35th International Electric Vehicle Symposium and Exhibition (EVS35)
Oslo, Norway, June 11-15, 2022

Cyber Attacks on Electric Vehicle Charging Infrastructure and Impact Analysis

Sjors Hijgenaar[1], Baerte de Brey[2], Alexandru Stefanov[3], Peter Palensky[3]

[1]*Stedin Netbeheer B.V., The Netherlands, sjors.hijgenaar@stedin.net*

[2]*ElaadNL, The Netherlands, baerte.de.brey@elaad.nl*

[3]*Delft University of Technology, The Netherlands, a.i.stefanov@tudelft.nl, p.palensky@tudelft.nl*

Summary

As a global response to climate change, fossil fuelled cars are replaced by Electric Vehicles (EVs) at an accelerating pace. The EV charging infrastructure relies on Information and Communication Technology (ICT) and Internet of Things (IoT). It is well recognised that ICTs and IoT are vulnerable to cyber attacks. Therefore, power grids become susceptible to disruptions at the grid's edge. Models are needed to analyse the power grid resilience to cyber attacks on EV charging infrastructures and quantify the impact on the distribution system operation. In this paper, we propose a method to assess the impact of cyber attacks on EVs considering their stochastic charging behaviour, and energy transition scenarios. We describe cyber attack scenarios on EV charging infrastructures and assess their impact on the Dutch distribution system operation. Simulation results under different scenarios of EV adoption show that currently the Dutch distribution system is cyber resilient. However, we conclude that the expected 370% increase in EV-related load by 2030 may cause significant operational issues. Therefore, we emphasise the necessity for a paradigm shift to cyber secure the EV charging infrastructure.

Keywords: charging infrastructure, cyber attacks, cyber security, EV (electric vehicle), legislation, resilience

1 Introduction

As a global response to climate change, fossil fuelled cars are replaced by Electric Vehicles (EVs). The widespread introduction of the necessary EV charging infrastructure has accelerated [1]. This charging infrastructure relies on Internet of Things (IoT) and Information and Communication Technology (ICT). It is widely recognized that IoT and ICTs are vulnerable to cyber attacks. Thus, EV charging infrastructures are susceptible to malicious interference with varying, potentially disastrous effects for electric power distribution systems.

Several works have been published on the vulnerabilities of internal EV and Charge Point (CP) components [2], [3]. Examples of vulnerabilities are access to the EV Control Area Network (CAN) bus or physically tampering with a CP to install malware. A cyber attack exploiting these kinds of vulnerabilities is largely limited to the individual EV or a limited section of the charging infrastructure. Other authors report on more intelligent attack scenarios [4]. Attacks in this category require intricate knowledge of the cyber-physical system, how it is operated

and prevailing market conditions. These attacks target service providers, disrupting flexibility schemes or the operation of larger amounts of CPs. Their effects may disrupt distribution networks. Several authors reported vulnerabilities in widely used communication protocols [5]. As an example, most CPs use the Open Charge Point Protocol (OCPP) to communicate with Charge Point Operator (CPO) back offices. Alcaraz et al. [5] demonstrate that subversion and malicious endpoints allowed for Man-in-the-Middle (MitM) attacks in OCPP v1.6. They show how attackers can control the charging rate of multiple CPs when communication can be intercepted. An attack utilizing a vulnerability of this scale may lead to a power system blackout. As more EV charging infrastructures are introduced, cyber attacks may threaten the entire continental power grid in Europe. However, much is unknown about the impact of cyber attacks on EV charging infrastructures. Therefore, in this paper, we propose a method to model cyber attacks on the EV charging infrastructure and assess their impact on power system operation. The contributions in this paper are:

- A description of cyber attack scenarios based on vulnerabilities found in literature.
- A novel method to model cyber attacks on EV charging infrastructures using stochastic charging behaviour and energy transition scenarios.
- Impact analysis of cyber attacks on the distribution system operation.
- A discussion on the necessity of legally binding cyber security requirements for EV charging infrastructures, including an analysis of the relevant legal framework.

The remainder of this paper is organised as follows. Chapter 2 describes the cyber resilience of power grids, the EV charging infrastructure, and cyber attack scenarios. Chapter 3 presents the modelling methodology. Chapter 4 presents the simulation results of a cyber attack scenario. Chapter 5 discusses the necessity for legislative measures. The conclusions are given in Chapter 6.

