Cyber Resilience of Electric Vehicle Charging in Smart Grids the Dutch Case

Hijgenaar, Sjors; Stefanov, Alexandru; Van Voorden, Arjan M.; Palensky, Peter

DOI
10.1109/ACCESS.2025.3580856

Publication date
2025

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 1 May 2025, accepted 20 May 2025, date of publication 18 June 2025, date of current version 3 July 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3580856

SURVEY

Cyber Resilience of Electric Vehicle Charging in Smart Grids: The Dutch Case

SJORS HIJGENAAR[1,2], (Student Member, IEEE), ALEXANDRU ŞTEFANOV[2], (Member, IEEE), ARJAN M. VAN VOORDEN[1,2], AND PETER PALENSKY[2], (Senior Member, IEEE)
[1]Stedin Netbeheer B.V., 3000 AA Rotterdam, The Netherlands
[2]Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands

Corresponding author: Sjors Hijgenaar (sjors.hijgenaar@stedin.net)

This work was supported by Stedin Netbeheer B.V., and the ROBUST Project through the Missiegedreven Onderzoek, Ontwikkeling en Innovatie (MOOI) Subsidy Program by The Netherlands Ministry of Economic Affairs and Climate Policy and the Ministry of the Interior and Kingdom Relations, executed by The Netherlands Enterprise Agency.

ABSTRACT As a part of energy transition, the shift from internal combustion engines (ICEs) to electric vehicles (EVs) has accelerated the development of the EV charging infrastructure (EVCI). EVCI rely heavily on information and communication technologies (ICTs) and the Internet of Things (IoT). As a result, the susceptibility to cyber attacks increases. However, although EVCI are strongly intertwined with cyber-physical power systems (CPPSs), the consequences of such a cyber attack on the power grid are not widely researched. In this paper, we present a comprehensive cyber-physical system architecture of the EV charging infrastructure based on the industry practice in The Netherlands, which is applicable to European distribution systems. We present a survey of work on EVCI cyber security and CPPS resilience. We combine unique industrial insights with the academic state-of-the-art. We show that although cyber security of EVCI is researched, the state-of-the-art inadequately covers the consequences for CPPSs, especially distribution networks. We survey the current work on CPPS resilience and conclude that while cyber attacks are often recognized as high impact low probability (HILP) disturbances of CPPSs, the resilience-related research on cyber attacks on EVCI is lacking. Therefore, we present a novel method to model the stochastic EV charging behaviour based on probability density functions (PDFs). We validate the method using PowerFactory models of distribution networks supplied by a Dutch distribution system operator (DSO). We demonstrate the effects of cyber attacks on EVCI on distribution networks voltages. Under the investigated operational scenario, the impact is not significant. However the results do underline the importance of researching cyber attacks on EVCI from a CPPS resilience perspective. Research into future scenarios of energy transition is essential for future resilient operation of power grids.

INDEX TERMS Electric vehicle charging, power distribution networks, cyber security, resilience.

I. INTRODUCTION

Energy transition is a radical shift in the paradigm of power generation and usage, shifting from fossil fuel-based to renewables in order to limit the enhanced greenhouse effect. Several sectors contribute significantly to greenhouse gas (GHG) emissions, consequently warming up of the planet, and transportation is an important example. Thus, electric mobility is being adopted at an accelerating rate for its clean propulsion [1]. However, while being beneficial for the environment, a household's load can easily be doubled by an electric vehicle (EV) and their collective impact on power systems can be vast.

EVs and their impact on power grids is, amongst others, researched in the context of cyber security of smart grids [2]. As a complex network of stakeholders and systems is required to operate EV charging infrastructure (EVCI), a strong dependency on information and communication technologies (ICTs) and the Internet of Things (IoT) is apparent. The operation of charge points (CPs) and administration of

The associate editor coordinating the review of this manuscript and approving it for publication was Elizete Maria Lourenco.

charging transactions is but a small part of the extensive task list of EVCI. It is widely recognised that ICTs and the IoT are susceptible to cyber attacks [3], [4]. Moreover, the close coupling of ICTs and operation of CPs, and the direct connection between EVCI and power systems have thinned the line between information and operational technology (IT, respectively OT). As a result, cyber attacks may not only impact digital systems, but also have consequences for the physical world [5]. Therefore, cyber security research should focus on the analysis of the entire cyber-physical system (CPS).

For instance, vulnerabilities of EV systems, including charging infrastructure are presented in [2]. A cyber attack on an American EVCI leading to power grid instabilities has been shown in [6] by Acharya et al. As an extension to EVCI, internal components of EVs are also at risk, as demonstrated in [7] and [8]. How cyber attacks may spread through EVCI is shown in [9]. Finally, vulnerabilities of ICTs used in EVCI are highlighted in [10] and [11].

Possible mitigations of the risk of cyber attacks in EVCI are also proposed in literature. However, as no system can be perfectly safe, research also needs to focus on cyber resilience. There appears to be no clear consensus on the definition of (cyber) resilience of power systems [12], but most definitions include the ability of the system to withstand high impact low probability (HILP) disturbances and quickly return to a stable state of operation afterwards.

A. RESEARCH OBJECTIVE

Cyber security and resilience research in EVCI should be two sides of the same coin. Whereas, the interconnected CPS should have an integral focus on cyber-securing systems. Thus, minimizing the potential for a successful cyber attack on its subsystems. However, residual risks and the worst-case scenario of a successful cyber attack have to be included in power grid planning procedures. Especially in the advent of widespread integration of EVCI and power CPSs (CPPSs).

Therefore, a survey on the combinations of these two topics is presented in this work. To the best of our knowledge this combination has not yet been presented in literature. The state-of-the-art of cyber security of EVCI, looking at vulnerabilities and attack scenarios, is investigated. Furthermore, the available body of work on power and distribution system resilience is surveyed. An overview of definitions, metrics and improvement strategies is presented. Finally the two topics are combined to address the impact of cyber attacks in EVCI on distribution systems.

The specific focus of this work is on distribution systems. However, as was found that the bulk of work is on transmission systems, literature search was extended to power systems. To perform the literature survey presented in this work, literature was found through IEEE Xplore and Scopus. Search terms are presented in Table 1. A very strong preference was given to papers presented in journals.

II. RELATED WORK

In order to manage increasingly complex power systems, digitization has received significant attention in both academia and industry. With the emergence and growing adoption of electric mobility this has resulted in more research on cyber security in EVCI. On the other hand, resilience of power systems is most often researched in the context of extreme weather conditions, or, in the case of cyber resilience, cyber attacks on power system components. Table 2 gives an overview of the six topics chosen for the literature survey in this work. These topics were selected to cover the two main themes – EVCI cyber security and CPPS resilience – in its entirety.

1) **Vulnerabilities** covers the exploitable components in EVCI physical and digital systems, ranging from internal EV components, physic CPs and charging locations, CP management systems (CPMSs) and EVCI ICT, IoT and protocols.
2) **Cyber attack scenarios** deal with how the vulnerabilities of topic 1 might be exploited to conduct cyber attacks. This category addresses where the cyber attack originates from and what proportion of EVCI may be affected.
3) **Impact analysis** comprises the consequences of cyber attack scenarios on EVCI for distribution networks, including methods for modelling and mitigation.
4) **Modelling** of CPPS includes metrics and methods for modelling, quantifying and simulating resilience of distribution systems.
5) The **enhancing** category covers literature on different methods for improving the resilience of distribution systems against different HILP disturbances.
6) Finally, **cyber** resilience addresses power system resilience with cyber attacks as HILP events specifically.

Several surveys of literature in these categories can be found through the search terms found in Table 1.

The authors in [2] present an overview of EVCI physical and digital systems. They present different vulnerabilities and how they may lead to cyber attacks targeting the operational stability of power systems. In their work they highlight the potential effect to power system resilience, but do not dive into particular details of the topic. Reference [7] focusses on onboard components and how vulnerabilities in EV internal systems may be abused by cyber attackers. However, other subsystems of EVCI are not discussed, nor the potential impact on power systems. In [14] the Open Charge Point Protocol (OCPP) is of specific interest. Vulnerabilities and cyber security measures are presented. While OCPP is an extensively used protocol in EVCI worldwide, the survey includes limited insights in components of EVCI beyond protocols or the effects on power systems. Sayed et al. present a comprehensive overview of vulnerabilities in EVCI CPSs in [15]. They formulate potential cyber attacks that may affect power grid operational stability, presenting a case study

TABLE 1. Literature survey search terms.

Category	Query
Cyber security of EVCI	("electric vehicle" OR "EV" OR "EVS" OR "PEV" OR "PEVS" OR "BEV" OR "BEVS") AND ("cyber security" OR "cybersecurity" OR "cyber attack" OR "cyberattack")
Resilience of power systems	"resilience" AND (("power distribution" OR "power" OR "smart") AND ("grid" OR "system" OR "network"))

that looks at the potential effects on voltage and frequency stability. While the stability part of resilience is included in the overview, post-disturbance performance of the power system is not. A comprehensive analysis of vulnerabilities in EVCI is presented in [16]. The authors use the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege (STRIDE) threat model to identify the risks, focussing on the first step of the resilience: anticipate. The following steps – identify, absorb, adapt and recover – are not discussed in detail. In [17] a review of digital systems of EVCI and their vulnerabilities is presented. The work doesn't cover other components, nor how vulnerabilities may lead to cyber attacks and the consequences on power system resilience. The authors of [18] give an outlook on cyber security of DERs, of which EVs are an important example. They present vulnerabilities, attack scenarios, power system impact, and mitigations, but the specific focus on EVs is limited. Metrics for power system resilience are discussed, but not analysed in the light of cyber attacks on EV CPSs.

Several reviewing or surveying works on power system resilience have been published. Most often resilience of power systems is analysed under natural disasters [29], giving specific attention to evaluating, measuring or quantifying, and improving resilience [20], focusing on different time horizons [23] and different ways of formalizing evaluation models [24]. Fragility curves have received special attention as a way to quantify and forecast power system resilience [27] fragility curves. A technique for improving power system resilience that has received specific attention is networked microgrids (NMGs) [21], including distribution system resilience [22], energy storage [29], and even including EV scheduling as part of the enhancement strategy [22]. Finally, cyber resilience has significantly gained attention over the past years [19], [26]. In [25] EVCI are mentioned as the potential origin of cyber attacks.

