IPv4, the name of the technical administrator, etc. The second section is information regarding the organization such as its complete name, the physical address, the contact in case there was an abuse with the DNS, and the technical contact (of the IT department including the names of the IT people in charge).
The third element is information regarding the person in charge of the Web Service (which, in this case, is not directly working in the targeted company). The information of the contact person includes, the complete name, two physical addresses, the phone number and email addresses. The fourth element is vital as it contains information regarding the host, which goes from the route, the description, the creation date, among other sensitive elements. From this research it has been understood that the company that contains the information from the EV charging points in The Netherlands is the mother-firm of the CPO and also owns other companies in North Europe. Moreover, the geographical position of the server is not located in The Netherlands, but in the headquarters of the mother-firm. Furthermore, the person that is responsible for the web server is a third party, hired from a company that serves this purpose.

WhatsmyIP is another tool that can be found online (www.whatsmyip.org) that also provides valuable information of a server or a host when using an IP as input. The information obtained is similar to the one retrieved from the Whois command. WhatsmyIP provides another way to retrieve this information, without using the shell.

From this point, there are several ways for performing the attack. The first option is that the attacker delivers the threat to the targeted IPs that have been discovered with NSlookup, exploiting a vulnerability in the Server with a tool such a Metasploit Framework. The second option is to deliver the threat via a spoofed email (or a USB in case the attacker can have physical access) to the people that have been targeted in the reconnaissance step and in the Whois command. For either way, the next step is analyzing the open ports and details of the Operational System where the Web service is running (type and version). This information is valuable for discovering vulnerabilities in the system and finding the most adequate weapon. This will be covered in the next subsection.

**OUTPUT:** Physical address of the server, company, contact person’s data, phone number, email, physical address, server information, route of the server
3. Nmap

Nmap, which stands for Network Mapper, is a security scanner that is mainly used for discovering hosts and services with the aim of creating a map of the network. The latter is achieved by sending packages to the targeted hosts and analyzing the response. This tool is used mostly as port scanning (that reveals if a port is open or closed) but other features of Nmap include host discovery, services and Operational System detection. There are three different types of network scanners: Vertical, Horizontal and Mix. The vertical analyses all ports of a determined host. The horizontal a determined port of a series of hosts and the mixed a series of both. Scanners can be easily identified by the defender’s Intrusion Detection Systems as an anomalous activity. To reduce the likelihood to be detected the velocity of scanning can be reduced [10].

For the following research work the Nmap command was used in the targeted IP to know the type of Operational System and version that the system is running. With the information obtained, a Virtual Machine (Virtual Box) was customized with the same specifications as the targeted system. This is done due to privacy purposes. The following steps of Nmap and the rest of the attack scenario were developed in this Virtual Machine. The Nmap command that is used for port scanning and Operational System reconnaissance is `nmap -A -v4 IP`, as `-A`. The element `-A` provides the version of the Operational System and `-v4` manages the latency/velocity of the scanning. Figure 4.9 provides an example on the output information of this command applying it to the Virtual Machine:

```
(root@darkstar ~)$ nmap -v4 --script扫描.nmap.org
Starting nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org
Host is up (0.10s latency).
rDNS record for scanme.nmap.org
Not shown 993 filtered ports
PORT STATE SERVICE
25/tcp closed smtp
53/tcp open domain
79/tcp closed gopher
80/tcp open http
113/tcp closed auth
8009/tcp open ajpi3
31337/tcp closed Elite
device type: general purpose
OS detected: Linux 2.6.0
OS details: Linux 2.6.15 – 2.6.26

Map done: 1 IP address (1 host up) scanned in 16.99 seconds
(root@darkstar ~)$
```

Figure 4.9: Example of the Nmap output command line

From Figure 4.9, the information obtained is the status of the ports (open or closed) and the type and version of the operational system of the web server. Having open ports imply that those services are exposed to a potential attack. A customized attack is done according to the type and version of the Operational System and the ports that are listening (open). The attack will be performed in the next section: Weaponization.

**OUTPUT:** Type and number of open ports, type and version of Operational System
4.2.3. **Planning: Operational Technology**

Operational Technology stands for all the hardware and software that monitors or manipulates the physical processes by controlling the operation of diverse devices. Examples of OT technology include SCADA systems, PLCs, DCS, among others. In most ICS, there is a clear segmentation between IT and OT networks due to security reasons. Nonetheless, with the inclusion of new technologies and to facilitate the ease of controlling the systems, there has been a recent inter-connection between both.

When talking about OT technologies in the EV Charging Infrastructure, there are more elements that are needed to be understood besides the system that controls the charging stations. The composition and characteristics of the Distribution Grid of Amsterdam, for example, is one of the most important elements that are necessary to know prior the execution of the attack.

When launching the attack against the EV Chargers, the main element that the attacker would be looking forward to compromise is the Electrical Distribution Grid. It is unknown, if the topology and elements of the distribution grid are capable of withstanding high loads. Outputs that can be expected are the damage of cables, transformers, feeders (voltage drops) that could even lead to a blackout. More than just disrupting the electricity, damages of the grid's components can be highly costly and disrupting the electricity of certain services (police station, health clinics, etc.) can have serious consequences.

As mentioned in Chapter 3, the second step of Stage II of the ICS Cyber Kill Chain includes the testing phase, where the attacker replicates the attack in a mirrored environment, to assure that it will work when launching it in the real field. In this case the replicated environment is the Distribution Grid of Amsterdam. Therefore, to test the attack, the reconstruction of the Grid will be performed in the next sections with the simulation software Power Factory. To achieve this, it is necessary to know the elements and the characteristics of the distribution grid.

The information needed to reconstruct the Distribution Grid is: The electrical demand per zone, the number and power provided per each EV charging point, their geographical distribution, the topology of the distribution grid, the characteristics of the substations, the geographical position of the substations, the generator plants and their characteristics, the distribution cables (number, capacity, length), the characteristics of the distribution transformers and the topology of the feeders.

In this section, the aforementioned elements will be explained in order to make a reconstruction of the Distribution Grid of Amsterdam and test the attack scenarios. Moreover, the growth of the Electric Vehicle Chargers in the year 2025 (goal of zero emission in transportation) will also be calculated to provide the outcome of an attack in a future scenario.
1. Electrical and EV Chargers’ Demand in Amsterdam

The first element that needs to be understood in order to perform the analysis is the Electrical Demand in Amsterdam. This will be determined in the Control zone which was already identified in the last chapter. The electrical demand of Amsterdam is of vital importance for two main reasons: In first place, understanding the electrical demand behaviour in the city is an initial indicator of which zones are more vulnerable to the attack (however the strength of the components and the topology also plays an important role). In second place, this information will be needed to generate a replicated environment of the city of Amsterdam to use it as a test bench for launching the attacks.

For the analysis of the electrical demand in Amsterdam, the data sets that have been used are the ElectricalDemandPerHour and the FourDigitPostCode. The sources for the generation of this data sets are included in the annexed documents Description - FourDigitPostCode and Description - ElectricalDemandPerHour. The first data set contains information regarding the hourly demand of Amsterdam in a year period. The second one includes information per four digit post code such as the total electrical demand (including commercial, residential and industrial loads) in kWh in a year period, the latitude and longitude of the post code, its surface, the total number of objects that require electricity, the number of neighborhoods, the number of inhabitants, the average income per person, the quantity of households, businesses and autos (with gasoline and with an alternative fuel). As modelling the load of each household, commerce or industry in Amsterdam will require high computational resources, the electrical loads have been aggregated by Four-digit post code. For the next analysis, only the average electricity demand per post code information from the FourDigitPostCode data set has been used together with the ElectricalDemandPerHour data set. Using the Four Digit Post Code has several advantages: Firstly it will reduce the computational power needed to simulate the environment, secondly this allows to have a better visibility of the loading behaviour per zone and in third place this helps to recreate a structure of the city.

The electrical demand in the data set FourDigitPostCode is converted to total kW per hour. As the loading behaviour is already known from the ElectricalDemandPerHour Dataset, this is adapted correspondingly to the electrical demand per hour of the FourDigitPostCode. This provides as a result the behaviour of the loads per hour in a year period per Four Digit Post Code. For the following analysis the months that correspond to the summer period were taken into account as mentioned in Chapter 2. The average demand in summer period at 21:00 hours for each Four Digit Post Code was calculated using the software Tableau. Figure 4.10 shows the electrical demand of Amsterdam in kWh at the peak hour (21:00 hour) per each four-digit Post Code inside the defined Control zone:

The electrical demand behaviour in Figure 4.10 covers the residential, commercial and industrial activities. The highest electrical demand is in the Post Code 1012 which covers most of the central part of the city. This is considered as the most vulnerable one, as it also has the highest density of EV charging stations as commented in Chapter 2.
Moreover it is also important to determine the potential electrical demand due to the number of EV charging stations installed per Post Code. This indicates the likelihood of the zone to be affected by the Cyber attack.

The complete demand should consider on one side the electricity loads due to residential, commercial and industrial activities and on the other side, the demand due to the number of EV charging stations installed. Therefore, Figure 4.11 displays 10 post codes with the highest demand considering both aforementioned elements:

Figure 4.11: Top 10 Electrical Demand per Post Code. The red bars represent the total electricity demand, the green bars commercial, residential and industrial activities together and the blue bars the amount of consumption of the EV Charging Stations
The red bars in Figure 4.11 correspond to the value of the total electricity demand in MWh per hour per post code. The green bars represent the electrical demand due to the residential, commercial and industrial activities and finally the blue bar represents the electrical demand per the amount of EV Charging Stations installed. This analysis has been performed for all the Post Codes inside the established control zone, nonetheless just 10 of them are displayed due to visualization purposes. The complete analysis can be seen in the FourDigitPostCode Data Set Annexed to this thesis work.

In order to visualize the distribution of the loads in a geographical fashion, two heat maps have been created with the software Tableau, which represent the electricity demand per activity (residential, commercial and industrial) and the second one representing the electrical demand due to the amount of EV charging stations installed. These two maps can be visualized in Figure 4.12.
Figure 4.12 provides a graphical representation of the distribution of the electrical demand and the EV charging station loading. As it was expected, the highest electrical demand is located at the center and the highest amount of charging station is in the residential areas. As mentioned before, this information will be necessary to replicate the behaviour of the Distribution grid of Amsterdam when testing the attacks. These maps, identify graphically the most vulnerable zones due to a high electrical demand and also due to a high density of EV charging stations.

Besides the electrical demand, other elements that constitute the Distribution Grid should be also analyzed in order to be able to set the mirrored environment. The next subsection will focus on covering the characteristics of the elements that compose the distribution grid and on establishing a future scenario (2025) with an expected increase in the number of charging stations.
2. Characteristics of the Amsterdam's Distribution Grid

The mission of the Distribution Grid can be segregated into four different goals: The first one is to cover the service territory in order to reach all the customers, the second one is make sure to have enough capacity to meet the peak demands, the third to provide a reliable delivery to the customers and finally the last one is to provide a stable voltage quality to their customers [25]. The design and pacification of a distribution grid implies the knowledge of several factors in order to make sure that it will deliver the necessary electricity when needed in a safe way. A good design involves a satisfactory performance with the lowest possible cost. Therefore, the characteristics of the elements that compose the grid should be designed in a way that they can stand the expected day-to-day loading. At the same time the design should be optimal from an economical standpoint. The topology of the grid also plays a fundamental role when defining the strength of the grid.

The last section was focused on understanding the demand behaviour in the city of Amsterdam. In this section the characteristics of the elements that compose the grid (substations, generators, cables, buses, transformers) will be analyzed as well as the topology of the grid. The topology will cover the connections between substations, connections to an external grid, the geographical position of the substations, the paths of the cables, the amount of cables and the geographical position of the generators and their connections with determined substations. Is important to mention that when the capacity of any of the aforementioned elements is not enough to cope with the loads, this may lead to a disturbance of the electrical supply. These elements will also be used for the replication of the environment that will be done with the Simulation Software Power Factory in the next Chapter.