2 Cyber Threats in the EV Charging Infrastructure

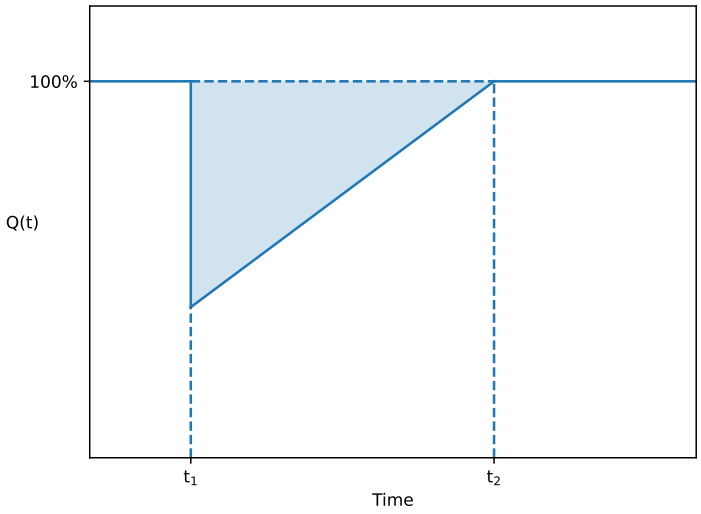
2.1 Power Grid Cyber Resilience

The notion of resilience stems from ecology in 1973 [6] and was adopted by numerous engineering fields in the decades that followed [7], of which power system engineering is no exception. Resilience has been widely recognized as the ability of a system to withstand High Impact Low Probability (HILP) disruptions and quickly return to an equilibrium state afterwards [8]. Research on power system resilience mainly considers extreme weather events [9], i.e., how power grids are physically affected by the destructive force of hurricanes, earthquakes, floods, and other natural disasters. Cyber attacks on power systems are considered HILP disturbances [10] due to their disruptive impact and complexity. Therefore, their effects on power system resilience must be analysed.

The resilience of power systems is often expressed through the resilience triangle [8]. The triangle is formed by taking an indicator of power system performance over time, $Q(t)$, degraded by a disturbance at t_1, followed by a slope of system restoration back to a stable state (t_2), as represented in Figure 1. The graphical representation can also be extended by relative stable phases in degraded states and different restoration phases, forming a resilience trapezoid [11]. The relative stable phases form a critical part of resilience engineering theory. Four phases are foundational to power system resilience engineering [10]:

1. Anticipate: system weaknesses are identified, making the necessary preparations for disturbances based on their likelihood and impact. In available power system resilience literature, this often entails hardening principles and weather prediction models.
2. Absorb: the system withstands the initial brunt of the disturbance, limiting its negative effect on system performance, e.g., through line switching.

3. Recover: the system is recovered to a pre-disturbance state. In power system resilience research two separate topics are addressed. The first deals with load restoration and generation capacity maximization. The second addresses the physical repairs to the infrastructure using e.g. resource allocation.
4. Adapt: system operators learn from the disturbance and use the experience to improve system resilience. In power system resilience, this entails revisiting long term planning strategies, line switching strategies, resource allocation plans, and modelling approaches.



5.

6. *Figure 1: The resilience triangle*

Current research mainly focuses on extreme weather-related HILP disturbances, which can be physically identified. However, cyber attacks on EV charging infrastructures can be stealthy and remain undetected for a long period. Therefore, a fifth phase is added for cyber resilience, i.e., identify [10]. Intrusion detection and prevention is at the core of the identify phase.

2.2 EV Charging Infrastructure

Figure 2 represents an overview of the EV charging infrastructure, which is a complex system of physical assets, stakeholders, and ICTs. The infrastructure is an example of a cyber-physical system. In the top of the figure the physical part is shown. It comprises the transmission and distribution grid, with the CPs connected to the Low Voltage (LV) distribution network. In the bottom part, the cyber system is shown, with different ICTs operated by different stakeholders. The cyber system covers both operational and administrative functions.

Cyber attacks may focus on controlling CPs' charging power. There are four points in the system that attackers may target:

1) EV has the ability to start, stop or slow down the charging. It also plays a role in future Vehicle to Grid (V2G) technologies.
2) Communication protocols contain the measurements and setpoints that control the EV charging at a CP, e.g., OCPP and Open Smart Charging Protocol (OSCP).
3) Back offices of CPOs, where large aggregations of CPs can be controlled simultaneously.
4) Flexibility services such as frequency containment and congestion management. They are contracted by a system operator from Balancing Service Providers (BSPs). An attacker may penetrate either side to disrupt the flexibility operation.