Other works have presented methods for modelling EV charging behaviour. In [30] the authors model EV charging according to data obtained from the Alternative Fuels Data Center [31]. The authors assign a static peak charging power demand to each load bus in Manhattan, NY based on the number of chargers and distribution of cars. In [6] the same dataset is combined with usage patterns obtained by crawling the ChargePoint smartphone application. This results in average power consumption per CP type (Type 2 and 3, see Section III-B) per hour.

While the focus of this work is on the vulnerabilities in EVCI, the potential for cyber attacks in EVCI and eventual impact on power systems; the potential effects on internal EV power electronic components cannot be ignored. For more on that topic, the reader is directed to the excellent work of Ronanki and Karneddi [13].

A. CONTRIBUTIONS

Considering the previous sections, it can be concluded that EVCI pose significant risks for cyber attacks of which the impact on power systems might be vast. However, as cyber attacks should be considered as HILP disturbances, the body of work that combines EVCI cyber security and CPPS resilience is limited. This work aims to contribute to mitigating that research gap.

In this survey, the current state-of-the-art of EVCI cyber security is analysed. Secondly, resilience of power systems is investigated. We conclude that research on cyber resilience of power systems often focusses on cyber attacks originating from the power system components, not a sub-system such as EVCI. A recent example of this is presented in [32] where cyber resilience of EVCI is researched but the actual cyber attack is conducted on a busbar level. Additionally, distribution networks are under-represented in resilience research, while being the main connection point of EVCI. Therefore, we signal a research gap on the impact analysis of cyber attacks on EVCI on distribution systems. This paper contributes to addressing that gap. The specific contributions of this work are as follows:

- We present a comprehensive cyber-physical system architecture of EVCI based on the industry practice in The Netherlands, which is applicable to European distribution systems.
- A survey of EVCI-specific cyber vulnerabilities and attack scenarios, followed by a survey on definitions, metrics and modelling of (cyber-) resilience of power systems.
- A method to model stochastic EV charging behaviour is proposed. Probability density functions based on a large number of real charging sessions are used. Its novelty lies in realistic load profiles for individual CPs per location type: public, private and work. The method allows for running large numbers of scenarios. It is used to analyse the impact of EVCI cyber attacks on medium voltage (MV) distribution network operation.
- We present simulation results of a real Dutch MV distribution network to validate the method and underline the importance of the presented research topics.

The remainder of this paper is structured as follows. Section III describes the EVCI CPS. Section IV presents a survey on EV-related cyber security research. A survey on resilience

TABLE 2. Overview of related work, coverage of topics: red = low, orange = medium, green = high.

Ref	Vulnerabilities	Cyber attack scenarios	Impact analysis	Modelling	Enhancing	Cyber	Remarks
[2]	🟩	🟩	🟩	🟥	🟥	🟥	Comprehensive review of EVCI CPSs, attack scenarios and impact, from a mostly academic perspective.
[13]	🟩	🟩	🟧	🟥	🟥	🟥	Overview of EVCI from a mostly American perspective, cyber attack scenarios, mitigation techniques and future challenges, impact on grid is not presented.
[7]	🟧	🟧	🟥	🟥	🟥	🟥	Review of vulnerabilities in internal EV components, potential cyber attacks and consequences for the EV itself.
[14]	🟧	🟥	🟥	🟥	🟥	🟥	Survey on the vulnerabilities in the OCPP and cyber security measures proposed in literature.
[15]	🟩	🟩	🟩	🟥	🟥	🟥	Overview of vulnerabilities across EVCI and how they may affect the grid. Includes a case study on power grid stability.
[16]	🟩	🟩	🟥	🟥	🟧	🟥	Analysis of vulnerabilities in EVCI and a risk assessment framework.
[17]	🟧	🟥	🟥	🟥	🟥	🟥	Review of mostly cyber systems in EVCI and their vulnerabilities.
[18]	🟧	🟧	🟧	🟧	🟥	🟥	Outlook on DER cyber security, with remarks on EVs specifically, includes analysis of resilience metrics.
[19]	🟥	🟥	🟥	🟩	🟩	🟩	Critical review of power system resilience metrics, evaluation and enhancement.
[20]	🟥	🟥	🟥	🟩	🟩	🟥	Review of metrics and evaluation frameworks, and hardening strategies.
[21]	🟥	🟥	🟥	🟧	🟩	🟥	Review of using networked micrograids to improve power grid resilience.
[22]	🟥	🟥	🟧	🟧	🟩	🟥	Comprehensive review of using networked microgrids to improve distribution system resilience.
[23]	🟥	🟥	🟥	🟥	🟩	🟥	Review of methodologies to improve power system resilience, classified according to time horizon.
[24]	🟥	🟥	🟥	🟩	🟥	🟥	Analysis of works on conceptualization of power system resilience.
[25]	🟥	🟥	🟧	🟩	🟩	🟩	Survey on modelling and improving power system resilience under cyber attacks.
[26]	🟥	🟥	🟥	🟩	🟩	🟩	Overview of CPPS resilience definitions, assessment methods, and quantification.
[27]	🟥	🟥	🟥	🟩	🟥	🟥	Review of fragility curves used to quantify power system resilience.
[28]	🟥	🟥	🟥	🟧	🟩	🟥	Review of using energy storage as power system resilience enhancement.
[29]	🟥	🟥	🟥	🟩	🟩	🟥	Review of modelling impact to and improving of power system resilience under natural disasters.
This work	🟩	🟩	🟩	🟩	🟩	🟩	A comprehensive survey of cyber security in EVCI, including unique and valuable industrial insights, connected to the topic of power system resilience.

in power systems is presented in Section V. Section VI gives a method to model EV charging behaviour based on which simulation results for a Dutch MV distribution grid are given in Section VII. Finally, conclusions are given in Section VIII.

III. CYBER-PHYSICAL EV CHARGING INFRASTRUCTURE

EVCI is the interface between EVs and power systems. On the one hand, there is a physical connection between the EV supply equipment (EVSE) and power grids. On the other hand, ICT and the IoT are used for CP operation and administration of charging sessions. Therefore, EVCI are CPSs and should be analysed as such. This section gives an overview of EVCI based on extensive survey of both academic and industrial literatures [33], [34], [35], and [36], as well as grid design documents supplied by a Dutch DSO. An overview of this chapter is given in Figure 1.

A. STAKEHOLDERS AND ROLES

Below a summation of key stakeholders in EVCI is given:

- A physical connection between EV and CP is created by the **EV driver/owner**. **A**uthentication of the charging session for administrative functions is commonly done using a radio frequency identification (RFID) tag or near a field communication (NFC) card, swiping an authentication terminal on the CP.
- Asset management of the CP is conducted by **CP operators** (**CPOs**). Tasks include, amongst others, operation of the CP (including remote load control), firmware upgrades and maintenance. A CPO can also act as an aggregator (see below for a description).
- The necessary infrastructure for authenticating EV drivers is provided by **mobility service providers** (**MSPs**), contributing heavily to administrative functions.
- The physical connection between the CP and power grid is realised by a **grid operator**. **For example, in The Netherlands** the majority of CPs are connected directly to low voltage (LV) feeders. LV (0.23 or 0.4 kV), MV (10, 13, 21 or 23 kV) and high voltage (HV: 25, 50 or 66 kV) distribution grids are constructed, maintained and operated by **distribution grid operators** (**DGOs**). While transmission grids with voltages of 150, 220 or 380 kV fall under jurisdiction of the **transmission system operator** (**TSO**). TSOs are responsible for system balance and frequency stability. As a result of energy transition more intermittent renewable energy sources (RESs) are used, leading to more complex system to operate. distributed energy resources (DERs) are often employed to help in maintaining stable operation [37], [38]. As an example, EVs are increasingly employed for system services to maintain voltage stability and local energy balance. More specifically smart charging is contracted for congestion management in distribution networks (DNs) by DGOs. Consequently, grid operation no longer is the sole responsibility of the DGO, it is being expanded with system operation. Therefore, DGOs are increasingly becoming distribution **system** operators (**DSOs**).
- The administrative/financial functions of delivering electricity to the CP are performed by **suppliers**. They form the interface between customers (i.e. the CPO, MSP or EV owner) and the energy market. A strong connection exists between suppliers and **balance responsible parties** (**BRPs**) or wholesalers. Energy markets are formed by BRPs, whose bids and tenders are used to form energy prices on day-ahead, intraday and balancing markets. Bilateral, often long-term contracts are sometimes signed between BRPs and large consumers. Furthermore, BRPs have a legal obligation to prevent system imbalances and can be penalized by the TSO for violating energy bids or tenders.
- (Smart) metering data, for example CP metering data, is collected, stored and processed by **register operators** (**ROs**). Their administrative functions contribute to advanced metering infrastructure (AMI), asset data collection (ADC), identification and access management (IAM) and authentication, allocation, and reconciliation. A Dutch example is EnergieData Services Nederland (EDSN): a joint venture of the Dutch DSOs to centralise common data processing tasks.
- **Balancing service providers** (**BSPs**), commonly referred to as **aggregators**, combine flexible energy assets – such as EVs and other DERs – to offer system services to system operators. Congestion management to DSOs or frequency restoration – for example automatic or manual Frequency Restoration Response aFRR/mFRR – to TSOs are prime examples. An aggregator role is often fulfilled by other stakeholders such as CPOs, MSPs and suppliers.
- **Roaming service providers** (**RSPs**) operate clearing houses used to enable interoperability in EVCI. With the complex relationship of technology and stakeholders, the risk of vendor lock-in becomes apparent. An important pilar of EVCI is standardization. In combination with interoperability, it allows for the same infrastructure to be used by as many users and stakeholders as possible. Amongst others, this is done to allow users to use their own MSP-supplied charging card at CPs operated by other stakeholders. The latter is called roaming.