In order to reverse engineer the distribution grid of Amsterdam, data from different sources such as Liander [24], The municipality of Amsterdam [4], the Central Bureau of Statistics of The Netherlands (in the annexed data sets) and open maps such as Hoogspanning net [17], open power map [18] and PICO map [15] were used to achieve the latter. With the information acquired from this different sources three data sets were created FourPostCodeDataSet, SixPostCodeDataSet and HourlyElectricityDemand that contain the characteristics that are the input for the testing mirrored environment in this research work.

The layout of this section starts with a summary of the elements that compose the Amsterdam's distribution grid, followed by the characteristics of the substations and finalizes with the attributes of the distribution lines.
2.1 Summary of the Distribution Network Elements

The elements that have been taken into account in this thesis work for the replication of the distribution grid of Amsterdam are: The substations, the terminals, bus bars, generators and distribution lines. All the values of the capacity of the elements and their geographical position correspond to the real values. A summary of the number of elements and their characteristics can be seen in Figure 4.13:

Figure 4.13: Summary of the characteristics of the Electrical Distribution Grid of Amsterdam

Figure 4.13 shows that the distribution grid of Amsterdam is composed by 19 substations that reduce the voltage levels at different stages going from the maximum (at transmission level) of 280 [kV] to 0.4 [kV]. The model consists of a total of 48 bus bars distributed across 19 substations. Amsterdam counts on 4 generators which are divided in two stations: Hemweg and Diemen. Hemweg generates power at 150 [kV] level while Diemen at 380 [kV]. There are 27 lines that carry voltages at 50 [kV] and 150 [kV] level. The lines at 50 [kV] have a capacity of 44 MVA while the lines at 150 [kV] have a capacity that ranges from 132 up to 250 MVA. The detailed characteristics of the aforementioned elements will be covered in the next sections.
2.2 Substations' Characteristics

The city of Amsterdam has a total of 19 substations distributed across the city. These substations reduce voltage levels at five stages: From 380 kV to 150 kV, from 150 kV to 60 kV, from 50 kV to 20 kV, from 150 kV to 10 kV and 50kV to 10kV. Two of these substations are connected to the two major generators in Amsterdam: Diemen and Hemweg. Figure 4.14 shows the voltage levels of the 19 substations:

![Figure 4.14: Characteristics of the Substations by Voltage Levels](image)

Figure 4.15 shows the 19 substations with their voltage levels. The red bars represent the highest voltage while the blue bars the lowest. Other important characteristic are the connections among them which also identify the substations that are connected to an external grid. The latter will influence the results of the Power Flow calculations. These can be appreciated in Figure 4.15:

![Figure 4.15: Characteristics of the Substations by number and type of connection](image)
Figure 4.15 displays the number of connections per substation, and if the substation is connected to an external grid (which means that the substation that is connected to, is not inside the Amsterdam Region or Control Zone defined in Chapter 1). The blue squares represent connections between substations while the red squares imply that the substation is connected to a generator, which is the case for Hemweg and Diemen.

2.3 Line Characteristics

The distribution lines’ characteristics were also taken into account for this research work. The elements that were analyzed were the capacity of the lines, the number of lines and their longitude. The distribution lines are considered as a very important element for the mirrored environment as overloading a line can cause physical damage of the element that could lead to a potential black out. Figure 4.16 shows the characteristics of the distribution lines in Amsterdam:

![Figure 4.16: Characteristics of the distribution Lines in the electrical grid of Amsterdam](image)

Figure 4.16 shows the elements of the distribution lines that will be taken into account for the replication of the Amsterdam's grid. The information that is display per line is the name of the stations that are being connected to, the length of the line in km, the number of parallel lines, the capacity of the lines and who is the responsible administrator. For the lines that transport voltages up to 50 kV the administrator is Liander, while for voltages higher than this the administrator is the Transmission System Operator of The Netherlands: Tennet.
2.4 Recreation of the Amsterdam’s Distribution Grid

All the aforementioned elements were used for the recreation of the Amsterdam’s Distribution Grid. As it will be further explained in Chapter 5, the grid has been reversed engineered and simulated with the Software Power Factory. In this section the steps that have been used for the replication of the grid will be further explained:

The first element was the analysis of the geographical location of the substations that are relevant in the selected control zone of the Amsterdam Region (Reviewed in Chapter 2). These information has been obtained from [17] and [18]. The relevant substations have been selected, which are the mentioned in Figure 4.14 and Figure 4.15. Some substations are connected to others that are not considered inside the selected control zone, therefore an external grid has been connected to these substations. The geographical position of the substations is as close as possible to the real location. The simulation of each one of the 19 substations in Power Factory can be visualized in the Annex I. Besides the geographical location of the substations and their connections with an external grid, other element that has also been taken into account is their voltage characteristics. These information has been obtained from [17] and from [20]. Figure 4.14 show the voltage levels of the different substations. Is important to mention that some substations have in their high level voltage section 380 kV. The reason is that two of these substations are connected to two generators: Hemweg and Diemen. These two have been also simulated in Power Factory and contain a governor (or a speed limiter controller) that regulates the speed of a generator and consequently controls the frequency of the grid.

The second element is the connection of the lines between each one of the substations. The geographical paths that the lines follow are as close as possible to the real ones. This information has been retrieved from [17]. Moreover, the characteristics of the lines such as the length (in km), the number of lines and its capacity has been obtained from [17], [18] and [21]. These parameters have been added to the model in Power Factory.

For the simulation of the loads, as mentioned before, these have been aggregated by Four Digit Post Code in order to reduce computational power. These aggregated loads have been connected to the closest substation according to the paths that the distribution lines of 0.4 kV follow according to [16]. As mentioned before the these contains information from residential, commercial and industrial loading at 21:00 of a summer period.

The information regarding the number, location, type and owner of the charging stations has been obtained from [16], [21] and [23]. The number of charging stations has been clustered per four digit post code. From these clustering, the type of each one these charging stations has been identified (7.4 kW, 11.2 kW, 22 kW and 43 kW) and the maximal potential load has been calculated which corresponds to the power of each substation multiplied by the number of substations of that type in each cluster. Therefore, similar to the electrical loads, these have been connected according to the closest substation. Is important to mention that the EV Charging Stations that have been selected are the ones operated by Noun. Nonetheless, the information of the EV Charging Sta-
tions of all Charging Point Operators is available.

The reconstruction of the grid in Power Factory will be further explained in the Section 2 of Chapter 5: *Testing*, where the simulation in Power Factory will be further explained.
3. Growth of EV Charging stations by 2025

As mentioned previously, by the year 2025 Amsterdam has the goal of zero emissions in the transportation sector in order to achieve a sustainable scenario. In order to achieve these ambitious targets, the amount of EV Charging stations is expected to increase in the following years. In this section, the amount of charging stations that will be needed to achieve the zero-emissions goal by the year 2025 will be estimated, taking into account the increase of electric vehicles expected by that year.

To understand the growing trend in The Netherlands in the transportation sector, the following table has been retrieved from the Central Bureau of Statistics in The Netherlands that displays the growth in the vehicular sector:

<table>
<thead>
<tr>
<th>Year</th>
<th>Cars Netherlands</th>
<th>Cars Amsterdam</th>
<th>Electric Cars Amsterdam</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>7,230,000</td>
<td>213,285</td>
<td>No Info</td>
</tr>
<tr>
<td>2010</td>
<td>7,622,000</td>
<td>224,849</td>
<td>No Info</td>
</tr>
<tr>
<td>2013</td>
<td>7,916,000</td>
<td>233,522</td>
<td>No Info</td>
</tr>
<tr>
<td>2014</td>
<td>7,932,000</td>
<td>233,994</td>
<td>No Info</td>
</tr>
<tr>
<td>2015</td>
<td>7,979,000</td>
<td>235,380</td>
<td>45,975</td>
</tr>
<tr>
<td>2016</td>
<td>8,101,000</td>
<td>238,979</td>
<td>48,700</td>
</tr>
</tbody>
</table>

Table 4.2: Mobility growth in The Netherlands and Amsterdam in conventional and electric vehicles

From this trend, it can be seen that approximately 2.95% of the vehicles in The Netherlands belongs to the Amsterdam Region. Moreover, the number of vehicles in Amsterdam shows an increasing behaviour. From the total number of cars in Amsterdam around 20% are Electric Cars. Therefore, the number of electric cars has also increased from 2015 and 2016. By the year 2016 a total of 28,700 electric cars were registered which needed around 2000 charging stations. In the year 2018 the number of charging stations have increased by 49% up to 4048 EV charging points.

As in the year 2025, Amsterdam’s target is to become zero-emission in the transportation sector an assessment is needed to understand the number of EV Charging stations that will be required. As the historical trend in the automobile sector in Amsterdam and in the Netherlands has shown an increasing behaviour of approximately 2.95% annually, it can be assumed that this trend (without taking into account external factors such as policies or a decay in the EV market) will have this increasing behaviour of approximately 2.95% annually. If the goal of zero-emissions in the transportation sector is covered, this means that 100% of the cars should be electric. If by the year 2016 the number of charging stations was 2000 and by the year 2018 it duplicated the number by 4048 stations, it means that for the year 2025 the number of EV cars would be approximately 273,950 and approximately 11,252 of charging stations would be needed.

According to this projections, we assume an EV demand of 123.772 [MW] in the year
2025. For the testing scenario, where we project the increase on the EV Charging Stations (Chapter 5), the demand is evenly distributed across all considered Zip Codes.
4.3. **Preparation: Weaponization**

Weaponization is the second step in the first stage: Cyber Intrusion, Preparation and Execution. In this section the information that was previously gathered during the Reconnaissance is used to find an adequate weapon that could bypass the security of the target. The most suitable weapon depends on different factors such as the operational system, its version, the open ports and these define the vulnerabilities of the system [34].

A vulnerability can be defined as a hole in the security. These can be bugs in a piece of code or errors in the design or implementation of the system. Every day new vulnerabilities are being discovered in web applications, services and operational systems. To rectify these security holes, the developers need to create a patch for each vulnerability discovered and distribute it to their customers via updates. There are two types of vulnerabilities: The already recognized ones and the, so called, Zero-Day vulnerabilities. The first ones are vulnerabilities already discovered and publicly available from different websites and defence tools like anti-virus have knowledge of them. For the Zero-Day there is not public knowledge about their existence and can bypass several detection methods. These can be found in the black market and be purchased at high prices [7].

In order to exploit these vulnerabilities, there are different tools that can facilitate this work. The most common tool is Metasploit Framework. Metasploit Framework is an open source, offensive tool initially created for pen-testing activities. Five steps are mainly needed to exploit a vulnerability. The first step is that according to the type of operational system of the targeted server/host, the attacker should select and configure the most suitable exploit. These are given by the tool and more than 900 exploits are available for all operational systems. The second step is analyzing if the host/server target is susceptible to the selected exploit. In the third step, the attacker chooses the payload, which means the code that will be executed once the delivery of the threat is successful. The payload can be either a remote shell, back doors, key loggers or any other gadget that can be used in further stages. The fourth step is selecting a proper encoding technique in order to trick the security systems (such as intrusion detection systems) about the nature of the payload. Finally, in the last step the exploit is sent and executed [37]. This steps are visualized in Figure 4.17.

![Figure 4.17: The five steps for using Metasploit Framework](image)
1. Armitage

In this research work, the exploitation step has been performed in the pre-configured Virtual Machine to avoid the violation of any policy. The weaponization stage has been developed using the GUI version of Metasploit Framework: Armitage. Similar to Nmap, Armitage has also the possibility to scan the targeted IP or ranges of IPs. It provides a list of the open ports and the different hosts that are available in the network [38].