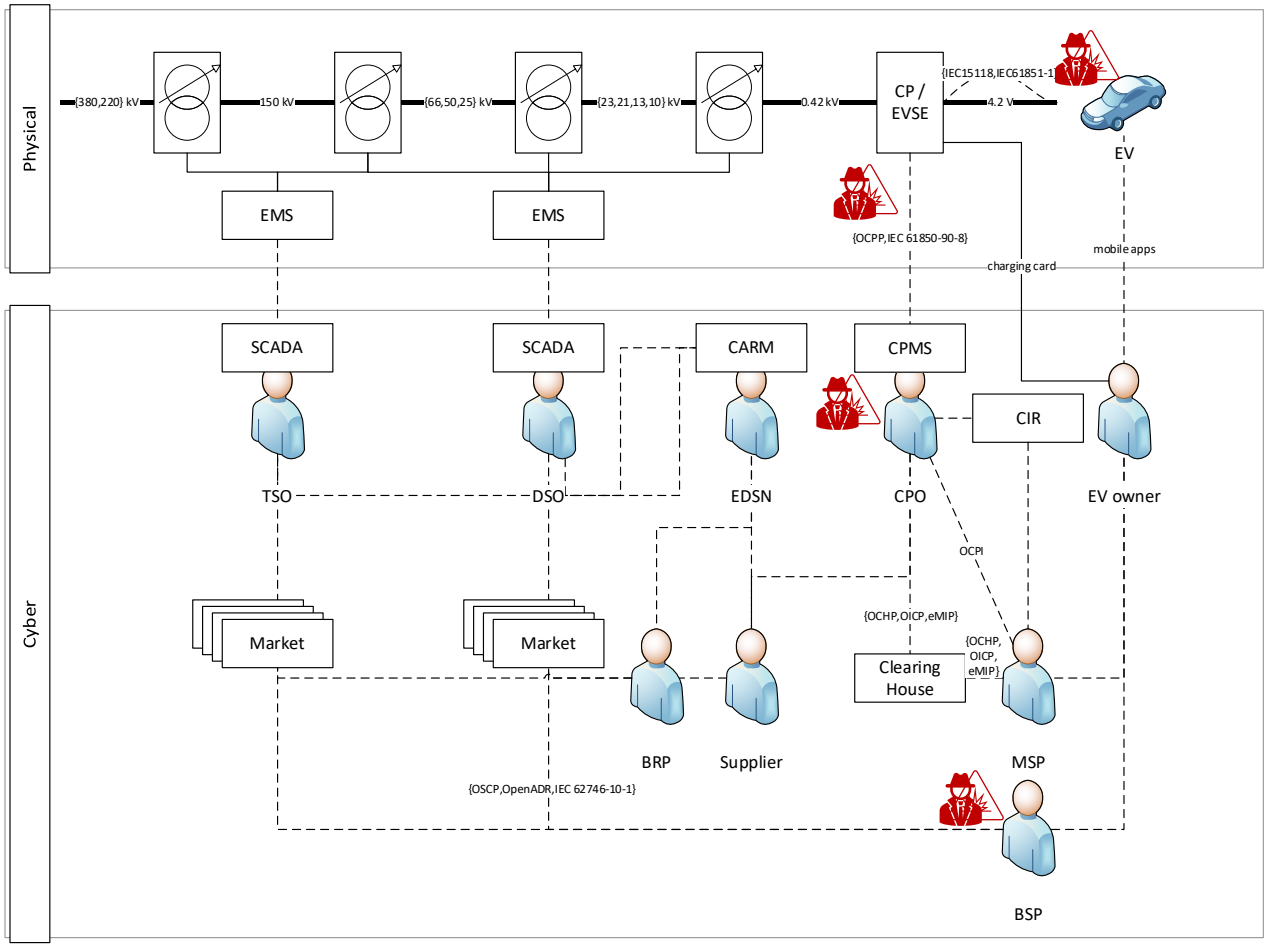


Figure 2: Overview of an EV charging infrastructure

2.3 Cyber Attack Scenarios

2.3.1 Attacks on Physical EV and Charging Points

A critical attack vector is the spread of malware through charging infrastructure by means of the EVs themselves [12]. EVs may be infected through physical tampering with the EV, corrupting internal components, or by an already infected charging point. Subsequent malware infections would then be achieved as EV drivers use different CPs to charge their vehicles. The infection would spread following a reproduction number *R*. It is probable that the attack would originate from a public CP, as it most accessible by the attackers. Nonetheless, it may spread to private charging networks through semi-public charging locations such as workplaces. Considering that most EV drivers tend to visit a limited number of different CPs, the attack may take a considerate time to accumulate a sufficient attack surface. Nevertheless, the attack surface may grow beyond any one stakeholder's influence, asking for complex coordination for attack mitigation. Additionally, it is possible that this surface may function as an gateway to other attacks.

2.3.2 Attacks on Flexibility Services

Flexibility in power systems was introduced and increased by two major developments:

1) The shift to renewable energy generation introduced a highly weather-dependent and thus intermittent power supply.

2) The electrification of our society causes load to exceed the power grid capacity. Increasingly, grid operators can no longer facilitate this rapid expansion.

Flexibility is described as shifting consumption and/or generation in order to optimally use the grid capacity. In modern energy systems, flexibility is bilaterally contracted by a Distribution or Transmission System Operator (DSO or TSO) from BSPs that may aggregate multiple sources of flexibility. Both sides are susceptible to cyber attacks, which may affect the flexibility schemes using, amongst others, EVs [4], [13]. Furthermore, the insider threats increase the attack risks for a DSO/TSO or BSP . Other risks may include social engineering and (spear) phishing attacks. The attack surface may affect all contracted assets of the BSP, i.e., EVs and CPs. Upon a successful intrusion, an attacker may broadcast malicious flexibility bids or asks.

2.3.3 Attacks on Charging Point Operation

The majority of charging points are operated and maintained by CPOs. Charging point operators use IoT and cloud applications to control CPs in bulk. As a result, CPOs may become a prominent target for cyber attacks. Through a single point of entry an immense attack could be launched, resulting in a significant impact on the power grid [13].

In the Netherlands, the public charging networks in cities are tendered to a single CPO. Combined with the private chargers, the attack surface may spread over the entire power grid. As a result, the cyber resilience is a joint-responsibility of a large number of stakeholders.