B. PHYSICAL SYSTEMS

The physical part of energy systems comprises the tangible assets required to transport electricity from generation to load. An overview of relevant physical systems to EVCI is given below:

- **Power grid**. Public CPs are primarily connected to LV feeders. Only high voltage direct current (HVDC) chargers and charging hubs are connected to the MV grid. LV feeders are operated radially and consist of 3-phase and one neutral copper or aluminium cables. For example, in The Netherlands, the capacity of CP connections is mostly $3 \times 25\text{A}$ at $400\,V \cong 17.5\,kW$. This is consistent with private chargers which are connected behind the meter, thus not directly to the power grid. Most household consumers have a 3 × 25A at 400V inbound connection and therefore a maximum 17.5 kW capacity. Like LV grids, MV distribution grids are

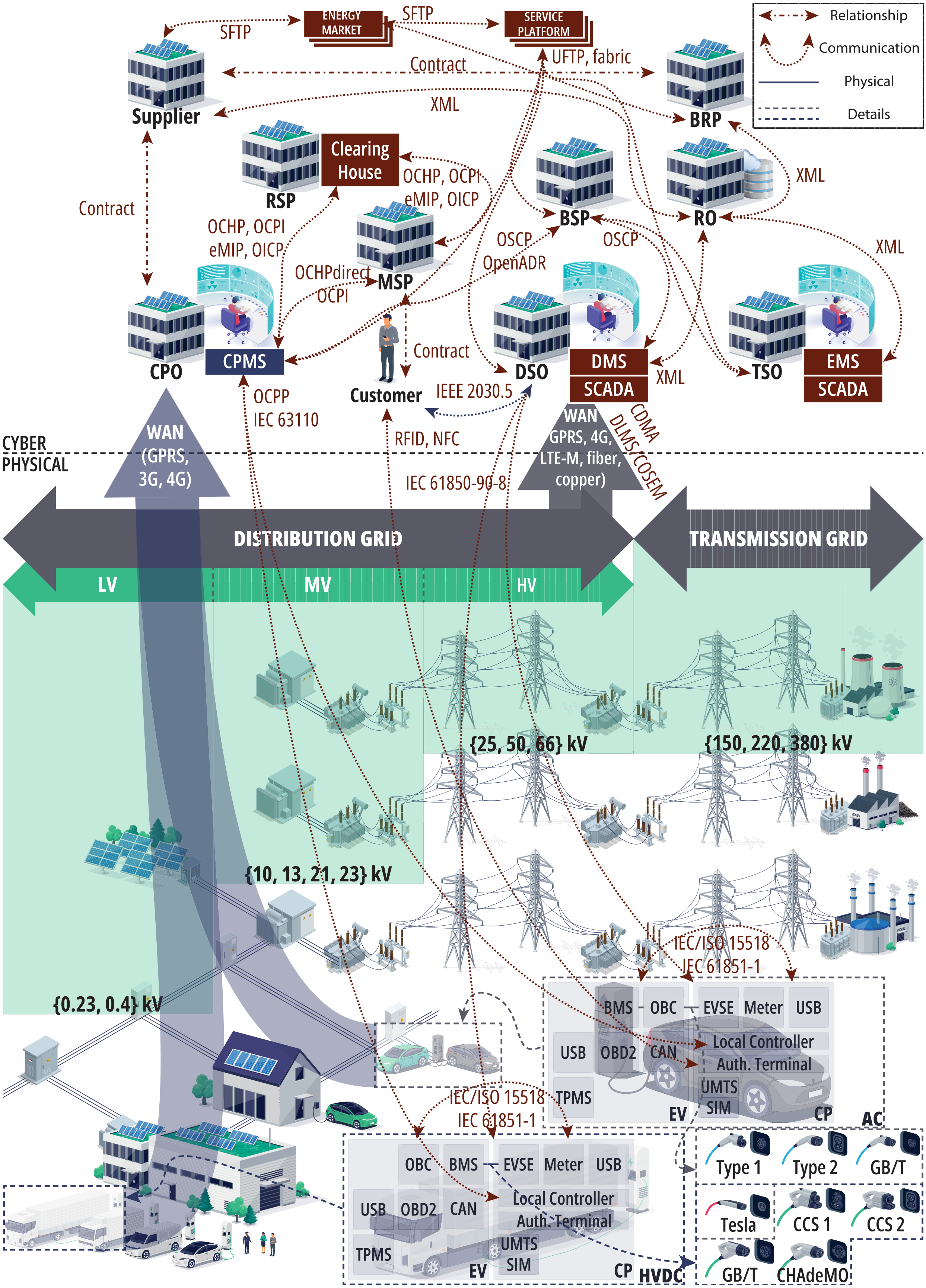


FIGURE 1. Cyber-physical system architecture of EVCI.

operated radially. Underground XLPE aluminium cables are used and vary in length between approximately 4 and 12 km with a nominal current of 275-640 A. Generally, this allows for approximately 10-30 MV/LV transformers with a nominal power rating of typically 400-600 kVA. MV and LV grids are designed to allow for a total voltage drop of 10% – combined over the HV/MV transformer, the MV feeder and entire connected LV grid. Lines in MV grids have a maximum loading of 60% of thermal limits. This is to ensure N-1 contingency reliability.

- **CPs** consist of AC or DC EVSE, a local controller, an authentication terminal, and an energy meter [39]. DC EVSE, used in fast chargers, have a fixed cable, whereas AC EVSE can only be used using an external cable brought with the EV. The former have seen the most developments over recent years, now with a capacity ranging from 50, to 175 and even 350 kW. The latter can commonly provide power over one or three phases, typically with 16 or 32 A, resulting in either 3.6 (Type 1 CPs, mostly typical household sockets), 11 or 22 kW (Type 2 CPs) charging capacity (where 11 kW is most often used, especially for public CPs). Up to 2 MW DC chargers (Type 3 CPs) have been developed, mostly for charging buses and trucks. Generally, OCPP is used by CPs to communicate with central back-office systems (see the following subsections) over wide area network (WAN). The WAN is predominantly accessed Iy installing a Universal Mobile Telecommunication Service (UMTS) module with a (locked) SIM card. Several standards have been developed for connecting EV to CP, for example: AC chargers Type 1, Type 2 and GB/T (AC); DC chargers CCS1, CCS2, GB/T (DC), and CHAdeMO. Tesla chargers offer both AC and DC charging.
- **Electric vehicles** have an onboard charger (OBC) with an invertor for charging from an AC EVSE. The OBC can charge using one, three, or occasionally two phases. Then, with, for instance, typical currents in The Netherlands per phase of 24 or 32 A, a 7.2, 11, 16.5 or 22 kW charging capacity is achieved. Together with the charging capacity of the CP, the actual charging power is determined by the weakest link. DC current is directly supplied to the onboard DC battery system (BMS). Internal components communicate over a Controller Area Network (CAN) bus [2]. The onboard diagnostics (OBD2, for version 2) make sure different components exchange the correct information to enable safe operation of the EV. The tire pressure monitoring system (TPMS) makes sure information about tire pressure values are given to the end user. The EV communicates with the CP/EVSE, either using the user-supplied or CP-connected charging cable, following the International Electrotechnical Commission / International Organisation for Standardisation (IEC/ISO) 15118 standard (see the following sections) or newly developed IEC61851-1. An USB port is available for maintenance and connecting end-user appliances.

C. CYBER SYSTEMS

EVCI rely on ICTs to operate. An overview of the most important ICTs and related communication protocols are given in the subsequent sections.

1) INFORMATION AND COMMUNICATION TECHNOLOGIES

- **Energy management systems** (**EMSs**) and **distribution management systems** (**DMSs**) are used by TSOs and DSOs respectively to operate the transmission, respectively distribution grid. They combine sensor readings and actuator states from **supervisory, control and data acquisition** (**SCADA**) systems with geospatial information system (GIS), market conditions, and state estimations to make informed decisions on how to best effectuate control mechanisms to keep the grid within safe and stable operational margins. Information from the grid is exchanged over public WAN, often GRPS, 4G or LTE-M, using CDMA or DLMS/COSEM protocol. A private connection is ensured through secured access point names (APNs). Communication over physical networks is often done through fiber optics or copper wiring.
- **Clearing houses** are responsible for administrative/ financial processing of charging sessions. They are used to identify the stakeholders and their digital systems [34]. Communication for financial transactions is also conducted through clearing houses.
- **Registers** are used amongst the stakeholders in EVCI to exchange asset and metering data. For example, **Central Allocation, Reconciliation and Metering data (CARM)** is the main system developed and maintained by EDSN. It is used to collect and exchange energy data between grid operators and market parties (mainly suppliers and BRPs). The data is necessary for administrative processes. Another example is the **Central Interoperability Register (CIR)**, which contains unique identifiers of EV owners managed by MSPs and CPOs. The identifiers are used by CPs to identify EV owners and authenticate charging sessions initiated by EV owners. EV owners initiate authentication by scanning for instance a charging card at the CP's authentication terminal [40].
- **A CP management system (CPMS)** is used by a CPO to remotely operate CPs. They receive information from CPs over GPRS, 3G, or 4G.
- **Markets**. Different markets are used in order to maintain a strict balance between supply and demand. This balance is crucial for frequency and voltage stability. Example markets are day-ahead, intraday, imbalance and ancillary services markets.' **Service platforms** may act as interfaces between stakeholders and markets to unlock system services. Service platform define means

of communication and allow exchange of information through application programming interfaces (APIs). Platforms then deal with relaying information to regular energy markets. This ensures system services provided do not create problems elsewhere in the grid. For instance, **GOPACS** is a congestion management platform specifically used in The Netherlands. Congestion is predicted by a DSO or TSO and put in the platform. BSPs can offer a congestion management service through two options 1) placing a buy order 2) adjusting load according to an agreed upon capacity limit contract (CLC). Buy orders always have to be combined with a sell order elsewhere to prevent national balancing issues. Market orders are conducted through connections to regular energy markets [41]. Messages on the platform are exchanged according to the Universal Smart Energy Framework (USEF) Flex Trading Protocol (UTFP) [42]. **Equigy** is an example of a platform used to connect BSPs with TSOs in Europe. The platform uses blockchain (Hyperledger fabric) to ensure non-repudiation of executed system services. Equigy enables using the aggregated flexibility of a large number of smaller DERs [43].