![Figure 4.18: Scanning hosts and networks with Armitage](image1)

![Figure 4.19: Output of the scanning with Armitage](image2)

Figure 4.18 shows the window that allows the user to input the IPs or range of IPs that Armitage will use to start the scanning. The output of the scanning will show the different hosts available in the network, open ports and type of Operational System just as displayed in Figure 4.19. For the next step Armitage can be configured to scan the available attacks for each hosts according to their characteristics:
Figure 4.20 and Figure 4.21 show how the list of available attacks is generated for each one of the hosts. Figure 4.20 shows the option to find attacks per each one of the hosts. Once this analysis is completed, the pop-up in Figure 4.21 appears which mentions that now all the different attacks per host are already available. Many different type of attacks are possible that range form ftp, http, misc, etc. The next step is the selection and delivery of the attack.
Figure 4.22 displays all the available attacks per each one of the hosts. The attacker selects the most suitable one according to his/hers expertise. Armitage offers an attack option called *Hail Mary* where the attacker can launch all the available exploits to the victim. This option is not suggested as it is very noisy and it will be likely to raise an alarm in the target’s security system.

Before launching the attack, Armitage also offers the option for selecting the payload. As previously mentioned the payload can be either a shell for controlling remotely the system, key loggers, back doors or any other element that could help to perform the attack. Encoding Techniques also play a fundamental role as they reduce the probability of the payload to be detected by any security system.

The exploit can be delivered via Armitage, moreover other delivery techniques have been recorded in other attack scenarios. The latter range from email, USB or other removable drives, etc. The delivery techniques, the exploitation state and the installation of the required tools for performing the attack will be explained in the next section.
4.4. CYBER INTRUSION: DELIVERY, EXPLOIT, INSTALL

After having the adequate weapons for attacking the system, the next step is delivering the threat to the victim, exploiting the vulnerability and installing the necessary payload to launch the attack. This section will explain each one of these aspects. It is important to mention that these steps were not executed for privacy purposes, however an explanation how will the attack could potentially be developed will be given.

4.4.1. DELIVERY

Delivery is the procedure where the attacker tries to find the most suitable channel to "deliver" the threat to the victim. There are different potential channels that could lead to a favourable outcome. Delivery is considered inside the attempt phase, as deliver the payload does not necessarily mean that the victim will accept it. Two common delivery methods that would be plausible to occur in this attack scenario will be briefly discussed:

1. Phishing Attacks

Phishing attacks are forged attempts to obtain valuable information by pretending to be a trustworthy entity. Phishing can be carried out by fake web sites, email spoofing, instant messages, social media profiles, among others. In the case of attacks to ICS, email spoofing has been reported to be one successful delivery tool. By sending the target an email from a trustworthy authority, the attacker can hide the payload in attacked files. In order to make this attack successful, social engineering is also used as a parallel tool that will help to convince the target about the legitimacy of the sender. An available tool to send spoof emails is the Social Engineering Toolkit (SET) which is an open source framework which contains different tools to perform phishing attacks. For this attack scenario, spoofing emails can be delivered to the key people previously identified in the reconnaissance stage. This messages can contain information regarding aspects relevant to their activities. The success of the attack relays on how credible the email can be. Therefore, acquiring as much information as possible from the victim activities is a crucial step.

2. External Drives

External Drives, such as USB or external memories are also a known channel to deliver threats. It has been suspected that Sutxnet malware used this delivery channel for its propagation. In order have a successful delivery, physical access to the facility and to the targeted host is needed. This delivery channel has a higher complexity in the sense that requires the presence of an insider in the company to make it possible. For this attack scenario, having physical access to the facilities or an insider would be needed in order to make this delivery channel successful. An insider can range from a unhappy employee to a contractor that looks forward to obtain any gain.

If the delivery stage is successful, the attack advances to the next step: The exploitation of the vulnerability and the installation of the payload. This is covered in the next section.
4.4.2. EXPLOITATION AND INSTALLATION

If the delivery of the payload is successful, the following two steps involve the exploitation of the vulnerability and the installation of the selected payload. As mentioned before, the payload are the tools selected by the adversary that will be used to develop the attack. In the following section both elements will be explained together with their application in the suggested attack scenario.

An exploit is a piece of software that is designed to take advantage of a bug or a vulnerability in a determined system. The selection of the exploit has been already covered in the last section, weaponization. In this stage, the exploitation of the vulnerability is successful and the attacker can already installed the payload.

For the scenario where the attacker compromises the web server the payload can be a command shell to control the system remotely, a key logger to register the information typed on the target system and a backdoor to assure having continuous access to the system. The location where the payload can be installed and the name given to the files play a very important role in assuring that they won't be detected by the victim. For the scenario where the attacker compromises the computer of the CPO's operator, the payload installed can be a control shell, key loggers to register the information that has been an input by the victim (such as credentials) and also a back-door to keep having access to the system.

Once the payload has been successfully installed in the targeted system, the next step is the remotely command and control to execute the necessary actions or gather relevant information to launch attack the Industrial Control System.
Management and Enablement is the last step of the Stage I of the Cyber Kill Chain. In this step, the attacker has already compromised the system and installed the necessary tools to launch the attack.

In this attack scenario, the goal is to obtain the relevant credentials of the administrator of the EV charging stations control system. From the reconnaissance step, the key people in the targeted company has been already identified. The characteristics of the web server that controls the logging of the EV charging station control system has been also analyzed together with the vulnerabilities of the system. The vulnerabilities have been exploited and the payload installed. Therefore the next action is to find the director that has access to the user names and passwords.

The user names and passwords are not stored in plain text. Usually the hashes are the ones stored. They are either in the Windows SAM file located at C:/Windows/ System32/ config or at the registry ay HKEY-LOCAL-MACHINE/ SAM. As the attacker will be accessing the computer from the remote console, what can be used to obtain the hashes is the Fizzgig's fgdump utility. When running it, it will create a dump of the local machine SAM file. This contains a list of accounts, LM hashes and NTLMv2 hashes. As hashes are not understandable from a human standpoint, the next step will be using the tool Cain and Abel to generate the plain text passwords from the hashes. Once the hashes are provided as input for Cain and Abel, the brute force attack is selected which provides all the possible combinations of against the hash value until if finds a match. The time it will take to provide the plain text value depends on the complexity of the password.

The output of this step is the acquisition of the user name and passwords that will allow to access the EV Charging Station Control System. This is the final step of Stage I. The next step of the kill chain will be Stage II which is mainly focused on the attack at the Industrial Control System Level.
"There was a stunning cyberattack on a critical Middle Eastern infrastructure site recently and it hasn’t gotten the public scrutiny it deserves. Triton (A.K.A. Trisis), a new strain of malware, was discovered last month via intelligence sharing reports provided by the security vendors FireEye and Dragos. The news was the latest in a series of public disclosures about progressively more sophisticated energy plant hacks. The specter of attacks on the power grid and other systems is no longer a matter of speculation. Hackers are testing the protections for critical infrastructure, and energy plant operators need to take the threat seriously, as do the decision makers in the industrial sector at large."

Adam Levin
5.1. **INTRODUCTION**

In this section the three steps of Stage II will be developed. As mentioned in Chapter 3, in Stage II it is already assumed that the hacker has already access to the system and here the focus is solely on launching the attack to the Industrial Control Systems.

In the first step, the attacker should already have the necessary knowledge regarding the system and should be able to understand which is the most suitable attack, the outcome that is expected and the likelihood of success. In this research work five different attack scenarios will be developed for present and future cases. These scenarios involved the manipulation of the EV Charging Stations by activating them, which results in an increase in the electrical load at peak hour. The outcome expected is physical damage in the components of the grid, voltage drop and potentially an electrical disruption. These five attack scenarios will be explained with more detail in the next subsection.

The second step is testing the attack. In order to do so, a mirrored environment of the distribution grid of Amsterdam has been created using the simulation software Power Factory. The characteristic of the grid contains the elements that have been discussed in the last chapter in the *Planning: Reconnaissance* section. As mentioned in Chapter 3, planning is one of the most important steps as this can prove or reject the initial hypothesis of the attacker. Therefore, several iterations of the attack can be made until the achievement of the expected outcome.

The third and final steps is launching the ICS attack. The threat is delivered, exploited and the attacker has control over the Industrial Control System. In this section, the results of launching the attack in the grid components will be further explained and this will be the final step of the Kill Chain.
5.2. **Attack Development & Tuning: Develop**

In this step: *Attack Development and Tuning* the focus of the adversary is designing the most suitable attacks for this specific IDS. In this step it is already assumed that the attacker has already access to the Electric Vehicle Charging Infrastructure as it has been described in Step I and has the necessary knowledge to identify which are the attack vectors and the potential outcomes.

As previously mentioned, the objective of the following attack scenario is to gain access to the Electric Vehicle Charging Station Control System in order to manipulate the Electric Vehicle Charging Stations. From an attacker perspective activating all the charging stations at a peak hour can lead to damages of the electrical grid of Amsterdam. As there is not enough technical expertise to understand if the electrical grid is capable of withstand this increase in the load, it is of high interest to understand how is going to be the outcome. Expected outcomes can be the damage of distribution cables, distribution buses, transformers and provoke an instability in the voltage at feeder level.

Once the objective has been settled, the next element is to define the scenarios that will be replicated in the mirrored test bench:

<table>
<thead>
<tr>
<th>Scenario's Number</th>
<th>Present/Future</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><em>Present</em></td>
<td>Testing in the most vulnerable zones (Hospitals, Police Stations, etc.)</td>
</tr>
<tr>
<td>2</td>
<td><em>Present</em></td>
<td>Testing from 0% to 100% of EV Chargers Manipulation</td>
</tr>
<tr>
<td>3</td>
<td><em>Future</em></td>
<td>Testing from 110% to 200% of EV Chargers Manipulation</td>
</tr>
<tr>
<td>4</td>
<td><em>Future</em></td>
<td>Testing for 2025 EV Chargers’ Panorama</td>
</tr>
<tr>
<td>5</td>
<td><em>Present</em></td>
<td>Feeder Behaviour in the most vulnerable zone</td>
</tr>
</tbody>
</table>

Table 5.1: Scenarios that will be tested in the replicated environment

The first scenario is focused on testing the outcome is the most vulnerable zones which have a higher density of EV charging stations and higher electrical load. Vulnerable zones can also contain important services such as police stations, hospitals, train stations, etc. For the three following scenarios the elements that will be analyzed are the overloading of the cables and the voltage drop in the buses. It is expected that a voltage drop of +/- 10% can lead to a blackout. Therefore, the capacity of the cables should not exceed the designed value as this will imply the physical damage of the components. The fifth and last scenario will be focused on understanding the consequences at feeder level. In this case, the feeder should also avoid having a voltage drop of +/- 10% as this can be also traduced a in a potential blackout.

In the next section, the replication of the mirrored environment will be further develop and in the last section the results of executing the six steps will be shown.
5.3. Testing Attack

When launching an attack to an Industrial Control System, it should be first tested in a mirrored environment. The mirrored environment should have the same characteristics than real scenario in order to assess the likelihood of success or to understand if any change is needed in the attack scenario. For this research work, the replicated environment is the Distribution Grid of Amsterdam, which has been reversed engineered using information from different sources.