2.3.4 Attacks Exploiting Protocol Vulnerabilities

The "doomsday" scenario is described as the exploitation of a vulnerability in commonly used charging protocols, e.g., OCPP, OCPI or OSCP. Alcaraz et al. discuss the vulnerabilities of an older version of OCPP [5]. Although they were patched in recent OCPP versions, vulnerabilities in various charging protocols exist. Thus, a protocol-level attack can never be ruled out from a cyber resilience standpoint. Considering the high adoption of interoperable charging protocols in combination with future adoption of EVs, this attack vector may lead to cyber attacks on a continental scale.

2.3.5 Attack Objectives

The attack vectors may be exploited to maliciously control connected EVs and disrupt the power grid. Such attacks may be:

1) Coordinated attacks turning on or shutting off the CPs, especially at peak hours for power consumption and/or generation.
2) Cyclic attacks by switching the charging states on and off with a high frequency.
3) Intelligent attacks using market knowledge, such as inverse actions to flexibility asks or bids, e.g., charging at a moment when smart charging is offered.

3 Modelling the Stochastic EV Charging Behaviour

A new method is proposed to (i) model the stochastic EV charging behaviour using different (semi-)public data sources, (ii) simulate cyber attacks on EV charging infrastructure, and (iii) assess their impact on distribution system operation. Algorithm 1 presents the pseudocode of the proposed method, which uses an iterative approach to generate the average EV load profiles based on different Probability Density Functions (PDFs). Chance experiments are conducted using Bernoulli trial draws.

The algorithm is initialized with the simulation times, preparing the power grid model and generating class instantiations based on the selected power grid and its components, e.g., loads. It also includes assigning a charging power and type to CPs through Bernoulli trial. Power flow analysis is conducted to find initial conditions

and determine a base load situation. For each iteration, a new load profile is computed by considering all time steps and performing Bernoulli trials for EV arrival, energy demand, and connection time. Based on the outcomes of the trials, an EV is either charging at the respective CP or otherwise, resulting in a total load originating from CPs in the network. The total load is the decisive factor for the size of the attack vector, i.e., the amount of controllable load by a potential attacker. Considering the cyber attack scenario, the load from the EV charging infrastructure is maliciously modified and a new power flow analysis is conducted. The impact of the attack is assessed by comparing line loading and voltage levels simulation results to the base load.