2) COMMUNICATION PROTOCOLS

Rademakers & Klapwijk give an overview of commonly used protocols and communication standards in [34]:

- The **Open Smart Charging Protocol (OSCP)** is designed to facilitate communication between an (DSO) EMS and a (CPO) CPMS, allowing for optimal charging based on 24-hour capacity forecasts. The protocol is maintained by the Open Charge Alliance and current adoption is expected to be low, due to few active implementations of smart charging [44], [45], [46].
- The **Open Automated Demand Response (OpenADR)** standard is used as a standard to communicate demand response (DR) messages between system operators, energy service providers and consumers. The standard, current version 2.0, features two profiles: "a" for information subscribing (or "Virtual End") nodes (VEN) and an extension, "b", for information publishing (or "Virtual Top") nodes (VTN). Considering the amount of applications world-wide utilising the standard, the adoption is considered highest amongst smart charging protocols [45], [47], [48]. OpenADR 2.0 is recognised as **IEC 62746-10-1** [2].
- **IEEE 2030.5** is a standard developed to communicate from DSO to end user for DR activities such as "load control, time of day pricing, distributed generation, EVs, etc." [49].
- **IEC 61850-90-8** defines a model for V2G communication, allowing EVs to be used as DERs as described **in IEC 61850-7-420** [50].
- The **Open Clearing House Protocol** (**OCHP**) offers a standard way of connecting MSPs and CPOs to clearing houses in order to enable roaming services, thus providing charging sessions at different CPOs from a single Customer-MSP contract. OCHPdirect is used to provide direct information exchange between MSP and CPO without requiring a RSP and clearing house [51], [52].
- The **Open Charge Point Interface** (**OCPI**) was designed for communication between CPOs and MSPs and facilitate roaming services through clearing houses. Moreover, it offers information about locations and prices of CPs to end users [52], [53],.
- The **eMobility Interoperation Protocol** (**eMIP**) was developed by GIREVE to enable roaming services, combining authentication and authorization over different MSPs and CPOs. In that regard it is similar to OCPI, OCHP and OICP, however does not share their open source character [52], [55].
- Interoperability and roaming services may also be achieved through **Open Intercharge Protocol** (**OICP**). The protocol enables customers with different MSPs to charge at CPs operated by different CPOs. Amongst other things authentication and authorization is defined, including the management of both personal and anonymized user data [52], [56].
- The **Open Charge Point Protocol** (**OCPP**) is most commonly used standard for communication between CPs and CPOs and is used for a wide variety of use cases concerning the operation of (aggregations of) CPs [46], [57], [58].
- **IEC 63110(-1:2022)** is mainly targeted at operation of CPs, enabling control over functionality such as energy transfer, firmware updates and monitoring. However, the functionality also stretches to roaming services, payment administration and user authentication/authorization. The standard is relatively new, but seems a contender for a multi-functional e-mobility ecosystem [59].
- **IEC 61851-1** is a standard for communication between EV and CP for up to 1,000 V AC or 1,500 V DC conductive charging. It describes operation, connection and electrical safety standards [60].
- **IEC/ISO 15118** is used to set up communication between EV and CP for EV charging and V2G purposes [61].

An overview of how the different protocols connect to different stakeholder is given in Table 3.

IV. A SURVEY ON THE CYBER SECURITY OF EV CHARGING INFRASTRUCTURE

In the previous chapter an overview of the EVCI-relevant CPS is given. Considering cyber systems' susceptance to cyber attacks [3], [4], literature on cyber security in smart grids is considered. Table 4 gives an overview of the literature used in a survey on research on the topics of cyber security in power grids and EVCI.

TABLE 3. Overview of protocols and stakeholders and their relations.

Protocol ↓ / Actor →	CPO	MSP	DSO	TSO	BSP	RSP	Cust.	CP	EV	Description
OSCP	x		x	x	x					Smart charging
OpenADR	x		x		x					Smart charging
IEEE 2030.5			x				x			Smart charging
IEC 61850-90-8			x					x		Smart charging
OCHP	x	x				x				Roaming
OCHPdirect	x	x								Roaming
OCPI	x	x				x				Roaming
eMIP	x	x				x				Roaming
OICP	x	x				x				Roaming
OCPP	x							x		CP operation
IEC 63110(-1:2022)	x							x		CP operation
IEC 61851-1								x	x	EV Charging
IEC 11518								x	x	EV Charging

Literature on cyber security in EVCI is divided into categories based on the specific focus of cyber security considerations: 1) reviews and surveys, 2) EV CPSs, focusing on individual EVs and internal systems, 3) CP CPSs, focussing on (communication) between individual CPs, 4) CP operation and CPMS, focussing on larger aggregations of CPs for instance through a CPO, and 5) protocols, ICT and IoT, focussing on the largest collective implications, as most CPs may use these and may be affected by the considerations. Often literature may fall in two or more categories. The category selected is then based on the size of potentially affected proportion of the infrastructure, going from smaller to bigger respectively. When multiple categories are selected for the same reference, cyber security of multiple subsystems is considered (for instance when a cyber attack are launched on EVs to maliciously affect CPs). An overview of vulnerabilities in EVCIs is given in Figure 3.

Cyber security of power systems is addressed by many authors [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [92], [93], [94], [95], [96], [97], [98], [99]. Of those, research into false data injection attacks (FDIA) has received a significant amount of attention in recent years [66], [72], [73], [86], [88], [89], [90], [91], [97], as well as intrusion/anomaly detection [64], [71], [75], [77], [80], [83], [87], [95], and cyber security of supervisory control and data acquisition (SCADA) systems [62], [70], [94], [96], [98], [99]. Furthermore, topics include the cyber security of (remote and/or automated) control systems [76], [78], [81], [92], data management [65], [74] and communications (especially substation communication protocols IEC 61850 and 62351), and the IoT in a power systems context [85], [93]. An overview is given in Table 4.

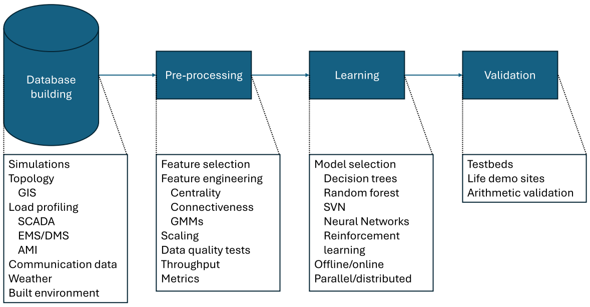


FIGURE 2. Overview of ML applied to power system research.

Anomaly or intrusion detection and prevention systems (IDSs and IPSs respectively) are often employed to improve cyber security in smart grids [77], [83], [87], [95], [100], [101]. These systems allow for timely identification of anomalies, thus allowing the operator for adequate response in manual attack mitigation. IPSs are equipped with logic for automated response based on intrusion severity assessment. In [77] the authors employ support vector machine (SVM) to detect anomalies in smart meters as critical part of AMI in smart grids. A temporal failure propagation graph is used to identify the attack origin in case of an anomaly. Finally the authors introduce a pattern recognition algorithm based on simulated cyber attacks, to determine the severity of the detected attack. Molzahn & Wang identify anomalies in data used for control centre algorithms. It could be seen as an IDS against FDIAs targeting optimal power flow derivation. Their method compares specified parameter data to historical operating point data to detect intrusions. An IDS for DoS attacks against BSPs/aggregators is presented in [100]. The authors present a method to impose a gateway to monitor incoming traffic in EVs. They compare their method with existing IDSs such as Cuckoo and show their method improves on throughput, packet delivery rate and jitter. In [83] Yang et al. present an IDS for SCADA. They use whitelists for access-control and protocols, as well as behaviour-based rules. Incoming traffic is compared to these lists and rules sequentially and any deviations are reported and logged. A testbed specific for SCADA simulation is presented and used to show an improvement of SCADA cyber security through the work's IDS. Finally, the authors in [95] present a distributed IDS, covering multiple layers in smart grids. The IDS covers home, neighbourhood and wide area networks (HANs, NANs, and WANs respectively).

TABLE 4. Overview of literature on cyber security in power grids and EVCI.

Topic	Refs
FDIA	[66], [72], [73], [86], [88], [89], [90], [91], [97]
Intrusion/anomaly detection and prevention	[64], [71], [75], [77], [80], [83], [87], [95]
SCADA	[62], [70], [94], [96], [98], [99]
Industrial Control Systems (ICS)	[76], [78], [81], [92]
AMI	[65], [74]
ICTs and IoT	[85], [93]

EVS AND CHARGING INFRASTRUCTURE

Topics	Refs
Review or survey	[2], [14], [15], [17], [18], [102], [13], [103], [104], [105]
EV cyber-physical systems	[7], [8], [106], [107], [108], [109], [110], [111], [112], [113], [114]
CP cyber-physical systems	[9], [115], [113], [114], [116], [117], [118], [119], [120], [121], [122], [123], [124]
CP operation and CPMS	[6], [11], [125], [126], [119], [127], [128], [100], [129], [130]
Protocols, ICT and IoT	[10], [11], [14], [125], [128], [131], [132], [133], [134]

The method is based on a SVM for anomaly classification. It is combined with an artificial immune system, where the immune system is taken as analogy for attack detection. The authors show the performance of their method using a form of confusion matrix and report an acceptable performance, but there is room for improvement. An overview of AI and ML applied to power system research is presented in Figure 2.

Encryption, through different cryptographic schemes, is often employed to improve cyber security in general. However, due to time criticality of monitoring and control in power systems, this is an especially difficult security control to implement. Encryption results in overhead that often renders typical schemes unusable. Nevertheless, IEC62351 is researched as security extension to the widely used IEC61850 standard for substation automation [69], [84], [135].

Recent years have seen the introduction of artificial intelligence (AI) and machine learning (ML) for improving cyber security in power systems. For instance, they are used for improving IDSs/IPSs [75], [77], [80], [95], data analysis for threat assessment and investment decision making [85] cyber security assessment [68], [71], and demand response automation [86].

While research on cyber security of smart grids in general is widespread, with a large variety of focus areas in terms of vulnerabilities and mitigation, the specific focus on electric vehicles – DERs with a significant impact on smart grids – is less thoroughly investigated [8]. However, this is contradicted in [2], where a survey is presented in which EVs get similar attention as for instance AMI and SCADA. One might conclude that this specific research topic is not always findable or part of research into a broader topic, such as DER security [16].

In order to gain a complete understanding of vulnerabilities and potential attack scenarios in EVCI, the use of assessment frameworks can contribute to coverage of the analysis. An example of such an assessment framework is the widely used STRIDE threat model. Short for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DoS) and Elevation of privilege, STRIDE was first published on by Microsoft in the November 2006 edition of MSDN Magazine [136].

- Spoofing: acting as someone or something else.
- Tampering: modifying data.
- Repudiation: erasing proof of action responsibility.
- Information disclosure: leaking information to unauthorized people or systems.
- Denial of service: overloading assets to discontinue services.
- Elevation of privilege: enabling access to systems otherwise unauthorized to.