For this research work, the testing bench has been created using the software Power Factory 2015. Power factory is a software that is used in Power Engineering for simulating generation, transmission, distribution and industrial systems. The mirrored environment has exactly the same characteristics than the real distribution grid of Amsterdam (even the exact geographical location of all the components). The elements that are included in the tested environment are:

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generators</td>
<td>Four Generators (Hemweg, Diemen)</td>
</tr>
<tr>
<td>Sub-Stations</td>
<td>19 substations in Amsterdam Region</td>
</tr>
<tr>
<td>Distribution Lines</td>
<td>Lines (real values: Capacity, length, material, num. lines)</td>
</tr>
<tr>
<td>Transformers</td>
<td>VA values according to Distribution Grid Handbook</td>
</tr>
<tr>
<td>Feeders</td>
<td>Local level. Center of Amsterdam</td>
</tr>
<tr>
<td>Loads (Commercial, Residential, Industrial)</td>
<td>Aggregated Load per 4 digit Post Code</td>
</tr>
<tr>
<td>EV Charging Stations</td>
<td>Aggregated Load due to capacity and num. of stations per 4 digit Post Code</td>
</tr>
</tbody>
</table>

Table 5.2: Characteristics of the reversed engineer distribution grid of Amsterdam

The information from the testing environment has been retrieved from open source maps and data sets. For this thesis work three data sets were elaborated that contain the characteristics of the distribution grid of Amsterdam. These are included additionally to this research work. The first data set `FourPostCodeDataSet` contains all the information of the distribution grid when segmenting the Amsterdam region per four digit post code. The data set `SixPostCodeDataSet` includes the same information but by segmenting the city in six digit post code which results in a more defined area. The last data set `Hourly-ElectricityDemand` contains the information of the electricity demand per hour in a year period. Moreover, three open source maps [13, 14, 15] have been consulted to design the topology of the system. For the load modelling, these have been aggregated by four digit post code to make easier the segmentation of the city and to reduce the computational power of the simulation. If one would like to have a higher granularity the analysis of the loads per Six Digit Post Code would have been also possible, nonetheless as mentioned previously this required a higher computational effort.
The results of replicating the grid in Power Factory can be visualized on Figure 5.1. The 19 different substations are in the same geographical position than the real ones and each one of them contain different voltage transformation ratios. The specifications of the simulations of each one of the substations can be visualized in Annex 1. The distribution lines that connect the substations have the same number of cables, capacity and follow almost the same path than the real distribution grid of Amsterdam.

The labels in the substations of Figure 5.1 have three different colors. The yellow labels indicate that the substation reduces the voltage from 50 [kV] to 10 [kV]. Blue from 150 [kV] to 10 [kV] and the pink labels indicate the substations directly connected to the generators. Diemen has a maximum voltage level of 380 [kV] while Hemweg of 150 [kV].

The transformers for each substation have been configured according to the Distribution Grid Handbook. It is important to mention that there is not a standard design. They vary in specifications, types, styles. This is because the manufacturers build the transformers according to their utility. Nonetheless, there are certain transformers that do have a higher usage in distribution grid such as the 138 kV to 12.47 kV. The most important characteristic of the transformers is the capacity (given in kVA or MVA). This is also called the size of the transformer. Determining the transformer’s capacity is a result of very specific conditions and there is not an standard for it. The unit considered in this research work can handle 37 MVA for two hours, not exceeding the ambient temperature of 65 Degrees Celsius if it has not been loaded above 20 MVA for the previous two hours.
5.4. **ICS Attack Scenario**
In the ICS Attack step, the attacker has already successfully tested the attack, delivered the threat and has already launched it. Therefore, in section we will focus on analyzing the outcome of the attack. This analysis will include the behaviour of the grid components post-attack such as lines, buses and feeders and an examination of the most vulnerable zone of Amsterdam.

5.4.1. **Most Vulnerable Zones**
A first analysis will be on analyzing those stressing points which are considered more vulnerable in the city of Amsterdam. These vulnerable zones are areas with a high concentration of EV Charging Stations that also have higher average loads. The grid components in these zones are expected to be the most damaged when performing this attack scenario. These zones can be visualized in Figure 5.2:

![Figure 5.2: Vulnerable Zones in the EV Charging Station Attack Scenario](image)

As it can be seen from Figure 5.2, the most vulnerable zones form an attacker perspective are mainly four: 1012, 1017, 1071 and 1077. These four zones have a higher average electrical demand per year in comparison with the other areas and at the same time have a considerable high electric vehicle charging density. The latter is due to the number of residential and commercial activities in these areas. Other characteristics that can also make an area more vulnerable is the number of sensitive assets that it contains. A sensitive asset can be considered hospitals, train stations or any other service that people depend upon it. Figure 5.3 and Figure 5.4 shows the density of hospitals and trains stations respectively:
Figure 5.3: Number of hospitals/health clinics per zip code

Figure 5.4: Number of Train Stations per Zip Code
Therefore, from Figure 5.3 the top 5 most vulnerable zip codes are 1013 (with 203 EV Charging Stations equivalent to 2334.5 [kW]), 1067 (with 102 EV Charging Stations equivalent to 1207.5 [kW]), 1053 (with 252 EV Charging Stations equivalent to 2898 [kW]), 1054 (with 255 EV Charging Stations equivalent to 2932.5 [kW]) and 1025 (with 241 EV Charging Stations equivalent to 2771.5 [kW]), while from Figure 5.4 the top 5 most vulnerable zip codes are 1025 (with 241 EV Charging Stations equivalent to 2771.5 [kW]), 1013 (with 203 EV Charging Stations equivalent to 2334.5 [kW]), 1067 (with 372 EV Charging Stations equivalent to 4278 [kW]), 1053 (with 252 EV Charging Stations equivalent to 2898 [kW]) and 1054 (with 254 EV Charging Stations equivalent to 2926.08 [kW]).

The feeder analysis will be generated for the most vulnerable zones that are displayed on Figure 5.2. It is expected that these zones will have a higher voltage drop in the feeder in comparison with the other areas.
5.4. ICS Attack Scenario

5.4.2. Present Scenario: From 0% to 100% of EV Manipulation

The first scenario that will be analyzed is the present situation, when the attacker has control over the EV Charging Stations in Amsterdam. This scenario will test what are the consequences from a grid perspective if the attacker has 10%, 50%, 80% and 100% of EV charging manipulation. Is important to understand what will be the behaviour of the components in the grid for each one of the aforementioned cases. The Table 5.3 shows the values that are used as input in the simulation:

<table>
<thead>
<tr>
<th>Power Station</th>
<th>Number EV Stations</th>
<th>10% EV Demand [MWh]</th>
<th>50% EV Demand [MWh]</th>
<th>80% EV Demand [MWh]</th>
<th>100% EV Demand [MWh]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basisweg</td>
<td>104</td>
<td>0.1276</td>
<td>1.0211</td>
<td>1.2764</td>
<td></td>
</tr>
<tr>
<td>Frederiksplein</td>
<td>280</td>
<td>0.3316</td>
<td>2.6528</td>
<td>3.3160</td>
<td></td>
</tr>
<tr>
<td>Hemweg</td>
<td>102</td>
<td>0.1246</td>
<td>0.9964</td>
<td>1.2455</td>
<td></td>
</tr>
<tr>
<td>Hoogte Kadijk</td>
<td>365</td>
<td>0.4240</td>
<td>3.3919</td>
<td>4.2399</td>
<td></td>
</tr>
<tr>
<td>Karpenweg</td>
<td>448</td>
<td>0.5125</td>
<td>4.1003</td>
<td>5.1254</td>
<td></td>
</tr>
<tr>
<td>Marnixstraat</td>
<td>252</td>
<td>0.2914</td>
<td>2.3314</td>
<td>2.9142</td>
<td></td>
</tr>
<tr>
<td>Papaverstraat</td>
<td>241</td>
<td>0.2791</td>
<td>2.2329</td>
<td>2.7911</td>
<td></td>
</tr>
<tr>
<td>Rijnspoor</td>
<td>317</td>
<td>0.3717</td>
<td>2.9734</td>
<td>3.7168</td>
<td></td>
</tr>
<tr>
<td>Schipluidenlaan</td>
<td>372</td>
<td>0.4286</td>
<td>3.4287</td>
<td>4.2859</td>
<td></td>
</tr>
<tr>
<td>Slotermeer</td>
<td>233</td>
<td>0.2874</td>
<td>2.2990</td>
<td>2.8737</td>
<td></td>
</tr>
<tr>
<td>Uilenburg</td>
<td>122</td>
<td>0.1544</td>
<td>1.2343</td>
<td>1.5436</td>
<td></td>
</tr>
<tr>
<td>Venserweg</td>
<td>325</td>
<td>0.4173</td>
<td>3.3385</td>
<td>4.1731</td>
<td></td>
</tr>
<tr>
<td>Vliegenbos</td>
<td>108</td>
<td>0.1226</td>
<td>0.9811</td>
<td>1.2264</td>
<td></td>
</tr>
<tr>
<td>Watergraafsmeer</td>
<td>103</td>
<td>0.1172</td>
<td>0.9378</td>
<td>1.1723</td>
<td></td>
</tr>
<tr>
<td>Westzaanstraat</td>
<td>203</td>
<td>0.2335</td>
<td>1.8676</td>
<td>2.3345</td>
<td></td>
</tr>
<tr>
<td>Zorgvlied</td>
<td>509</td>
<td>0.7351</td>
<td>5.8807</td>
<td>7.3509</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>4084</td>
<td>4.9586</td>
<td>39.6686</td>
<td>49.59</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.3: Input variable values for the simulation in the first case

As it can be seen from Table 5.3 the input variable values that are used for the first simulation include the demand generated by the charging stations when they are being manipulated by 10%, 50%, 80% and 100%. The electrical load values are the ones that have been analyzed on Chapter 4 and they are aggregated by Four Digit Post code. The values that will be examined in the simulation are the behaviour of the distribution cables and of the buses.
The code of colors of node elements (buses, feeders) and edge elements (lines, transformers) has been set in Power Factory in the following manner:

![Figure 5.5: Code of colors of node elements](image1)

![Figure 5.6: Code of colors for edge elements](image2)
5.4. ICS Attack Scenario

Overview of the Grid of Scenario 1

The simulation of the present scenario is defined as Steady State where the electricity loading due to residential, commercial and industrial activities has been taken at 21:00 hours of a summer period. This simulation corresponds in Power Factory as the RMS simulation. The loads for the EV charging station has been changed ranging from No EV loading up to 100%. In the Figure 5.7 the result of the simulation can be shown. The colors of the edge elements (lines) and the node elements (buses) correspond to code of colours signalized in the last subsection. As the loading of the elements for 0%, 50%, 80% and 100% of EV manipulation remain inside similar colour ranges, just the snapshot of the simulation of the results for 100% EV manipulation is shown in Figure 5.7.

![Figure 5.7: Present Scenario simulation when adversary has 100% EV Station Manipulation](image)

As it can be seen in Figure 5.7 the lines that present a major over loading are Slotermeer-Karpenweg and Papaverweg-Uilemburg. The lines that have the lowest complication are the ones directly connected to the generators Hemweg and Diemen. A more detailed analysis of each distribution line per scenario will be explained in the next section.
**Line Analysis**

In this section the loading of each one of the lines for the different present scenarios of EV charging station manipulation are shown (0%, 10%, 50%, 80% and 100%). The data has been obtained from the simulation in Power Factory and has been treated with the Data Analytics software Tableau for visualization purposes. The results for each one of the five aforementioned scenarios are shown in Figures 5.8, 5.9, 5.10, 5.11 and 5.12:

![Figure 5.8: Line Loading with no EV Charging Stations’ presence](image1)

![Figure 5.9: Line Loading with 10% EV Charging Stations’ presence](image2)
Figure 5.10: Line Loading with 50% EV Charging Stations’ presence

Figure 5.11: Line Loading with 80% EV Charging Stations’ presence
The lines in the city of Amsterdam are underground cables as they are suitable for areas where elements such as the aesthetics, the width and clearance problems are one of the major concerns. Every line has a capacity limit, meaning a thermal capacity according to the maximum current that each conductor can transport. When selecting the most suitable cable, this capacity is taken into account together with a safety factor in case an unpredictable load event could occur to avoid damages in the infrastructure. Moreover, every line experiences a voltage drop due to the impedance. In terms of design, it is imperative that the voltage drop does not exceed a certain threshold according to the distance of the line. Underground lines also increase the reliability, specially in the case of urban zones as Amsterdam.