Algorithm 1 Method to Assess the Impact of Cyber Attacks on EVs

```
Data: PDF of arrival times, connection times, energy demand and charging power, number of charging points
per year per area, simulation time, timestep size, number of iterations, grid topology.
Result: average EV charging load profile on transformer level
initialization;
power flow analysis;
for each i in iterations do
        for each loads in loads do
                for each timestep in simulation time do
                        for each charge point in transformer charge points do
                                if occupied then
                                        if timestep = departure timestep then
                                                charging = false;
                                                occupied = false;
                                        if timestep = idle timestep then
                                                charging = false;
                                        if timestep < idle timestep then
                                                load += charge point outlet power;
                                else
                                        draw from arrival times PDF;
                                        if EV arrives then
                                                departure timestep = draw from connection times PDF;
                                                idle timestep = draw from energy demand PDF;
                                                load += charge point outlet power;
simulate cyber attack;
power flow analysis;
comparison of line loading and voltage levels;
```

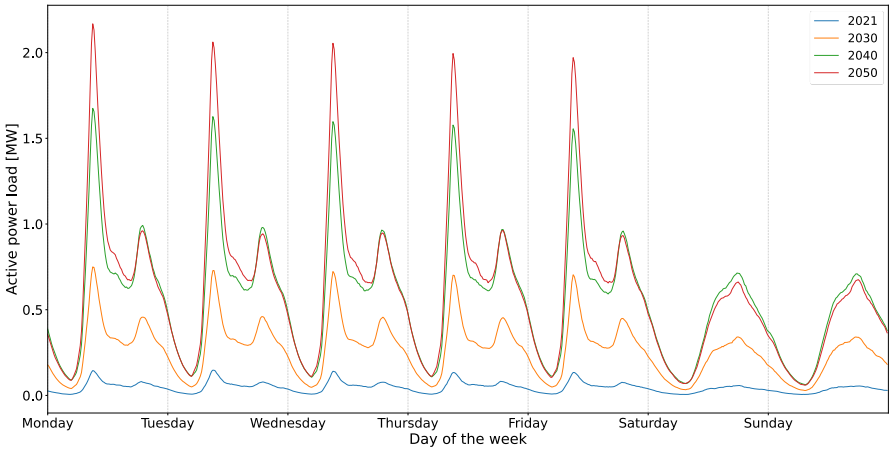


Figure 3: A week of generated EV load profiles for different scenarios

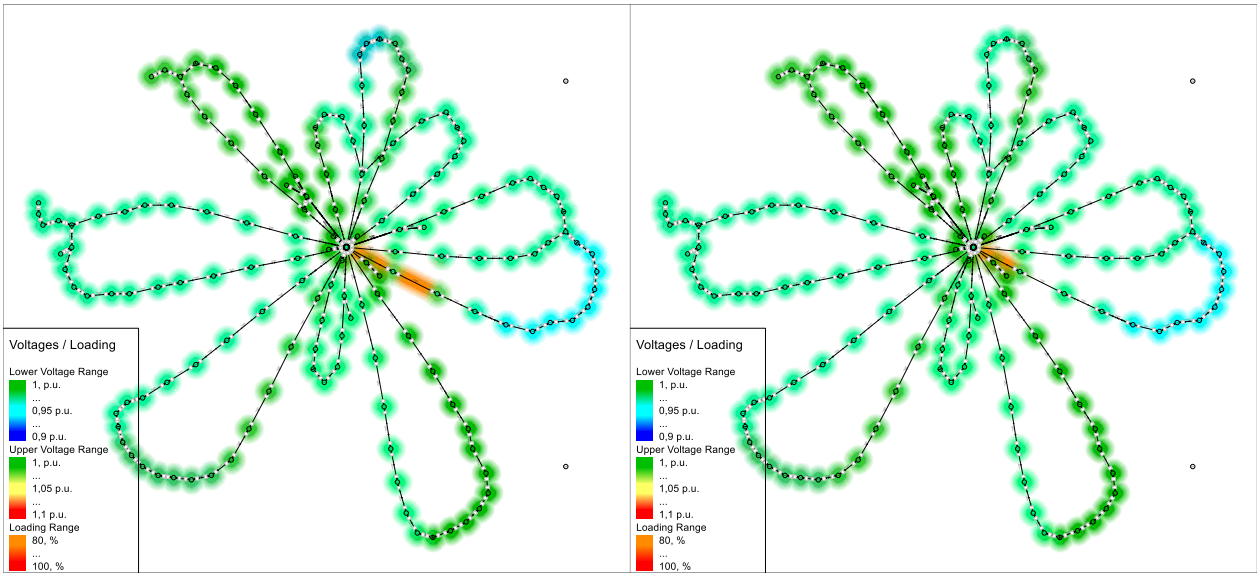
4 Simulation Results

A part of the Medium Voltage (MV) distribution network of a large city in the Netherlands is simulated using DIgSILENT PowerFactory. The distribution network model and data are provided by a Dutch DSO. The probability density functions are adopted from [14]. The number of charging points per area is based on [1]. The simulation time is set to one year, divided into 15 minute intervals. Experiments are repeated for 100 iterations to limit statistical bias and increase representativeness.

The cyber attack scenario is exploiting the CP protocol vulnerabilities. As a result, an attacker gains the ability to control the charging state of all charging points in the simulation.

Quasi-dynamic simulations are conducted to assess the impact of the cyber attack on long periods, i.e., one year for different future scenarios. Given the 15 minutes granularity, cyclic attack scenarios – requiring sub-second dynamic simulations – are not simulated. Moreover, considering the current technology, with limited adoption of V2G and flexibility schemes, the intelligent attack types are outside of scope. Therefore, periodic shutting down of large aggregations of charging points was simulated, i.e., monthly. Figure 3 shows an example for one week of modelled EV charging load on one MV/LV transformer in 2021, 2030, 2040, and 2050. Considering the morning peak, the example features an aggregation of primarily work-related charging points.