The STRIDE framework proposes an analysis on authentication, integrity, nonrepudiation, confidentiality, availability, and authorization on a system decomposition. A potential decomposition of EVCI could be EV internals, CPs, CPMS and protocols, as suggested in 4. EVCI may also be broken down in to their cyber and physical parts, internal and external [2]. When diving deeper vulnerabilities may include, amongst others, CAN bus architecture – especially the on-board diagnostics (OBD2) port –, tire TPMSs and USB-ports as important internal EV vulnerabilities An attacker would need physical access to the EV to exploit them. Externally, several key EV charging communication interfaces – ISO 15118, Global Positioning System (GPS) and OCPP – may be prone to cyber attacks. These interfaces may also serve as the base for EVCI system fragmentation for STRIDE. For instance into CPs, information privacy, connection types (vehicle-to-anything, V2x) and autonomous EV systems [16]. An overview of the found vulnerabilities in EVCI components and their potential for STRIDE cyber attacks is given in Table 5.

Digital twins (DTs) may be used to detect and mitigate cyber attacks on EVCI. An important step in applying DTs is this context is state estimation. Namely, in order to detect a cyber attack a comparison to some viable base operation must be made. In [115] the authors use a long short-term memory (LSTM) model trained as a recurrent neural network (RNN). The data used to train the LSTM offline is generated using time series data generated by the DT model. The model is then trained online using deep reinforcement learning (DRL). The trained LSTM-DRL model is used to detect and mitigate FDIA and switching attacks, the latter described as controlling circuit breakers. They demonstrate

TABLE 5. Overview of components in EVCI and their found vulnerabilities to STRIDE-defined cyber attacks.

Attack → Component ↓	Spoofing	Tampering	Repudiation	Information disclosure	DoS	Elevation	Ref.
OSCP	x	x	x	x			[137]
OpenADR		x		x			[138]
IEEE 2030.5		x	x	x			[139], [140]
IEC 61850-90-8	x	x	x				[84]
OCPP		x			x	x	[10], [11], [14], [141], [134]
IEC 11518							[142]
OBC		x		x	x		[7]
BMS		x					[110]
USB (EV)		x		x		x	
OBD2				x	x		[108]
CAN	x	x	x	x	x		[7]
TPMS	x			x	x		[107]
EVSE		x		x			[7], [8]
Meter	x	x		x	x		[143]
USB (CP)				x		x	
Auth. term	x		x	x			[137]
UMTS & SIM					x		[144]

their algorithm can maintain system stability using the IEEE 30-bus test system.

As a form of digital twins, testbeds offer a modelling environment useable by other researchers. They often include both physical and cyber models of power systems [3], [141], [145], [146], occasionally incorporating EVCI [125]. Testbed may be used to design and test experiments by running self-made scenarios. The most advanced testbeds allow for modular selection of different test systems and different power system functionalities, such as markets, DERs (including EVs) and RES. Most relevant for EVCI cyber-physical security research are testbeds that include at least models for the categories presented in 4. Such a testbed is presented in [125]. The testbed includes a CPS implementation of CPs, a CPMS and OCPP (see below). The authors use the vulnerabilities described in [10] to deploy a load oscillation attack in a WSCC 9-bus grid model implementation. They conclude that through the attack, maximum frequency is exceeded, likely leading to tripped generator protection relays and blackouts.

The use of CPs, especially public chargers, are highly dependent on availability. In order to increase the user friendliness CPOs, BSPs, energy suppliers, and other EVCI stakeholders have developed an array of websites and applications that aim to aid in finding suitable charging locations. Applications, often on smart phone devices, often offer a map interface with CP locations and availability. While these applications may enhance user experience, they also create an additional vulnerability. Namely, cyber attacks could be launched by using the, mostly publicly available, data these applications generate. Potential attackers could employ data grabbing or even use APIs developed by application publishers. Especially in combination with open grid data [147], [148], [149], [150] public data might contribute to cyber attacks. Acharya, Dvorkin & Karri present an attack scenario based solely on publicly available data in [6]. The authors use open data on power grid infrastructure and common smartphone apps for EVSE usage patterns. The attack is based on similar vulnerabilities as presented in [2]. They construct a model based on linear (DC) power flow assumptions and swing equations in order to find the minimum requirements for an attack on the stability of the power grid of Manhattan. Such an attack will likely not succeed with current EV penetration and state of technology [6], [141]. However, by 2030 the adoption of EVs may result in power system frequency and voltage instability [30].

In order to conduct an extensive survey on the cyber security of EVCI, four cyber attack categories were identified and used to structure the remainder of this section:

- Cyber attacks on **internal EV components**. An attacker should have physical access to the car and a prime entry points are USB or the OBD ports. An important target system may be the CAN bus, where most internal communication is transported. The impact may be minimal, as only the infected car is affected. However, malware may spread from car to car through charging at (semi-)public CPs.
- Cyber attacks on **CPs**. Although also requiring access to physical infrastructure (the intended CP), this attack scenario could have an increased impact compared to the former attack scenario. Namely, the most obvious targets would be publicly accessible CPs, precisely those CPs where multiple EVs may visit. Moreover, specific vulnerabilities may be filtered on in the search for attack targets. Those vulnerabilities may be exploited to increase the attack vector for instance by entering CPMSs.
- **Operation of CPs.** In most cases large aggregations of CPs are operated by CPOs through a single CPMS. This poses a single point of failure. Especially as those systems may not be thoroughly secured. The affected number of CPs in this attack scenario would

be significantly bigger and therefore the impact on the power grid more severe.

- **Protocols.** Finally, the attack scenario with the biggest impact on the power grid is where an attack would be able to exploit vulnerabilities in charging protocols. As much effort has been put in standardising the communication in EVCI, a majority of CPs tend to use the same protocols for communication between EV and CP, CP and CPMS, and other parts of the EVCI. This introduces an even more centralised single point of failure than the former attack scenario: an succesful attack may allow the operation of CPs of multiple CPOs.

Some real-life examples of hacked EVCI can already be found in popular media. For instance, in 2022, during the ongoing war between Ukraine and Russia, parts of Russian charging networks were hacked to display Ukrainian propaganda [151]. Furthermore, high-risk zero-day vulnerabilities in Phoenix Contact EV chargers were successfully exploited during the Pwn2Own Automotive 2024 event [152]. Hackers were able to elevate privileges and, among other things, disrupt charging services—potentially affecting the connected power grid. Finally, in 2024, ElaadNL demonstrated large-scale risks in modern charging points (CPs), exploiting vulnerabilities in charging cables [153]. ElaadNL, an organisation formed by the Dutch DSOs, focuses on the development and standardisation of EVCI. Among other services, they offer large-scale testing for OEMs of both EVs and CPs. During their demonstration, they showed that 10 out of 18 CP models were broadcasting more services over the charging cable than necessary. These services could potentially be exploited to elevate user privileges—particularly in DC fast chargers—and allow attackers to target the CPMS. According to the researchers, this could ultimately destabilise the power grid.

A. CYBER SECURITY OF INTERNAL EV COMPONENTS

While the prime physical effects might not extend to the power grid, cyber attacks on internal EV components may affect EV operation. In order to safely drive, EVs rely on many onboard devices for sensing, actuating and diagnostics. In case these sub-systems are compromised, different EV functions may be affected. These functions include driving and braking, battery management, internal climate controls, and others. Cyber attacks on internal components might result in decreased driving experience, damage to the EV and even harm to driver and passengers [7], [8], [106], [107], [108], [109], [110], [111], [112], [113], [114].

Chandwani, Dey and Malik focus on vulnerabilities of internal EV components in [7]. They investigate vulnerabilities in OBCs – mainly the main charger controller – , (interfaces with and between) other engine control units (ECUs) on the CAN bus – similar to [2] and [6] – and the \BMS. They develop countermeasures and simulate data integrity attacks using MATLAB & Simulink to test their effectiveness. The work concludes that proper detection measures can effectively counteract attacks on internal EV CPSs.

Similarly the authors in [8] focus on potential damages to the EV itself, while recognising the potential for destabilising the grid. They model FDIA based on an exogenous input-based model, corresponding to their state-space modelling setup and target overcharging of the EV. They design and test a static and dynamic detection algorithm. The static algorithm uses only terminal voltage input data, while the dynamic algorithm combines that with system knowledge. Their conclusion is that the dynamic detector performs better overall, but given enough knowledge of the system, an attack may go unnoticed.

B. CYBER SECURITY OF EV CHARGE POINTS

Cyber attack on CPs may be launched in two ways 1) through physical access to either the CP or EV, or 2) exploiting communication between CPs, EVs, and their respective IT applications, e.g. smart phone apps or back-office systems. The latter will be discussed in more detail in Section IV-D. Vulnerabilities could be exploited by gaining access to the CP internals and installing malware, or infecting an EV and propagate during charging session interaction. Vulnerabilities to CP cyber systems, excluding CPMSs, are also considered in this category. Typically, these would entail wireless charging or session authentication. In this category, attack surface growth is dependent on a physical vessel – such as an EV or malicious USB – for spreading for instance malware. Considering the complexity of this, and thus the limited possibility for a large attack surface, the potential effects on power grids is limited 9], [72], [80], [81], [82], [83], [84], [85], [86], [87], [88], [88], [89], [90].

The authors of [154] mention the security flaws of OCPP (see Section IV-D). However, they recognize security patches in more recent versions. They design a new type of attack that is able to circumvent OCPP security measures, by one-time exploitation of CP vulnerabilities. Their man-in-the-middle (MitM) attack is based on vulnerabilities in the Transport Layer Security (TLS) used to secure communication between CPs and a CPMS. The novel attacks specifically target smart charging schemes. Attack objectives are energy markets, and ultimately BSP financial performance. The authors state compromising power system stability would require a very large number of exploited CPs.

In [9] and [116] the authors employ a mixed integer linear programming (MILP) model to optimise availability of grid components while minimising security risk of FDIA, either malicious or unintentional. In their model they simulate malware propagation through EVSEs and their communication networks similar to how a disease spreads in human populations. In their work they aim to show the interdependence of smart grids, EVCI and EVs.

Following recent technological developments in wireless charging, the authors of [117] write about the state-of-the-art in wireless charging, devoting a section on cyber security of such systems. Considering there's no physical connection between EV and CP, the handshake needs to happen over the air, making wireless charging specifically vulnerable to MitM, FDIA and DoS attacks. While it is stated that hacking a single CP may lead to damage of EV and CP, there is no analysis of larger attack vectors and the consequences for the grid. They test their solution on a NXP-ATOP and conclude it to be more secure than radio-frequency identification (RFID) or IEC 15118 at the time of writing.

Finally, [118] addresses MitM attacks that may be utilised to perform substitution, leading to possible charging transaction fraud and problems for DR programs. They propose an authentication protocol using an on-board IED that communicates with the EVSE to make sure the authenticated EV is the one physically connected to the grid.