When varying the load of each substation due to the change in numbers of the charging stations, we can see from Figures 5.8, 5.9, 5.10, 5.11 and 5.12 that in none of the above cases, the capacity of the lines is exceeded. Nonetheless, special interest should be placed in some sensitive cases where the loading of the lines is above 80%. The most sensitive case is the line that connects Slotermeer with Karperweg which has a loading equal to a 83.9 % of the line’s capacity. The second most sensitive case is the line that connects Zorgvlied with Karperweg with a 82.20 % and the third case is the line between Papaverweg and Uilenburg with a 81.10 % . Power Factory considers loading over 80% as sensitive case that should be considered to evaluation. On the other side, the least sensitive case is the line that connects Papaverweg and Vliegenbos with a 7.90% of loading due to the lower density of Electric Vehicle Charging Stations in comparison to the other zones.
BUS ANALYSIS
The second element that has been evaluated for the present scenario (0%, 10%, 50%, 80% and 100% of EV stations manipulation) is the voltage drop in the sub-stations buses. Similar than the line analysis, the results have been obtained from the simulation tool Power Factory and have been treated with the Data Analytics Software Tableau for visualization purposes. The results from the experiments can be seen in Figures 5.13, 5.14, 5.15, 5.16 and 5.17.

Figure 5.13: Voltage Drop in Buses with no EV Charging Stations’ presence

Figure 5.14: Voltage Drop in Buses with 10% EV Charging Stations’ presence
<table>
<thead>
<tr>
<th>Scenario / Bus Stop / EV Chargers</th>
<th>Voltage Deviation (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basisweg50</td>
<td>-0.100</td>
</tr>
<tr>
<td>Frederikplain10</td>
<td>-0.100</td>
</tr>
<tr>
<td>Frederikplain50</td>
<td>-0.160</td>
</tr>
<tr>
<td>Homweg50</td>
<td>0.020</td>
</tr>
<tr>
<td>Hooge Keldijk30</td>
<td>-0.200</td>
</tr>
<tr>
<td>Hooge Keldijk50</td>
<td>-0.013</td>
</tr>
<tr>
<td>Hooge Keldijk50</td>
<td>0.000</td>
</tr>
<tr>
<td>HW-Bus(3)</td>
<td>0.000</td>
</tr>
<tr>
<td>Karperveld</td>
<td>0.000</td>
</tr>
<tr>
<td>Karperveld50</td>
<td>0.000</td>
</tr>
<tr>
<td>Klaprozenweg150</td>
<td>-0.020</td>
</tr>
<tr>
<td>Marnixstraat10</td>
<td>0.553</td>
</tr>
<tr>
<td>Marnixstraat50</td>
<td>-0.200</td>
</tr>
<tr>
<td>Papaverweg10</td>
<td>-0.160</td>
</tr>
<tr>
<td>Papaverweg50</td>
<td>0.000</td>
</tr>
<tr>
<td>Papaverweg50</td>
<td>0.000</td>
</tr>
<tr>
<td>Rijnspoor10</td>
<td>0.567</td>
</tr>
<tr>
<td>Rijnspoor50</td>
<td>-0.100</td>
</tr>
<tr>
<td>Schipuijenlaan10</td>
<td>-0.200</td>
</tr>
<tr>
<td>Schipuijenlaan50</td>
<td>-0.100</td>
</tr>
<tr>
<td>Sloterdeel10</td>
<td>-0.180</td>
</tr>
<tr>
<td>Slootmeer10</td>
<td>-0.100</td>
</tr>
<tr>
<td>Slootmeer50</td>
<td>0.080</td>
</tr>
<tr>
<td>Uilenburg10</td>
<td>0.000</td>
</tr>
<tr>
<td>Uilenburg50</td>
<td>0.000</td>
</tr>
<tr>
<td>Verserweeg10</td>
<td>0.000</td>
</tr>
<tr>
<td>Verserweeg50</td>
<td>0.000</td>
</tr>
<tr>
<td>Vliegenbos10</td>
<td>0.000</td>
</tr>
<tr>
<td>Vliegenbos50</td>
<td>0.000</td>
</tr>
<tr>
<td>Watergraafsmeerslag30</td>
<td>1.000</td>
</tr>
<tr>
<td>Watergraafsmeerslag150</td>
<td>0.000</td>
</tr>
</tbody>
</table>

**Figure 5.15:** Voltage Drop in Buses with 50% EV Charging Stations’ presence

**Figure 5.16:** Voltage Drop in Buses with 80% EV Charging Stations’ presence
A bus operating inside the stable conditions should not have a voltage drop higher than +/- 5%. The voltage drop increases with the load and is in function of the distance that is supplies the energy to. As it can be seen from the results of Figures 5.13, 5.14, 5.15, 5.16 and 5.17 in none of the above cases, the voltage drop is higher than +/- 5% which means that even when all the charging stations are active, the electrical grid is still capable of withstanding the increase in the load, even in the peak hour of a summer period.

As a conclusion of the present scenario, the lines and the buses in the actual configuration of the Distribution Grid of Amsterdam are still able to cope with the increase of the loads due to the activation of 100% of the current installed Electric Vehicle Charging Stations. Therefore, a cyber-attack in the current scenario still would not present serious damages in the aforementioned elements. However, in the last subsection of this chapter, an analysis at feeder level will be develop in order to understand the voltage drop in the most vulnerable areas that have been identified in the first section of this chapter.

In the next section, a similar analysis at line and bus level will be carried on to assess the behaviour of the electrical grid for a future scenario where the number of charging stations is increased.
5.4.3. **Future Scenario: From 110% to 200% of EV Manipulation**

The analysis of line and bus behaviour has been also tested for a future scenario, where the amount of charging points has increased 110%, 150%, 180% and 200% taking into account the current infrastructure. This is of major importance to analyze at which point the number of charging points can increase before the stability of the distribution grid is compromised. Table 5.4 shows the input values that are added into the simulation regarding the electrical demand due to the EV charging points:

<table>
<thead>
<tr>
<th>Power Station</th>
<th>110% EV Demand [MWh]</th>
<th>150% EV Demand [MWh]</th>
<th>180% EV Demand [MWh]</th>
<th>200% EV Demand [MWh]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basisweg</td>
<td>1.4040</td>
<td>1.9146</td>
<td>2.2975</td>
<td>2.5528</td>
</tr>
<tr>
<td>Frederiksplein</td>
<td>3.6476</td>
<td>4.9740</td>
<td>5.9688</td>
<td>6.6320</td>
</tr>
<tr>
<td>Hemweg</td>
<td>1.3701</td>
<td>1.8683</td>
<td>2.2419</td>
<td>2.4910</td>
</tr>
<tr>
<td>Hoogte Kadijk</td>
<td>4.6639</td>
<td>6.3599</td>
<td>7.6318</td>
<td>8.4798</td>
</tr>
<tr>
<td>Karpenweg</td>
<td>5.6379</td>
<td>7.6881</td>
<td>9.2257</td>
<td>10.2508</td>
</tr>
<tr>
<td>Marnixstraat</td>
<td>3.2056</td>
<td>4.3713</td>
<td>5.2456</td>
<td>5.8284</td>
</tr>
<tr>
<td>Papaverstraat</td>
<td>3.0702</td>
<td>4.1867</td>
<td>5.0240</td>
<td>5.5822</td>
</tr>
<tr>
<td>Rhijnspoor</td>
<td>4.0885</td>
<td>5.5752</td>
<td>6.6902</td>
<td>7.4336</td>
</tr>
<tr>
<td>Schipluidenlaan</td>
<td>4.7145</td>
<td>6.4289</td>
<td>7.7146</td>
<td>8.5718</td>
</tr>
<tr>
<td>Slotermeer</td>
<td>3.1611</td>
<td>4.3106</td>
<td>5.1727</td>
<td>5.7474</td>
</tr>
<tr>
<td>Uilenburg</td>
<td>1.6980</td>
<td>2.3154</td>
<td>2.7785</td>
<td>3.0872</td>
</tr>
<tr>
<td>Venserweg</td>
<td>4.5904</td>
<td>6.2597</td>
<td>7.5116</td>
<td>8.3462</td>
</tr>
<tr>
<td>Vliegenbos</td>
<td>1.3490</td>
<td>1.8396</td>
<td>2.2075</td>
<td>2.4528</td>
</tr>
<tr>
<td>Watergraafsmeer</td>
<td>1.2895</td>
<td>1.7585</td>
<td>2.1101</td>
<td>2.3446</td>
</tr>
<tr>
<td>Westzaanstraat</td>
<td>2.5680</td>
<td>3.5018</td>
<td>4.2021</td>
<td>4.6690</td>
</tr>
<tr>
<td>Zorgvlied</td>
<td>8.0860</td>
<td>11.0264</td>
<td>13.2316</td>
<td>14.7018</td>
</tr>
<tr>
<td>TOTAL</td>
<td><strong>54.5443</strong></td>
<td><strong>74.3786</strong></td>
<td><strong>89.2543</strong></td>
<td><strong>99.1714</strong></td>
</tr>
</tbody>
</table>

Table 5.4: Input demand characteristics for simulating the future scenario with an increase of 110%, 150%, 180 & and 200 % of charging points

Similar than in the latter scenario, the EV Charging Station Loads will be aggregated by four digit post code. The value of the electrical loads is assumed to be the same than in the present scenario. However, it is expected that from a future standpoint there would be a potential increase in the electrical demand of the city, therefore in further research a safety factor can be added to the current load to compensate this increase.
OVERVIEW OF THE SYSTEM FOR DIFFERENT CASES

In this section, the overview of the results of each one of the simulations will be displayed. Figure 5.18 shows the map overview of the grid with the different code of colours already explained in the first part of this section.