Power flow analysis is conducted in DIgSILENT PowerFactory. The impact of cyber attacks is analysed by monitoring the bus voltage magnitudes and line loading. In general, the effects of dropped loads on the MV network are insignificant. In fact, the cyber attacks slightly benefit the operating conditions. Figure 4 represents the single line diagram of the simulated distribution system. The centre node represents the High Voltage (HV) to MV transformer. Each “petal” of the flow represents a radially operated MV ring, where each link represents an underground cable and each node a MV/LV distribution transformer. The LV feeders are not simulated. A heatmap overlay is shown, where the overloaded lines are represented in yellow-red and bus undervoltages are represented with green-blue nodes.



a. *b.*

Figure 4: Graphical representation of the MV network in 2030 with voltages and line loading for (a) the base scenario and (b) cyber attack scenario

Figure 4.a and 4.b, show that the line overloading is decreased and undervoltages are prevented when a cyber attack is conducted. This is due to the nature of the MV distribution network, i.e., voltage drops further along the

cable. As a result, the sudden load shedding of the cyber attack mitigates undervoltages and line overloadings. In conclusion, the impact of this cyber attack will most likely not have a significant effect on the MV networks in the Netherlands.

However, in the advent of increasing adoption of V2G and flexibility schemes, actors gain access to new attack surfaces. Most importantly, the ability to not only maliciously decrease load, but also ramp up and even cyclically shifting charging states. Moreover, the number of CPs in this MV network represents less than 0.5% of the total EV charging infrastructure As presented in Table 1, extrapolated to the rest of the Netherlands and aggregated to the level of transmission power grid, where synchronous generators are connected, we expect a more dynamic system response to a potential cyber attack. Large amounts of maliciously controlled loads may lead to frequency instability, disruption of national energy markets, and potential continental blackouts [13].

Table 1: Maximum simultaneous EV load in simulated power grid and extrapolated (based on [1]*) to The Netherlands*

Year	Simulated grid load [MW]	Extrapolated load [GW]
2021	~1.0	~0.2
2030	~4,7	~1.0
2040	~9,2	~2.3
2050	~12,3	~2.9

5 Discussion on the Legal Framework in the European Union

Maliciously controlled loads may significantly impact the electric power distribution networks, transmission power systems, regions, or even countries. Therefore, we emphasize the importance of European Union (EU) Member States' preparedness. A European vision and strategy are needed to ensure embedded cooperation and exchange of information among all of the Member States. It is not clear under the current legislative framework if the charging infrastructure stakeholders are identified as operators of essential services.