C. CYBER SECURITY OF CP OPERATION

In order to efficiently roll out EVCI and charging facilities for EVs, CPs are controlled by a mere handful of private companies (called CPOs) in a bid for economies of scale. On the one hand, this approach has resulted in an all-together quicker and cost-effective realization of EV charging capacity. On the other hand, it has resulted in potential single points of failure. Namely, CPOs operate their CPs through ICT in the form of CPMSs. Often, CPOs rely on cloud applications for connecting to tens or even hundreds of thousands of CPs for operation, firmware updates and diagnostics. As a result, huge aggregations of CPs may be vulnerable to insider threats, MitM attacks, DoS attacks, and others through a single point of access. Considering the accelerating adoption of EVs and subsequent increase in the number of CPs, the consequences for the power grid may be vast [6], [11], [100], [119], [125], [126], [127], [128], [129], [130]. Based on the National Institute of Standards and Technology (NIST) Internal or Interagency Reports (NISTIR) 7628 [119] propose a cyber security architecture and demand response scheme for smart EV charging. They claim their design is scalable and provides secure identification implemented between an on-board intelligent electronic device (IED) and a charge management server (i.e. CPO back-office). The system is tested on a NXP automotive telematics onboard unit platform (ATOP).

D. CYBER SECURITY OF PROTOCOLS AND OTHER ICT

The final category of literature analysed in this work focuses on ICT and IoT used in EVCI. ICTs and IoT are, amongst others, used for communication from EV to CP, between CPs, and from CP to several back-office systems such as CPMS (see above). It is widely recognized that ICTs and IoT may be vulnerable to cyber attacks. Seeing all or most CPs rely on identical or similar ICT and IoT components, this final category can be considered as the worst case scenario. A successful exploitation of vulnerabilities in ICTs or IoT might result in the entire EVCI being affected, with consequences for power grids stretching even beyond country borders. On top of that, in order to promote efficient operation and interoperability, standardization has been a top priority in the development of EVCI. ElaadNL, formed by Dutch DSOs, is a prime example of that endeavour. Standardization has resulted in a number of communication protocols that are used to perform various tasks of EVCI all over the world. A downside to this development is the potential for cyber attacks with unprecedented consequences for power grids [10], [11], [14], [125], [128], [131], [132], [133], [134].

OCPP is a communication protocol that is rapidly becoming the de facto standard for communication between EVSEs and a CPO's back-office. Therefore an attack on especially this communication protocol may lead to disastrous effects on power grids. This is exactly what is proven in [10]. The Internet Engineering Task Force (IETF) framework Request For Comments (RFC) 3552 and unified modelling language for security (UMLsec) notation is used to analyse the cyber security of the protocol. They conclude that design flaws may be used to launch cyber attacks. The consequences for power grids may be disastrous. However, their findings were based on the currently outdated OCPP version 1.6, which had a security update to version 1.6-j in 2018 (after publication of [10]).

The most recent OCPP version is 2.0.1. Alcaraz et al. present an in-depth analysis of that version using STRIDE and threat classification framework DREAD (Damage, Reproducibility, Exploitability, Affected users and Discoverability) in [134]. They argue that while the latest version has considerable security improvements, it is still susceptible to cyber attacks, namely tampering, and DoS attacks. A review of security and privacy-related literature in OCPP version 2.0.1. is presented in [14]. The author categorize attacks into cyber, physical, and cyber-physical and analyse literature in each category. They conclude that while an important improvement in terms of security, version 2.0.1. not all possible attacks already have countermeasures. Moreover, the authors report on blockchain as a frequently used technology to mitigate susceptibility to and consequences of cyber attacks.

The low security maturity of OCPP is also recognised by [129] and [141]. Kabir et al. describe a switching attack – described here as quick cycling of charging/discharging of a large amount of EVSEs – through the protocol. The attack could potentially go undetected and lead to inter-area oscillations and eventual blackouts if targeted at weakly connected generation areas. They design a back propagation neural network scheme that is effective at detecting and mitigating the effects of the attack scenario. The authors base their analysis on the claim that no authentication is required at private EVSEs/CPs. However often authentication procedures are very similar at public and private EVSEs (at least in The Netherlands). Private CPs are often also connected to a CPO back-office and require the same charging session authorisation, although newer versions of IEC 15118 enable identification of the plugged-in vehicle directly.

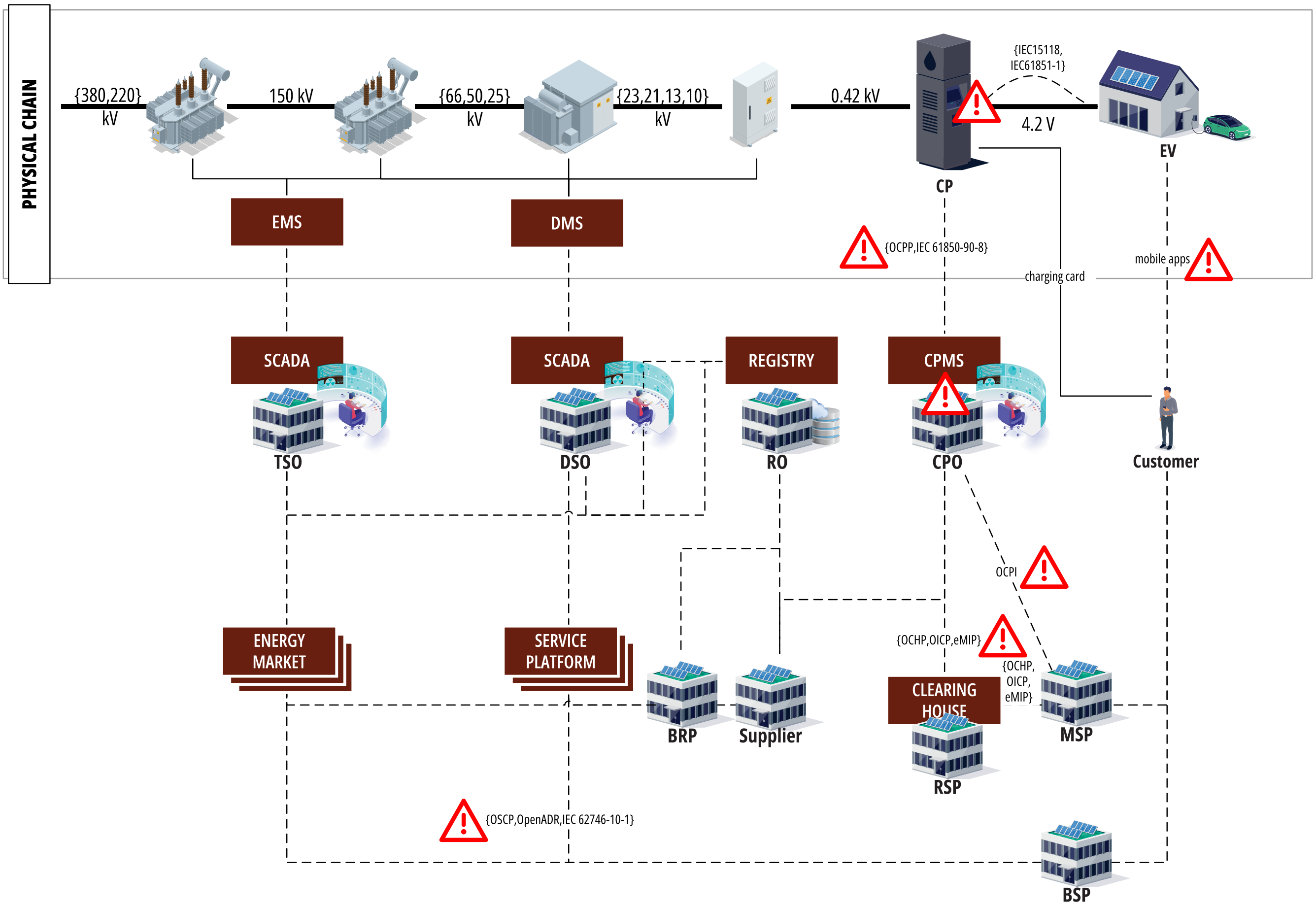


FIGURE 3. Overview of EVCI and related cyber security vulnerabilities.

Electrification is an important by-product of energy transition. As systems such as heating and transportation transitioned, a prime alternative to fossil fuels is often electricity. As a result, more and more strain is put on power grids. While grids are expanded, system services are required to optimal allocate available capacity. Congestion management is a relatively new example of this, especially for DSOs. In order to unlock the potential of DERs for providing system services – often called flexibility – new ways of communicating between stakeholders and assets is required. OpenADR and OSCP are examples of this (see Section III-C2). A security assessment of OSCP is described in [137]. The protocol in combination with weak authentication (through RFID) allow for spoofing, using a counterfeit card to enable charging sessions, or eavesdropping of valid session details. On top of that, due to the lack of end-to-end security, tampering with data at different parts in the communication chain is possible. This would prove detrimental if a stakeholder such as a CPO has been (unknowingly) compromised and an attacker could alter service provision. TLS information is not provided at the end of the secure tunnel, preventing integrity validation later in the process. Some of these issues are addressed in OpenADR systems by using XML signatures [138], although integrity is not fully guaranteed. Because IEEE 2030.5 lacks requirements for end-to-end security, secure communication implementation is questionable and may pose a number of cyber vulnerabilities [139]. IEC 61850-90-8 is an EV-specific implementation of the IEC 61850, which due to overhead constraints contains no specific cyber security measures [84]. Considering no out-of-the-box security is offered in IEC 61850, sub-standard IEC 61850-90-8 is assumed to have similar vulnerabilities. IEC 15118-2 was an extension to IEC 15118 incorporating security measures such as TLS tunnels and encrypted XML for end-to-end secure communication [142], securing most of the vulnerabilities prevalent in other protocols.

V. A SURVEY ON THE (CYBER) RESLIENCE OF POWER SYSTEMS

A. RESILIENCE ENGINEERING: THE ROOT OF ALL RESILIENT POWER SYSTEM

The notion of system resilience originates from robustness and stability. Thus combining the ability to overcome adverse conditions, respectively the ability to return to steady state after disturbances. The initial definition was adopted and extended to include different phases: anticipation, response, recovery and adaptation. Currently, resilience engineering is thoroughly researched field. It finds application, applied in various fields, including power system engineering. Holling is considered to have introduced the concept of system resilience in his work in 1973 [155] and further through works in 1986 [156], 1996 [157]. He describes resilience of (ecological) systems as the ability to persist despite external influences. He compares the term with the stability of a system, which is the ability to return to an equilibrium state after external influences. According to Holling resilience and stability are often inversely related and heterogeneity and complexity might promote the resilience of a system. In the author's more recent work, he further compares the two views, dubbing the former definition as ecological resilience and defines focusing on stability near an equilibrium state as engineering resilience [157]. The work describes that the short-term stabilisation success of resilience engineering might result in actual gradual decrease of system resilience.