Figure 5.18: Overview of the grid behaviour for the future scenarios when the EV load is increased by 110%, 150%, 180% and 200%

Figure 5.18 represents the behaviour of the edge elements (lines) and node elements (buses) according to the code of colours described at the beginning of this section. As it can be seen, the intensity of the colour of some lines increase when increasing the EV charging stations. Similar than in the later section, an analysis at lines and buses level has been carried on, and the results will be shown in the following sub sections.
LINE ANALYSIS

Similar than in the last section, the loading analysis for each one of the lines for the future scenario (110%, 150%, 180% and 200% of EV Charging Station's increase) has been carried on. The data has been obtained using the simulation tool Power Factory and it has been treated with the software Tableau for visualization purposes. It is expected that this analysis can give an overview of the analysis of results if the number of charging stations is duplicated considering the same electricity demand and Distribution Grid Infrastructure:

![Figure 5.19: Line Loading with 110% Charging Stations’ presence](image)
Figure 5.20: Line Loading with 150% EV Charging Stations’ presence

Figure 5.21: Line Loading with 180% EV Charging Stations’ presence
The objective of this analysis is to understand a potential future scenario if the number of Electric Vehicle Charging Stations is increased up to be duplicated while considering the same grid infrastructure. This increase in Electric Vehicle Stations has been relative to the density of the current EV charging stations per zone. When increasing the load from 10%, 50%, 80% and 100% it can be seen from the results in Figures 5.19, 5.20, 5.21 and 5.22 that in none of the above cases the loading of the lines overcome the 100% loading limit. For the case when the number of charging stations is doubled (the most extreme case) the line that has a higher loading is the one that connects Slotermeer with Karperweg with a line loading of 90.40% as this is the zone with the highest density of Electric Vehicle Charging Stations and also has a considerable high electricity demand. The second highest is the line connecting Papaverweg with Uilenburg with 86.90% and in third place Hemweg with Slotermeer with 86.90%. Even though the line loading has not overcome 100% is important to mention that the lines are already close to break the stability limits. Moreover, it is expected that by this future scenario there may be a considerable increase in the electrical load of Amsterdam. Therefore, further research should be performed by estimating the electrical load increase, and potentially the results could even show that the loading of the lines already overcomes the 100%. From a technical perspective, it is important to consider increasing the capacity of the cables in case the number of charging stations is already doubled in order to assure the resilience of the grid considering this as a security factor.
5.4. **ICS Attack Scenario**

**Bus Analysis**

The second element evaluated for the future scenario considering an increase of the EV Charging stations of 10%, 50%, 80% and 100% is the voltage drop at bus levels. These results have been also obtained with Power Factory and the data has been treated with the software Tableau. The results of the experiments can be shown in the Figures 5.23, 5.24, 5.25 and 5.26:

![Figure 5.23: Voltage Drop in Buses with 110% EV Charging Stations’ presence](image-url)
Figure 5.24: Voltage Drop in Buses with 150% EV Charging Stations’ presence

Figure 5.25: Voltage Drop in Buses with 180% EV Charging Stations’ presence
As mentioned in the last section a bus operating in stable conditions should not have a voltage drop higher than +/- 5%. From the results shown in the Figures 5.23, 5.24, 5.25 and 5.26 there is not a voltage drop that could destabilize the buses and they still remain inside stable operating conditions. Similar as what has been discussed for the line analysis, it is also expected that the electrical load of Amsterdam is likely to increase by this future scenario, and further research will be needed to test the outcome considering this growth.

As a general conclusion for the future scenario where the amount of charging stations is increased by 10%, 50%, 80% and 100% the loading of the lines is still inside the stability limits but the most sensitive case is almost close to overcome the maximum capacity of the line, therefore it is suggested to increase it, taking it as a security factor to avoid damages to the infrastructure and a potential electrical disruption. For the case of the buses from a substation level, they still have enough capacity to remain inside the stability limits (less than 5% of voltage drop). Moreover, is important that for the future scenario, forecasting methods should be implemented to predict the electric demand by this point of time. The latter could also represent a higher voltage drop that the one considered in this thesis work.
5.4.4. **Future Scenario: 2025 Panorama**

By the year 2025, The Netherlands has established as final goal, the zero-emissions in the transportation sector. As the implementation of electric mobility has been proved to be a promising path to achieve this goal, an increase in the number of EV Charging points is expected in the upcoming years. In Chapter 4 the number of charging points expected by the year 2025, in order to achieve the zero emission in the transportation sector, has been calculated. According to the values obtained, the simulation in Power Factory has run using these as input. Similar than in the present and future analysis carried on in the last subsection, the loading of the lines and the voltage drop of the buses have been calculated. The results of the experiments can be seen in Figure 5.27 and 5.28 respectively for lines and buses:

![Figure 5.27: Loading of the lines in % by the 2025 panorama](image-url)
The results of the experiment regarding the loading of the lines (Figure 5.27) shows that by the year 2025 the lines that connect Zorgvlied - Karperweg substations overcome its capacity by 109.5 %. The latter implies that the line may suffer from physical damage due to overheating and could potentially lead to an electrical disruption. The second most loaded line is the one that connects Papaverweg with Uilenburg with a 92.6 % loading and in third place the line that connects Hemweg with Slotermeer with a 80.5 %.

Regarding the analysis of the voltage drop of the buses, it can be seen that Hemweg does present a voltage drop of 5.509% which violates the stability of the system. Diemen has also a voltage drop close to 3% that even if it is inside the stability limits should be also taken into account.

Moreover, the electrical load (due to residential, commercial and industrial activities) that has been taken for this research work is the same as the present scenario. Therefore, a forecast analysis regarding the values that the electricity demand of the city may have by the year 2025 is imperative to have a more detailed analysis. In the case, the electricity demand is higher, then the results regarding the overloading of the lines and the voltage drop in the buses may be even considerably higher.
5.4.5. **Feeder Behaviour in the Most Vulnerable Zone**

The feeder is on charge of distributing power from the substations to the service transformers that are installed in the surroundings of the end customer. The power here is in the 0.4 kV level. Usually per substation the number of feeders can range from two to twelve in order to serve the area surrounding the substation. There are different configurations for the feeders which can range from radial, loop and network. Moreover, the feeders should be able to reach between substations within the engineering criteria.

The distribution feeder layout is a very important aspect that needs to be taken into account for this research work. Feeders tend to follow roads, highways or boundaries and the routing is most of the time estimated by using a rectangular grid that represents the roads or streets. Therefore, in order to calculate the distance between two locations, this is achieved by calculating the Euclidean metric Distance:

\[
\text{Distance} = \sqrt{\Delta X^2 + \Delta Y^2}
\]  

(5.1)

The maximum feeder delivery distance is 0.75 times the distance between the substations. According to the Power Distribution Planning Reference Book, this can be taken as rule of thumb. Moreover, today more than 80% of the electrical distribution in the world is achieved by radial feeders. Even if the design of the feeders is a radial circuit, in reality they are actually built as a network (which is the case of the Amsterdam’s grid according to the open map Pico [16]). Nonetheless they are operated radially due to the use of switches in strategic points to impose the radial flow pattern.

From a grid designer perspective is imperative to understand the criteria for the system when working in normal conditions and in a contingency scenario. The theory suggests that for normal operating conditions the ANSI C84.1-1989 range A should be the design criteria while the range B for contingency scenarios. The range A suggests a voltage drop on the primary feeder system of 7.5% (9 volts on a 120 volt scale) while Range B allows 10.8% of voltage drop (13 volts on a 120 volt scale).

In the following experiment the analysis of the most vulnerable zone detected on the subsection 1 of this chapter will be elaborated focusing on the voltage drop from a feeder level. The results of the experiments for the feeders in the Post Codes 1012, 1017, 1071 and 1077 can be shown in the following Figures 5.29, 5.30, 5.31 and 5.32 respectively:
5.4. ICS Attack Scenario

Figure 5.29: Voltage Drop of feeder and number of charging stations in Post Code 1012

Figure 5.30: Voltage Drop of feeder and number of charging stations in Post Code 1017
Figure 5.31: Voltage Drop of feeder and number of charging stations in Post Code 1071

Figure 5.32: Voltage Drop of feeder and number of charging stations in Post Code 1077
Figures 5.29, 5.30, 5.31 and 5.32 show the analysis of the voltage drop of the feeders in the most vulnerable zones that have been discussed at the beginning of this chapter. Furthermore, the number of charging stations that correspond to each value of the voltage drop, together with the percentage of charging stations relative to the present scenario is also shown.

For the case of the Post Code 1012 in Figure 5.29 it can be seen that in the present scenario, when 100% of the charging stations are active, it corresponds to a 7.262% of voltage drop at the feeder level which still is considered inside the stability limits. 100% of charging station corresponds to a value of 122. Nonetheless, for a future scenario where the number of charging stations is increased by 50% it is expected a voltage drop of 10% which can reduce the stability limits of the feeder.

For the case of the Post Code 1017 in Figure 5.30 it can be seen that when all the charging stations are active, the feeder presents a voltage drop of 9.62% which is higher than the range A (for a system operating in normal conditions) but still is lower than range B for contingency analysis. Nonetheless an increase of just 10% of charging stations in this area may lead the feeder to have a voltage drop higher than 10% and therefore, destabilize the system.

For the Post Code 1071 in Figure 5.31, the present scenario suggest than 100% of active EV stations is equal to a voltage drop of the feeder of 8.15% which is higher than range A and also lower than B. Nonetheless, if the number of charging stations in this area increases by 30% it is expected that the feeder will be violating range B of the voltage drop limits.

Finally, for the Post Code 1077 in Figure 5.32 100% use of the current EV charging stations already violates the stability of the Feeder. Therefore, special attention should be placed in this area, as we can see in the Figure 4.12b that this post code has the highest density of EV Charging Stations.
5.5. **Assumptions**

The assumptions made in this research work are:

1. **The aggregation of the loads and their connection to the different substations**
   As mentioned before, the loads have been aggregated by Four Digit Post Cost in order to reduce the computational power needed in the simulation. The aggregated loads have been connected to the closest substation according to the distribution lines paths that can be seen in [16]. Nonetheless, for some cases the two substations are connected to one single post code or other loading distributions can also be possible. The simulation deviation from this assumption has been tested with a sensitivity analysis that is displayed in the next paragraphs.

2. **The IT network topology of the CPO’s system**
   Each company has their own network topology that has been developed by the IT department. Their virtual or physical segmentation, the location of the firewall, the protection measures used, among other characteristics can only be known if a real pen-testing analysis is performed on the systems. As the latter exercises has not been done, the conventional IT configuration has been considered in this research work. This is conformed by the cloud - Firewall - DMZ (where the web sever is located) - Internal Network.

3. **Characteristics of the transformers**
   Determining the exact technical characteristics of the distribution transformers is a very complicated task as the theoretical values can change from the real ones depending on the decisions taken by the DSOs. Therefore, the technical characteristics that are suggested by [25] have been used.

4. **Distribution of the increment on EV Charging stations in the future scenario**
   For the future scenarios, the increase of the the charging stations has been done proportional to the present scenario. Nonetheless, is important to consider that this growth is in function of different variables that.

5. **Value of the load used in the future scenarios**
   The growth of the loads in the future scenario is the same than in the present scenario. The reason of the latter, is that even if by future scenarios the electrical demand is expected to increase, diverse variables such as the economical situation of Amsterdam, changes in the demographics, among other characteristics can change the outcome of this growth. Therefore, forecasting methods are expected to be used in order to determine accurately the loads in the future years.
5.6. Sensitivity Analysis

As mentioned before, the most sensitive assumption has been the aggregation of the loads by four digit zip code, as the loads can be distributed in a different way in the real scenario and connected to other substations than the ones in this research work. In order to perform the sensitivity analysis, the loads have been redistributed three different times in a random fashion. The loads in some zip codes have decreased while in the neighbor zip code have increased. The latter is because in most cases a zip code is connected to more than one substation and therefore, this variations are expected. In order to assess this variation the results, the changes in the loading in the capacity of the lines have been calculated. The result of the latter exercise can be seen in Figure 5.33.

![Figure 5.33: Sensitivity analysis for the overloading of the lines. Base case and three different variations](image-url)
Figure 5.33 shows the variations of the line loading for each electrical load re-distribution. The dark blue circles represent the baseline case, while the other three cases are represented by green, red and yellow. A close look of the stations that connect Hoogte Kadijk - Uilenburg and Klaprozenweg - Hoogte Kadijk can be visualized in Figure 5.34. As it can be seen, the differences in the line loading for the Hoogte Kadijk - Uilenburg are for the red case 2.37%, the green case 6.95% and for the yellow case 10.43 %. In the case of the line that connects Klaprozenweg - Hoogte Kadijk are for the red case 2.016%, the green case 1.77 % and for the yellow case 9.51%. Therefore, the variation of loading of the lines can range from 2.37% until 10.43%. In order to provide the least possible error, powerful co-simulation methods are suggested that could allow a better granularity of the electrical loads. The least the loads are aggregated, the more accurate the results could be.
Conclusion
The aim of this research work was to perform a cyber-security assessment of the Electrical Vehicle Charging Infrastructure in the Electrical Distribution Grid of the city of Amsterdam. The motivation behind this assessment was to analyze the capacity of the current electrical distribution grid, as the exponential increase of electric vehicles in the Amsterdam area has not given the adequate space for a proper planning from a technical standpoint. Moreover, cyber-security has become one of the major elements that should be taken into account when designing the infrastructure of any sensitive asset. Examples such as Stuxnet, have proved that cyber-security is not just a matter of Information Technology anymore, but that Operational Technology is also playing a very important role. Consequently, the second objective of this thesis work was the replication of the steps that a potential attacker would likely follow when targeting the EV Charging Station’s infrastructure. The outcome of this assessment can provide valuable recommendations that could improve the resilience of this ICS.