In the past few years, many Regulations and Directives relevant for charging infrastructures in the EU were reviewed and updated, i.e., Alternative Fuel Infrastructure Regulation (AFIR), European Performance of Buildings Directive (EPBD), Directive on the security of Network and Information Systems (NIS Directive), future Directive on measures for high common level of cyber security across the Union (NIS 2), and Radio Equipment Directive (RED). It is obvious that the development of a legal framework for EV charging infrastructures in the EU is fragmented. This leaves the risk that new vulnerabilities are not properly covered by new legislation. For example, OCPP has to be improved to strengthen the supply chain cyber security for key ICTs. OCPP is *de facto* the world standard for charging electric vehicles. However, OCPP is not recognised in the new AFIR. Cyber security and resilience measures in European regulation may be less effective if the European Commission does not recognise standards and widely adopted protocols. The NIS Directive provides legal measures to boost the overall level of cyber security in the EU. However, it is not clear how the NIS directive covers cyber resilience and which safeguards will guarantee quick restoration following a cyber attack. Furthermore, it is uncertain how cyber security and resilience will be addressed in the broader legal framework.

The European Cyber Resilience Act (ECRA) may clarify such issues. ECRA will be announced in the second half of 2022. The act will ensure common European standards for cyber security of products and services on the European market. It will complement the Delegated Regulation of 29 October 2021 under the Radio Equipment Directive. Ideally, this would protect a wide range of digital products and associated services, covering tangible

digital products, wireless and wired, as well as non-embedded software. It will also define the governance of Computer Security Incident Response Teams (CSIRTs) and a competent national NIS authority. However, it is not yet clear whether EV charging infrastructures are considered essential services and fall under ECRA. Therefore, we encourage an open dialogue for a shared vision on cyber security regulation and governance of EV charging infrastructures.

6 Conclusion

In this paper, we define cyber resilience of power systems and discuss cyber attack scenarios on EV charging infrastructures. A method is proposed to assess the impact of cyber attacks on EVs considering their stochastic charging behaviour. Quasi-dynamic simulations are conducted on a part of the MV distribution network in The Netherlands. We show that the Dutch distribution network is cyber resilient to the investigated cyber attack scenario. However, this may change with future developments under different scenarios of the energy transition. As technology advances, new cyber attack scenarios become possible, which may lead to threats to power system stability, and cause significant operational issues. Therefore, we emphasise the necessity for a paradigm shift to cyber secure EV charging infrastructures and discuss the need for a stronger legislative framework in the European Union.

References

[1] N. Refa, D. Hammer, and J. van Rookhuijzen, "Elektrisch rijden in stroomversnelling; Elektrificatie van personenauto's tot 2050," Arnhem, 2021. [Online]. Available: https://www.elaad.nl/uploads/files/2021Q3_Elaad_Outlook_Personenautos_2050.pdf.

[2] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020, doi: 10.1109/ACCESS.2020.3041074.

[3] A. Chandwani, S. Dey, and A. Mallik, "Cybersecurity of Onboard Charging Systems for Electric Vehicles - Review, Challenges and Countermeasures," *IEEE Access*, vol. 8, pp. 226982–226998, 2020, doi: 10.1109/ACCESS.2020.3045367.

[4] M. E. Kabir, M. Ghafouri, B. Moussa, and C. Assi, "A Two-Stage Protection Method for Detection and Mitigation of Coordinated EVSE Switching Attacks," *IEEE Trans. Smart Grid*, 2021, doi: 10.1109/TSG.2021.3083696.

[5] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017, doi: 10.1109/TSG.2017.2669647.

[6] C. S. Holling, "Resilience and Stability of Ecological Systems," *Annu. Rev. Ecol. Syst.*, vol. 4, no. 1, pp. 1–23, 1973, doi: 10.1146/annurev.es.04.110173.000245.

[7] C. S. Holling, "Engineering resilience versus ecological resilience," in *Engineering Within Ecological Constraints*, Washington, D.C.: National Academies Press, 1996, pp. 31–44.

[8] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016, doi: 10.1016/j.ress.2015.08.006.