Reference [158] extend the definition of resilience by not only incorporating persistence, but also returning to normal performance after a disrupted state. Their review concludes on common features of resilience definitions found in other works. The most important common aspects are: limiting negative effects of disruptions and quickly returning to normal operation. Other important aspects mentioned are quick identification and adequate adaptation to prevent future re-occurrence.

Bhamra, Dani & Burnard also include returning to a stable state in the definition of resilience in [159]. They base their claim on many definitions gathered through a literature survey. The authors argue that, based on reports of numerous small and large catastrophes, localised failures can cause cascading effects far beyond the directly impacted system. The resilience of a system then becomes a function of vulnerability, i.e. the ability to absorb shocks, and adaptive capacity, or the ability to adjust accordingly. The authors conclude that while many research focusses on defining system resilience, little work is spent on empirically proving said definitions.

[160] state that the resilience can be used to increase the scope of risk management as a part of systems engineering. Similar to [159] they describe resilience as a function of anticipating, absorbing, adapting to and recovering from inevitable disruptive events. From a review of resilience definitions, they conclude this is also true for critical infrastructure systems. They compare the two schools of resilience – as a static characteristic of the system versus an ever-changing function of the system characteristics – and give preference for looking at resilience from the latter, epistemic viewpoint, comparable to [156]. Besides defining resilience from multiple perspectives, Francis & Bekera in [160] compare the concepts of disruption – external and systemic, and of human, automated, and combined origin –, failures and success, and their implications for resilience strategies. Moreover, they compare the definition of resilience with that of safety, reliability and survivability. They indicate the overlap in terms of adaptation, but show large contrasts in terms of anticipation and the notion that resilience is a quality achieved through operations rather than a property of a system. The latter is also addressed by Holling in his works [155], [156], [157]. The authors identify robustness as part of resilience as the "withstand" or absorb phase.

B. RESILIENCE ENGINEERING OF POWER SYSTEMS

In 2015, Panteli & Mancarella considered the application of resilience to power systems as a novelty, lacking a "universally accepted [...] definition and even a common understanding of the concept" [12, p. 112]. Currently, there is an abundance of literature on the topic, often focussing on resilience of power systems against natural hazards or extreme weather events. Multiple authors distinguish the difference between stability against frequently occurring low impact events, and resilience against so-called HILP disturbances [19], [161], [162].

In [19] the authors present a review of the state-of-the-art in power system resilience, focussing on "extreme events" relating to weather and natural hazards, but also cyber events. While they state that there is no uniform consensus on a definition of resilience of power systems, the presented definitions correlate strongly. Below is a list of seemingly synonymous words used to define power system resilience per key element of resilience.

Not all definitions use all key elements – or a synonym thereof – but the most used terms include anticipate, absorb and recover [12], [162], [163], [164], [165], [166]. In short, the definition of power system resilience closely follows those found in general resilience (engineering) research. It revolves around anticipating high impact low probability events, absorbing as much as possible of the impact of such events and recovering quickly to a pre-disturbance service level.

1) METRICS FOR POWER SYSTEM RESILIENCE

Considering resilience as an epistemic characteristic [156], [160], the ability to monitor resilience is of the utmost importance. Therefore, metrics are defined in order to quantify and measure resilience during different phases.

Bruneau et al. are considered to have introduced what is now known as the resilience triangle, even though they do not mention it explicitly as such in their work [167] (see Figure 4). They present a metric to measure system performance over time: $Q(t)$. The graph forms a triangle between the time of a disturbance t_1, the time of return at stable system performance t_2, stable system performance Q_T and degraded system performance Q_1. The triangle was later extended by [162] and [168] to form a trapezoid. The resilience trapezoid includes the different phases of resilience. The performance $Q(t)$ remains relatively stable

TABLE 6. List of synonyms used to define power system resilience.

#	Most common	Synonyms
1	Anticipate	Prepare, prevention, prepare, plan
2	Identify	Resourcefulness, perceive
3	Absorb	Withstand, survive, tolerate, continuing to deliver, resist, maintain functionality, robustness
4	Recover	Respond
5	Adapt	Learning

in each phase, but each phase includes a plateau indicating the different phases of resilience (related to the terms presented in Table 6). This results in a trapezoid shape. The resilience triangle or trapezoid is often a starting point for visualizing and quantifying power system resilience [169]. For example [162], [168] make a distinction between operational and infrastructural resilience. They present a mathematical framework that describes the trapezoid in terms of degradation speed, depth and duration, and restoration speed. Their parameters include customer and generation power interruption, and tripped power lines.

In quantifying power system resilience, special attention needs to be given to the objective of the system. For power systems this is delivering power to customers connected to the grid. Often, resilience engineering is employed in power grid planning and an indication of resilience is required for important decision making. Fragility curves are often turned to in order to give this indication while respecting the stochastic nature of HILP events. Fragility curves or functions, are indicators of asset or system failure probability as function of some input or state variable. In power system resilience research the input often relates to extreme weather conditions such as wind speeds, precipitation, water levels, etc. [12], [19], [161], [163], [165], [166], [168], [170], [171], [172], [173], [174], [175], [176], [177]. For example, in [160] the authors further emphasize the importance of an objective setting for measuring resilience. The authors state that resilience is ultimately defined by absorptive, adaptive and recovery capabilities of the system. A metric is defined based on speed of recovery and system hardness, i.e. the ratio between original and new stable state system performance. Fragility curves are used to measure expected system degradation in the face of a disruptive event. An entropy-weighted factor is used for event stochastics. The metric is tested in a newly designed, experimental distribution system model.

Thus, resilience assessment needs a relevant metric as indicator of system performance. In [12] the loss of load frequency (LOLF) and loss of load expectation (LOLE) are used. The authors use them to model the resilience of power systems to extreme weather events. Moreover, they use the aforementioned fragility curves to determine probabilities of component failure.

In [166] the authors use a similar approach. Metrics are used for transmission substations and distribution nodes with power, the percentage of critical facilities with power, and the percentage of customers with power in the face of hurricane events.

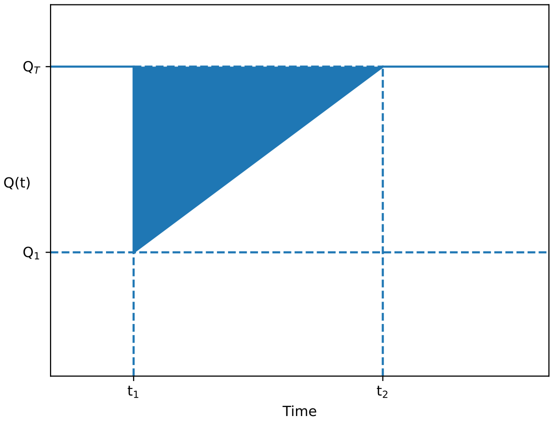


FIGURE 4. Resilience triangle.

Bhusal et al. present an extensive review of power system resilience in [19]. Their review includes definitions, metrics, enhancement and modelling methods. They compare attribute-based metrics – i.e. as a static characteristic – with performance-based metrics – i.e. epistemic. The former includes robustness, adaptability, resourcefulness, and recoverability. The latter is based on quantitative data. The authors present a review on both types, further categorising into 1) resilience features, such as betweenness centrality, 2) code-based (for instance based on running simulation models [178]), 3) reliability-based, such as LOLF, LOLE and energy not supplied, and 4) other metrics such as total energy curtailment.

Ji, Wei & Poor adapt two industry standards – system average interruption frequency index (SAIFI) and system average interruption duration index (SAIDI) – to measure power system resilience under extreme weather conditions [174]. Interestingly, the authors in [178] state that these are reliability metrics used to measure power system performance. Moreover, they state their usefulness is in decline due to 1) increasing numbers of HILP events, 2) renewable energy generation and 3) cyber security related events. Nevertheless, in [174] the author use the metrics in the form of the ratio between interrupted and un-interrupted customers, as well as the total interruption time and number of customers. The model does not include the customer average interruption duration index (CAIDI), which is also widely implemented in industry. CAIDI is the ratio SAIDI over SAIFI and could provide a meaningful extension in terms of recovery performance of the system. Namely, a low CAIDI would signal a short restoration time. In terms of resilience, these measures quantify how the system objective of transporting electricity to customers, is influenced by HILP events.

The authors of [179] present a risk assessment database containing 25 indexes that can be used as performance indication, thus they can quantify the resilience of power distribution systems. They include frequently used metrics for interrupted services such as loss of load probability (LOLP) and damage to grid components, but also resilience of DERs, and external factors such as related to emergency response services and meteorology.

There are many more works describing metrics for the quantification or assessment of power system resilience [180], [181], [182], [183], [184], and the aforementioned is not an exhaustive review of the entire state-of-the-art of power system resilience metrics. However, the explored body of work follows very similar patterns: starting from the resilience triangle or trapezoid, picking performance metrics relating to loss of load or power system component failures, and describing a mathematical, statistical, or modelling method to quantify and analyse resilience in the face of a HILP; most often related to extreme weather or natural hazards.

2) IMPROVING POWER SYSTEM RESILIENCE

After designing indicators for determining power system resilience, the next step is increasing the resilience to HILP disturbances. Taking measures to improve system resilience can be spread out over multiple time horizons, from short term to long term investments. Often, improving power system resilience is related to introducing redundancies, for instance the widely recognized N-1 contingencies. Making these types of changes to the power system, of the physical grid, is commonly referred to as grid hardening. However, as the impact of HILP disturbances is likely to exceed single contingency conditions, measures should in most cases extend this security fundamental. In [23] the authors categorise power system resilience improvements into planning, response and restoration, based on [185]. According to the authors, planning is related to long-term investments – both hardware- and software-based – focussing on anticipation and absorption. Response however, is short-term, and focusses on day-ahead and real-time measures. Finally, restoration includes system recovery measures. When regarding long-term planning of power system resilience, the authors consider software-based approaches to be most cost-effective. They review different measures in each category.

Mohamed et al. present a review of ''proactive'' measures for improving power system resilience [186]. They divide enhancement actions into short-term – days or weeks before and during HILP – and long-term planning, the latter further categorised into operational, hardening and ''smart technologies'' such as AMI, microgrids (MGs) and DERs.