The main difference between an ICS attack and the traditional IT attacks, is that the ICS attacker must have a detailed knowledge regarding the functionality of the system which increases its complexity. Moreover, an attack to an ICS is most of the times part of a campaign where the attacker has a clear motivation to disrupt the correct operation of a certain infrastructure. Due to the latter, several elements were needed to be understood prior to the planning of the attack. The first element was the selection of the most suitable area for launching it. In order to do that, the topology of the city of Amsterdam was analyzed, a segmentation of the city was created and the most suitable area for performing the attack was identified using a function composed of five variables. The most vulnerable zone is the one with the highest electrical load and a high electric vehicle chargers density. It has been found that the population density is directly proportional to the amount of charging stations and, also to the electricity demand. The selected zone for launching the attack includes the most vulnerable zones of Amsterdam, but also includes other zones with a lower risk ratio, as these are also important to be analyzed because they are not extreme scenarios. Furthermore, the zones where the electrical loads were high but the amount of charging stations low, were not taken into account as these zones are less susceptible to an attack targeting EV Charging Stations.

Other crucial component was the selection of the best moment to launch the attack. This is because the stability of the Electrical Grid depends on several factors such as the electrical demand, the characteristics of its components and seasonal factors (as the stability of the components is sensitive to variations in the temperature). Due to the latter, two elements were taken into account. The first was the electrical demand hourly behaviour in a year period and the second was the EV Charging users’ behaviour. The results showed that high peaks of electricity demand were registered at 21:00 of a summer period. In the case of the users’ charging behaviour, several research studies suggested that also 21:00 has been a trending hour for the users to charge their cars. Therefore, for this research work it has been assumed that best time to perform the attack is 21:00 o a summer period. Consequently, the data that has been used for the simulation at 21:00 covering the months from June to September in the year 2015.
It has been also concluded that the motivations behind an ICS Cyber attack can be a combination of political, socio-cultural and economical factors where typical examples can range from terrorism, cyber-war, hacker-reputation, state actors, revenge, among others. Even if some authors attribute the motives for compromising an ICS to be more likely from political or economical nature, some reported attacks against ICS, show that enhance hackers reputation has been a crucial reason. Therefore, it is important not to discard any motive and to be aware of the potential causes.

Moreover, in order to perform an accurate cyber-security assessment, one crucial element is to think as the adversary would do. The methodology that was used in this research work was the Kill Chain, as it describes the steps that a potential adversary will likely follow when performing an attack. As the Kill Chain has been created for traditional IT attacks, a variation of it made by the authors Assamte M. and Lee R. - the ICS Cyber Kill Chain - has been used. It has two stages, the first one is similar to the traditional IT Kill Chain where the attacker has access to the system and the second part is mainly focused on the ICS threat development.

The first step of the kill chain was the Planning: Reconnaissance stage where the attacker gathers all the sensitive information for launching the attack. This information gathering was performed at three levels: Understanding how the system that controls the charging station works, understanding the IT infrastructure of the targeted victim and how is the related OT infrastructure designed.

In the latter exercise, the most suitable victim was the CPO with the major coverage of charging stations in Amsterdam (quantity wise and also due to the amount of kW that it has access to). Moreover, when analyzing the characteristics of the system that controls the charging stations, it has been discovered that it is cloud-based and the access depends only on the credentials given by the users. The CPO administrator has the capacity to control remotely the charging stations, which is a necessary element for the development of the attack. An interesting characteristic is that usually most of the ICS are not connected to the internet and not even to an internal network. The fact that the system that controls the charging stations is cloud based, diminishes the level of complexity of the attack.

In the attack scenario purposed in this thesis work, the adversary can either choose to compromise the web sever that hosts all the information regarding the EV charging control system of the CPO company or can either try to access the computer of the administrator of the charging stations. The first possibility is more challenging in the sense that more security parameters will needed to be overcame but more information regarding the credentials can be obtained. On the other side, only by compromising the CPO administrator computer, the level of security layers that need to be bypassed are lower and only the credentials of this administrator will be obtained.
In any of the aforementioned scenarios, information was obtained regarding the key people working in the company together with their personal data and on the other side also information regarding the web server was retrieved. This shows a clear vulnerability in terms of the company’s security policies.

From an IT perspective, information regarding the IP of the web server, host data, open ports, the type and version of the operational system was also found. From this part, a Virtual Machine has been configured with the characteristics obtained from the IT reconnaissance section in order to execute the rest of the attack. This type of information can be easily obtained using conventional pentesting tools that are available online. From a company perspective it is important to understand the type of IT information that can be retrieved by a third party. The weaponization phase was carried out in the Virtual Machine where the targeted web server was replicated. The GUI version of Metasploit: Armitage has been used and the intrusion was successful. From an Information Technology perspective, the complexity to compromise the systems is not high and therefore, in the next chapter recommendations are given to increase the level of security.

On the other side, it has been essential to understand of the Operational Technology characteristics that surround the attack scenario. How does the distribution grid look like. In order to test the attack, a mirrored environment was generated. For this case, this environment is equal to the distribution grid of Amsterdam. The distribution grid of Amsterdam has been reversed engineered using information from open sources. This was replicated in the Simulation software for power systems: Power Factory 2015. This mirrored environment, has very similar characteristics to the real distribution grid in terms of the parameters of the substations, buses and lines. The geographical position of the aforementioned elements has also been considered to be as close as possible to the real grid. Since managing each house, commerce or industry as an individual load results in a very complex process from the computational effort that will be needed, an aggregation of the loads was elaborated at four-digit post code level. Three data sets were created from information retrieved from different open sources: FourPostCodeDataSet, SixPostCodeDataSet and DemandperHour. The load could have been considered by Six PostCode but this would also have increased the complexity from a computational standpoint, although it would have lead to a higher accuracy of the system.

Stage II of the Kill Chain, was focused on the attacks directed to the ICS infrastructure considering present and future scenarios. The results of the future scenarios can help to create preventive measures and to understand the weak points from the grid perspective.

For the present scenario, the attack was tested when the adversary had control over 10%, 50%, 80% and 100% of the charging stations. Even for the case that the attacker had control over all the charging stations, the lines did not overcome their loading limits, nonetheless the highest loading was 83.30 % which is close to violate the stability limits. In the case of the buses the simulation results suggest that none of them has a voltage drop higher than 10 %, therefore is still considered inside the stability limits.
For the future scenario where the number of charging station was doubled, the attack scenario was tested for the control of 110%, 150%, 180% and 200% of EV Charging Station manipulation. The lines, still remain below 100% of loading, where the most extreme case has an utilization of 92%. Moreover, the buses, are still inside the stability limits and do not have a higher voltage drop than 10.8 %. The most interesting case is for the 2025 scenario, where the lines are close to break their stability limits and one line overloads with 109.5 %. In the case of the buses, one of them goes beyond the +/- 10.8 % stability limit and this can mean a potential electrical interruption.

For the feeder analysis it is important to understand that a 100% activation of the charging station in some cases is already violating what is established on the Range A standards in voltage drop of feeders, but still does not violate range B for contingency situations. Nonetheless it is expected that an increase in the number of charging stations will definitely overcome the established 10.8% of voltage drop and this can lead to an electrical disruption. In the case the number of EV Charging Stations will increase in the upcoming years it is definitely necessary to evaluate the current infrastructure and upgrade it in order to overcome this vulnerability.

Finally, we can conclude that a cyber attack to the EV Charging Station Control System has a lower complexity than any other ICS that is not cloud base. The latter increases the ease of the process but definitely reduces the security of the whole system. Moreover, an attack in the current infrastructure would not provoke an electrical disruption and the current distribution grid can stand 100% of activation of the installed charging points. Nonetheless, in order to achieve the 2025 goal, changes in the current distribution grid would be needed, as from a technical perspective the infrastructure would not be capable to withstand the increase in the loads.
Recommendation for future work
THE main purpose of performing each one of the steps of the Kill Chain is to provide useful recommendations that can be used in the future for improving the security of the Industrial Control Systems. The recommendations will be divided on IT and on OT level, in order to follow the same structure as the one of the methodology used in this research work. The main objective of these recommendations is on one side to enumerate the vulnerabilities that the current infrastructure has and on the other side to give an idea of elements that could be improved that would allow a safe implementation of the Electric Vehicles technology into society.

From an IT standpoint, the system that controls the stations presents many facilities from an attacker perspective. The first recommendation is not to have the system cloud-based. Although such architecture eases the communication between the operator and the charge point, it is also exposed to the traditional IT attacks. As the rule of the thumb, I recommend that any ICS control system should not be connected to the internet, nor any internal network of the company, as this gives more channels for accessing the system. One of the most important elements, when planning a safe network infrastructure is the concept of Security in Depth, which means providing different layers of security elements (onion concept) such as DMZ, honeypots, Intrusion Detection Systems, Firewalls, virtual network segmentation’s, etc to decrease the likelihood of an attacker controlling the system. Another element that can be improved in this software is that a password should be required every time the operator wants to manage remotely the charging point, and a different password should be assigned per charging point. As the latter recommendation, increases the difficulty for the operator in terms of password managing, it does imply a new barrier for the attacker. Moreover, is important not to store those passwords in any place in the system (even if they are not in plain text). A solution could be the use of a password manager that can easily solve this problem. Another element that is always beneficial in terms of security is an activity log of each one of the users that have access to the control system. This allows no repudiation, which means that the person responsible of certain action cannot deny that she/he has done it. Securing this activity log with a very strong password is also required, as many attackers tend to erase the activities.

If the system infrastructure is only designed to be cloud-based and changing this element would lead to more complications, one solution would be to just allow one session per user and to notify a third party (or even a fourth) every time a session has started. Therefore, someone else is aware when a new session is on and who is the person responsible. Another element I consider vital, in the case that the attacker has already intruded into the web server and is looking for the hashes of the credentials of the users. Most of the network administrators tend to save these passwords in a default place or tend to give the folders obvious names (e.g. credentials, passwords). I consider that storing those in an uncommon place and giving the folders names that could miss lead the attacker could reduce the likelihood to be found.
Another element that I consider vital to discuss are the results from the reconnaissance step. Gathering the user information and the IT characteristics of the system was not a complicated task from an attacker perspective. It is very important that companies are aware of what their employees are sharing in social media channels or which information they are allowing to be public. All these information can be misused and can be seen as opportunities for potential blackmailing or for using social engineering against one of these employees. I could even imagine that directed and tailored made phishing attacks can be performed for each employee that seems to be a potential delivery point. Also from a technical perspective, it is important that the person/organization in charge of setting the web server is conscious of the information that an attacker can get from Whois, Nmap and even a tool like Metasploit Framework. It is important to reduce the amount of information that can be obtained by the usage of these tools, as they are open source, available to the public and one of the most popular elements among attackers in these days.

From the conventional security recommendations it is important not to forget to update the operational system every time it is needed, as well as any other tool that is used inside the company as they can be entry points for a potential attacker. Hiring pentesters can also help to understand which are the security breaches of the company and what can be done to reduce the likelihood of attacks. Finally, training the personnel about social engineering should be a must in every company. When I called to ask for information about the system, I got access to some information that could even be misused by a potential attacker.