[9] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power System Resilience to Extreme Weather: Fragility Modeling, Probabilistic Impact Assessment, and Adaptation Measures," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3747–3757, 2017, doi: 10.1109/TPWRS.2016.2641463.

[10] K. Hausken, "Cyber resilience in firms, organizations and societies," *Internet of Things*, vol. 11, p. 100204, 2020, doi: 10.1016/j.iot.2020.100204.

[11] M. Panteli, P. Mancarella, and S. Member, "Modelling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1733–1742, 2015.

[12] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6160–6169, 2018, doi: 10.1109/TSG.2017.2705188.

[13] ElaadNL and European Network for Cyber Security, "Security risk assessment for electric vehicle charging infrastructure," 2019. [Online]. Available: https://encs.eu/documents.

[14] ElaadNL, "ElaadNL Open Datasets for Electric Mobility Research | Update April 2020," 2020. https://platform.elaad.io/analyses/index.php?url=ElaadNL_opendata.php (accessed Jan. 24, 2022).

Authors

Sjors Hijgenaar is an Industrial PhD candidate working at grid operator Stedin in collaboration with the Intelligent Electrical Power Grids group of Delft University of Technology. His research and work as grid strategist focusses on the resilience of power grids against cyber attacks on EV charging infrastructure.

Baerte de Brey works at Stedin, a Dutch DSO on e-mobility, and is the Chief International Officer within ElaadNL. Responsible for analyzing the long-term effect of electric mobility on the electricity grids, Baerte helps building a sustainable business case around this transition. This includes V2G, EV-storage and cyber security. He graduated from Leiden University in 2001 with a law degree and received a MBA from Nyenrode Business University in 2006. On behalf of Stedin, he is one of the executive board members of ElaadNL, the knowledge and innovation centre in the field of (smart) charging infrastructure. As an expert for the European Commission he sometimes reviews collective European programs concerning EV interoperability and smart charging. In his spare time he is an elected member of the Provincial Council of Utrecht.

Alexandru Stefanov is Assistant Professor of Intelligent Electrical Power Grids and Technical Director of the Control Room of the Future (CRoF) technology centre at TU Delft, The Netherlands. His research interests are cyber security for power grids, resilience of cyber-physical systems, and next generation grid operation. He holds the professional title of Chartered Engineer from Engineers Ireland.

Peter Palensky is full Professor for intelligent electric power grids at TU Delft, Faculty for Electrical Engineering, Mathematics and Computer Science, Netherlands, since 2014, working on mastering the complexity of smart, sustainable and flexible electric power systems. He also serves as Scientific Director of TU Delft's PowerWeb institute, a cross-faculty think tank for integrated and intelligent energy systems, and as Principle Investigator at the Amsterdam Metropolitain Solutions (AMS) institute. He is past Editor-in-Chief of the IEEE Industrial Electronics Magazine and associate editor for several other IEEE journals. He is financial advisor and AdCom member-at-large of the IEEE Industrial Electronics Society.

List of Abbreviations

AFIR	Alternative Fuel Infrastructure Regulation
BRP	Balance Responsible Party
BSP	Balancing Service Provider
CAN	Control Area Network
CARM	Central Allocation Reconciliation and Meter data
CIR	Central Interoperability Register
CP	Charge Point
CPMS	CP Management System
CPO	CP Operator
CSIRT	Computer Security Incident Response Team
ECRA	European Cyber Resilience Act
EDSN	Energy Data Services Netherlands
eMIP	eMobility Interoperation Protocol
EMS	Energy Management System
ENISA	European Union Agency for Cybersecurity
EPBD	European Performance of Buildings Directive
EU	European Union
EV	Electric Vehicle
EVSE	EV Supply Equipment
HILP	High Impact Low Probability
HV	High Voltage
ICT	Information and Communication Technology
IoT	Internet of Things
LV	Low Voltage
MitM	Man-in-the-Middle
MSP	Mobility Service Provider
MV	Medium Voltage
NIS	Network and Information Systems
OCHP	Open Clearing House Protocol
OCPI	Open CP Interface
OCPP	Open Charge Point Protocol
OICP	Open InterCharge Protocol
OpenADR	Open Automated Demand Response
OSCP	Open Smart Charging Protocol
PDF	Probability Density Function
RED	Radio Equipment Directive
SCADA	Supervisory Control And Data Acquisition
TSO/DSO	Transmission/Distribution System Operator
V2G	Vehicle to Grid