From an Operational Technology perspective, there are many elements that can also be improved. In first place, there is enough information form open sources to replicate the grid of Amsterdam. From a government perspective, it is important to understand what information can a potential attacker have access to from a Infrastructure standpoint and if that available information online is enough to mirror a sensitive asset. The cables that are being used today will not have enough capacity to withstand the loads in a 2025 panorama. Those will need to be replaced with more capacity to reduce the overloading of cables. From a feeder level, these also need to be re design as they will not be able to cope with the high increase in the loads. The voltage drop results in the buses suggest that they are still capable of withstanding the loads without having a voltage drop higher than 10%.

Higher densities make a zone to be weaker. It is important to understand from a city planning perspective, that high population densities will lead to a higher electricity demand that will at the same time lead to a higher demand of electrical charging points. It is important to reduce this concentration points as these are vulnerable zones of the cities and are more prone to be targets to a potential attack. Making a better city distribution from a population perspective can definitely reduce the possibility of an attack.

Another element that has been already discussed by the municipality, is the modulation of the EV users’ charging behaviour. As many users follow a similar pattern, it is impor-
tant to manipulate the charging sessions in a sense that there is not a clear peak hour for charging, but there is an even distribution during the day. This also reduces the likelihood of a potential attack to be successful.

Finally I consider that sharing the risk is one of the most important elements that should be always expected. Having Nuon as the one with the main privilege to install charging stations do imply a higher risk as they become the most suitable target from an attacker perspective. Intruding into the systems of Nuon imply manipulating more that 80% of the cities charging stations. Having more companies that share this, will be challenging for an attacker as they will need to compromise more companies in order to control a high amount of MWh.

It is expected that this thesis work can be a stepping stone into the correct planning of the infrastructure, not just of the city of Amsterdam, but to any other city that intends to adopt the EV technology as part of its framework. Finally, I consider that cyber-security will play a new and crucial role for the humanity transition into a sustainable future.
APPENDIX I

Diagrams of the 19 substations in the simulation software Power Factory.

Figure 7.1: Hemweg 150 Sub-Station
7. Recommendation for future work

Figure 7.2: Hemweg 50 Sub-Station

Figure 7.3: Diemen Sub-Station
Figure 7.4: Basisweg Sub-Station

Figure 7.5: Frederiksplein Sub-Station
Figure 7.6: Hoogte Kadijk Sub-Station

Figure 7.7: Karpenweg Sub-Station
Figure 7.8: Klaprozenweg Sub-Station

Figure 7.9: Marnixstraat Sub-Station
7. RECOMMENDATION FOR FUTURE WORK

Figure 7.10: Papaverweg Sub-Station

Figure 7.11: Rhijnspoor Sub-Station
Figure 7.12: Schipluidenlaan Sub-Station

Figure 7.13: Sloteermeer Sub-Station
Figure 7.14: Uilenburg Sub-Station

Figure 7.15: Venserweg Sub-Station
Figure 7.16: Vliegenbos Sub-Station

Figure 7.17: Watergraafsmeer Sub-Station
Figure 7.18: Westzaanstraat Sub-Station

Figure 7.19: Zorgvlied Sub-Station
LIST OF FIGURES

1.1 Part of Stuxnet’s Code that targets Step 7 projects and PLC manufactured by Siemens. [1] .......................................................... 4
1.2 Characteristics of Stuxnet from a Technical and an Attack Scenario Perspective .......................................................... 5
1.3 Car2go launched in Amsterdam as an electrical car sharing concept [4] ......................................................... 7
1.4 Amsterdam encourages charging stations in parking lots [4] .................. 7
1.5 The ten-step process for requesting a charging station .................. 8

2.1 Motivation behind Cyber Attacks by type: Socio-Cultural, Political and Economic ..................................................... 13
2.2 Amsterdam’s topology and 7-zone division Ref. [17] ...................... 15
2.3 Graphical representation of different variables: Main activity per zone, population density, electricity demand and number of electric vehicle chargers. Ref. [13] .......................................................... 16
2.4 Amsterdam’s control zone selected for the attack scenario [17] .......... 17
2.5 Histogram of relative charging frequency by EV ownership Ref. [18] ... 18
2.6 Average summer and winter hourly electrical demand in Amsterdam per 10,000 customers in kWh/h ...................... 19
2.7 The EV Charging Station Infrastructure and communication protocols 20
2.8 OCPP Protocol communication scenarios. The red circle indicates the Smart Charging Command Ref. [26] .......................... 26

3.1 Cyber Kill Chain Methodology by Lockheed Martin ....................... 28
3.2 Steps in the ICS Cyber Kill Chain in Stage I [30] ...................... 30
3.3 Three steps of the ICS Cyber Kill Chain Stage II Ref. [30] ........... 33
3.4 Levels of complexity of an ICS Attack .................................. 35
3.5 Objectives of an ICS cyber attack ......................................... 36
3.6 Proposed Attack Scenario to EV Charging Station System .......... 37
3.7 ICS Cyber Kill Chain Stage I: Applying the attack scenario of this research work ........................................................................ 40
3.8 ICS Cyber Kill Chain Stage II: Applying the attack scenario of this research work .......................................................... 40

4.1 Three Levels covered in the Planning (Reconnaissance) stage ........ 42
4.2 Overview of the interface that manages the EC Charging Stations of the targeted company [36] ............................................. 46
4.3 EV Charging Station’s Administrator Interface [36] ................. 47
4.4 Charging Administration Manager Web Interface [36] .............. 48
4.5 Charging Station Transaction Web Interface [36] ........................................ 48
4.6 Steps to perform IT reconnaissance with their corresponding tool. *Metasploit Framework will be addressed in the next chapter, weaponization* ........................................ 49
4.7 NSLookup results: The IP addresses of important servers ................................ 50
4.8 Information obtained by the use of the command Whois ................................ 51
4.9 Example of the Nmap output command line ...................................................... 53
4.10 Electricity Demand in Amsterdam in kWh/hour per Four-Digit Post Code ............ 56
4.11 Top 10 Electrical Demand per Post Code. The red bars represent the total electricity demand, the green bars commercial, residential and industrial activities together and the blue bars the amount of consumption of the EV Charging Stations .................................................. 56
4.12 Heat Maps of the electricity demand in Amsterdam due to residential, commercial and industrial activities (left) and due to the amount of EV Charging Stations (right) .................................................. 58
4.13 Summary of the characteristics of the Electrical Distribution Grid of Amsterdam .................................................................................................................. 60
4.14 Characteristics of the Substations by Voltage Leves ........................................ 61
4.15 Characteristics of the Substations by number and type of connection ................ 61
4.16 Characteristics of the distribution Lines in the electrical grid of Amsterdam .... 62
4.17 The five steps for using Metasploit Framework ................................................. 67
4.18 Scanning hosts and networks with Armitage .................................................... 68
4.19 Output of the scanning with Armitage .............................................................. 68
4.20 Finding Attacks with Armitage ........................................................................... 69
4.21 Attack Analysis in Armitage .............................................................................. 69
4.22 Attack Options available per host in Armitage .................................................. 70

5.1 Reversed Engineering of the Amsterdam’s Distribution Grid in Power Factory 2015 ............................................................................................................. 79
5.2 Vulnerable Zones in the EV Charging Station Attack Scenario ....................... 80
5.3 Number of hospitals/health clinics per zip code ................................................. 81
5.4 Number of Train Stations per Zip Code ............................................................ 81
5.5 Code of colors of node elements ........................................................................ 84
5.6 Code of colors for edge elements ....................................................................... 84
5.7 Present Scenario simulation when adversary has 100% EV Station Manipulation .............................................................................................................. 85
5.8 Line Loading with no EV Charging Stations’ presence ..................................... 86
5.9 Line Loading with 10% EV Charging Stations’ presence ................................... 86
5.10 Line Loading with 50% EV Charging Stations’ presence .................................. 87
5.11 Line Loading with 80% EV Charging Stations’ presence .................................. 87
5.12 Line Loading with 100% EV Charging Stations’ presence ................................ 88
5.13 Voltage Drop in Buses with no EV Charging Stations’ presence .................... 89
5.14 Voltage Drop in Buses with 10% EV Charging Stations’ presence .................. 89
5.15 Voltage Drop in Buses with 50% EV Charging Stations’ presence .................. 89
5.16 Voltage Drop in Buses with 80% EV Charging Stations’ presence .................. 89
5.17 Voltage levels in buses for the 100% of EV Manipulation ................................. 91
5.18 Overview of the grid behaviour for the future scenarios when the EV load is increased by 110%, 150%, 180% and 200% ................................................. 93
5.19 Line Loading with 110% Charging Stations’ presence ................................ 94
5.20 Line Loading with 150% EV Charging Stations’ presence ............................ 95
5.21 Line Loading with 180% EV Charging Stations’ presence ............................ 95
5.22 Line Loading with 200% EV Charging Stations’ presence ............................ 96
5.23 Voltage Drop in Buses with 110% EV Charging Stations’ presence ............... 97
5.24 Voltage Drop in Buses with 150% EV Charging Stations’ presence ............... 98
5.25 Voltage Drop in Buses with 180% EV Charging Stations’ presence ............... 98
5.26 Voltage Drop in Buses with 200% EV Charging Stations’ presence ............... 99
5.27 Loading of the lines in % by the 2025 panorama ........................................ 100
5.28 voltage drop in the buses by the 2025 panorama .................................... 101
5.29 Voltage Drop of feeder and number of charging stations in Post Code 1012 .... 103
5.30 Voltage Drop of feeder and number of charging stations in Post Code 1017 .... 103
5.31 Voltage Drop of feeder and number of charging stations in Post Code 1071 .... 104
5.32 Voltage Drop of feeder and number of charging stations in Post Code 1077 .... 104
5.33 Sensitivity analysis for the overloading of the lines. Base case and three different variations ................................................................. 107
5.34 Sensitivity analysis for the overloading of the lines. Zoomed analysis for two substations ................................................................. 108

7.1 Hemweg 150 Sub-Station ................................................................. 119
7.2 Hemweg 50 Sub-Station ................................................................. 120
7.3 Diemen Sub-Station ................................................................. 120
7.4 Basisweg Sub-Station ................................................................. 121
7.5 Frederiksplein Sub-Station ................................................................. 121
7.6 Hoogte Kadijk Sub-Station ................................................................. 122
7.7 Karpenweg Sub-Station ................................................................. 122
7.8 Klaprozenweg Sub-Station ................................................................. 123
7.9 Marnixstraat Sub-Station ................................................................. 123
7.10 Papaverweg Sub-Station ................................................................. 124
7.11 Rhijnspoor Sub-Station ................................................................. 124
7.12 Schipluidenlaan Sub-Station ................................................................. 125
7.13 Slotermeer Sub-Station ................................................................. 125
7.14 Uilenburg Sub-Station ................................................................. 126
7.15 Venserweg Sub-Station ................................................................. 126
7.16 Vliegenbos Sub-Station ................................................................. 127
7.17 Watergraafsmeer Sub-Station ................................................................. 127
7.18 Westzaanstraat Sub-Station ................................................................. 128
7.19 Zorgvlied Sub-Station ................................................................. 128
LIST OF TABLES

2.1 Protocols in the EV Charging Infrastructure with their functionalities . . . 22

4.1 CPOs operating today in Amsterdam ........................................... 44
4.2 Mobility growth in The Netherlands and Amsterdam in conventional and electric vehicles ..................................................... 65

5.1 Scenarios that will be tested in the replicated environment ............ 77
5.2 Characteristics of the reversed engineer distribution grid of Amsterdam 78
5.3 Input variable values for the simulation in the first case ............... 83
5.4 Input demand characteristics for simulating the future scenario with an increase of 110%, 150%, 180 & and 200 % of charging points .......... 92
References


[7] Siddharth S., Manimaran G. (2010), *Data integrity attacks and their impacts on SCADA control system*, IEEE PES General Meeting