As mentioned by [23], one of the measures that can be used to increase power system resilience in all phases is the use of renewable energy generation (REG) combined with energy storage systems (ESS)s, often in a MG context. In [28] the authors present a review of location, allocation and operation optimisation of REG and ESSs. They conclude that most literature focusses on cost and network loss minimisation. Nazemi et al. present such an optimisation based on linear programming [187]. Based on fragility curves in an earthquake context, their approach aims to minimise loss of critical load with financial constraints of ESS deployment. Similarly, [188] use a two two-stage stochastic mixed-integer second order conic program to model cost-efficient deployment of mobile ESSs by a DSO to prevent load shedding. On the other hand, [189], [190], [191] present models to use mobile ESSs (MESSs) specifically for restoration purposes. In [192] the authors also focus on MESSs for the recovery phase, presenting an architecture based specifically on EVs. While, in [193] the authors combine different types of MESSs to address both the absorb and recovery phases. [194] present a multi-objective optimisation formulation for optimal allocation and location of REG and ESS combinations. They specifically focus on restoration, giving higher priority to non-black-start generators.

Chen et al. present a review of another much investigated measure for enhancing power system resilience: microgrids [21]. They address networked MGs and distinguish between MGs with fixed and dynamic boundaries, presenting work mostly on the absorption and recovery phases. In [195] the authors present utilise a strategy based on minimum state of charge (SoC) of ESS. The ESSs can be used in the case of a HILP even to improve resilience. A method for determining optimal identification of MG boundaries for resilience is presented in [196]. In [197] the authors use EVs to optimise resilience not only of the distribution grid, but also the individual MGs it comprises. Reference [198] formulate an optimisation problem to minimise load shedding using controlled islanding. Their constraints are based on system frequency constraints and active and reactive power balance.

MGs and islanding can also be utilised as a tool for speedy recovery, as is demonstrated by [199], [200], [201], [202], and [203]. Reference [199] exploit MGs to quickly isolate faults and begin restoring service. References [200] and [204] focus specifically on restoring service to critical loads. Reference [201] combine networked MGs through soft open points (SOPs) – electronics for controlling power flow at open ends in a distribution network – with planning of MESS, repair crews (similar to [203]) and, devices used for fault detection and voltage support. In [202] the specific focus is on restoring power supply to critical loads in distribution systems, which is achieved through the use of EVs as MESS.

C. CYBER RESILIENCE OF POWER SYSTEMS

Like power system resilience, cyber resilience deals with the ability of a system to anticipate, absorb, recover from and adapt to HILP events. However, the specific focus is on malicious cyber events [186], [205], [206], [207]. Nevertheless, the focus is unequivocally on maintaining an acceptable level of service, performance or output of the system in the face of HILP events. Power systems comprise of the physical system and a cyber system. The cyber system is used, amongst others, for monitoring and control. Therefore, the power system must be regarded as the cyber-physical system (CPS) [208]. In conclusion, it is important to recognise potential cyber-physical attacks as HILP events with potentially unprecedented effect on power systems [186].

One important difference between the application of the concept of resilience in power systems and cyber systems, is the ability to adequately and timely detect an ongoing cyber event [209], [210], [211], [212]. This gives rise to an additional resilience phase added in the context of cyber systems: identification. Moreover, for other types of HILPS there may be observable precursors, i.e. they can often be foreseen to some extent. For instance, this is the case when looking at changing weather conditions and climate influences for weather HILP disturbances. On the other hand, this will most likely not be the case for cyber attacks. Considering the power CPS is very complex, only the most sophisticated attacker would have the resources to penetrate its defences – which include intrusion detection. Capable actors would most likely be able to obscure their cyber attack until it's too late. As a result, a different approach has to be taken with cyber resilience, especially towards anticipation and response.

In [102] a survey is presented of cyber-physical security in active distribution networks (ADNs). A prime origin of cyber attacks may be the interconnected EVCI. Vulnerabilities in several of the system components discussed in Section IV are mentioned as source of potential cyber attacks. These cyber attacks may lead to electricity fraud, and damage to the connected AND in the form of voltage and frequency instability.

A security score for quantifying power system effects of cyber attacks on EVCI is presented in [141]. The metric is based on different indicators of feasibility, impact and detectability. Their approach is validated in a model of the New South Wales grid to train a LSTM-based method to detect and locate cyclic load attacks.

In [212] the authors present a survey on the state-of-the-art of power grid cyber resilience, starting with characteristics of cyber attacks on power systems, primarily on IT-OT interfaces of the CPS. They also underline the possibility of an attack coming from sub-systems such as EVCI. The authors recognise the importance of adequate detection of cyber events. They conduct a survey on the use of DERs for response and restoration purposes. Furthermore they review the application of cyber-physical testbeds.

Literature on metrics to assess cyber resilience of power system is underrepresented compared to "regular" power system resilience. The authors of [213] present a review of assessments frameworks used to quantify cyber resilience, not specifically in the context of power systems.

In [214] a resilience metric for CPS is proposed based on two variables 1) the degree to which the system is able to be steered to any state within the domain of the system and 2) the ratio of available sensors to state variable, taking the minimum over all state variables as parameter. In essence it looks at affected sensors and actuators in the CPS.

A game-theoretical approach to fragility curves for cyber-resilience is defined in [215]. The authors look at quantifying grid damage – in terms of tripped lines, loss of load and generation, and associated costs – as a result of cyber attacks, while grid hardening is employed to improve resilience to the attacks.

Smart grids rely heavily on data coming from IT and OT systems. Therefore, information models that relate that data to each other become crucial for extracting and standardising the information needed for operation of the system. In [216] these information interrelationships are used to create a quantitative exposure metric, depending on the corresponding security mechanisms.

Reference [217] have developed a database of cyber attacks on protection relays. The database is used to set up a dynamic security assessment. By measuring rotor angle, bus voltage, and frequency they classify the system's response to the attacks. The classification is based on pre-defined secure state operation limits.

Finally, several works have been published on the development of cyber-physical testbeds that can be utilised to analyse and characterise cyber-physical attacks on power systems. Extensive reviews are presented in [166] and [167].

VI. MODELING EV CHARGING BEHAVIOUR

In the previous sections evidence is given that EVCI are cyber-physical systems and are becoming an important sub-system of power systems. EVCI's susceptibility to cyber attacks has been shown. While the impact of a cyber-physical attack on EVCI might be vast for power grids, the topic is not widely researched. This holds especially for power distribution grids. Therefore, the findings of this survey are extended with preliminary simulation results to underpin the importance of the topic for future research.

In order to investigate the effects of cyber attacks on EVCI in distribution grids, an accurate estimation of EV charging-related load is required. Hence, a method to stochastically model EV charging behaviour is presented in this chapter. The method can be used to generate load profiles originating from CPs. Finally, the resulting load profiles are used to simulate cyber attacks on EVCI and their effects on distribution grid voltage.

The charging behaviour is modelled as a Markov chain, where each CP state transition is governed by probabilities. Each CP knows three states 1) unoccupied, 2) charging and 3) idle (occupied but not charging), see Figure 5. p_{12} is the probability of EV arrival at the CP and is time-dependent. p_{23} is related to the EV's energy demand, which is modelled probabilistically in the method. p_{23} related to a probabilistic connection time on top of energy demand, governing the departure of EVs before being fully charged. Finally, p_{31} embodies the probability of an EV reaching full state-of-charge before the connection time has expired.

Algorithm 1 Pseudocode for Stochastic Charging Behavior

```
**Input:** $f_{(A,\tau)}(t)$, $F_{(C,\tau)}(x)$, $F_{(E,\tau)}(x)$, $F_{(P,\tau)}(x)$, $\mathrm{CP}^{\mathrm{tr}}_{\tau}$, $T_r$, $T$, $t_0$, $t_T$, $I$
**Output:** EV charging load profile $P^{\mathrm{tr}}_{T}$ per transformer
Initialization
**for** $tr \in T_r$ **do**
    **for** $i \in I$ **do**
        **for** $t \in T$ **do**
            **for** $cp \in \mathrm{CP}^{\mathrm{tr}}_{\tau}$ **do**
                **if** $\alpha_{(cp,t)} = 1$ **then**
                    **if** $t = t^{cp}_{\mathrm{dep}}$ **then**
                        $\alpha_{(cp,t)} = 0$
                        $\beta_{(cp,t)} = 0$
                    **else if** $P_{cp}(t - t^{cp}_{\mathrm{arr}}) \geq E_{cp}$ **then**
                        $\beta_{(cp,t)} = 0$
                    **else**
                        $P^{\mathrm{tr}}_{t} = P_{cp}$
                    **end if**
                **else**
                    **if** $R \in [0, 1] < f_{(A,\tau)}(t)$ **then**
                        $\alpha_{(cp,t)} = 1$
                        $\beta_{(cp,t)} = 1$
                        $t^{cp}_{\mathrm{arr}} = t$
                        $t^{cp}_{\mathrm{dep}} = t + F_{(C,\tau)}(R \in [0, 1])$
                        $E_{cp} = F_{(E,\tau)}(R \in [0, 1])$
                        $P^{\mathrm{tr}}_{t} = P_{cp}$
                    **end if**
                **end if**
            **end for**
        **end for**
    **end for**
**end for**
```

An overview of the method is given in Algorithm 1 in pseudocode. The arrival times $f_{A,\tau}(t)$ were adopted from [218] as a Probability Density Function (PDF), giving the arrival time of an EV at a CP: t^{cp}_{arr}. From the same, three inverse Cumulative Distribution Functions (CDFs) were taken:

- Connection times, $F_{c,\tau}(t)$, resulting in departure time of the connected EV at a CP t^{cp}_{dep}.
- Energy demand, $F_{E,\tau}(t)$ resulting in the energy demand for the currently connected EV at a CP E_{cp}.
- Outlet power, $F_{P,\tau}(t)$ resulting in the outlet power per CP P_{cp}. During *Initialization* of the model, amongst other things, each CP is assigned with its outlet power.

Sampling from the PDF was done through Bernouilli trial and from the CDFs using random number draw.

The number of total CPs CP^{tr}_{τ} per charger type $\tau \in \{private, public, work\}$ and transformer (MV to LV) $tr \in Tr$ is deducted from [1]. The ratio per transformer is shown in Figure 7. A significant increase in the number of CPs is to be expected. As is apparent from the figure, the spread will also increase. This spread can mostly be attributed to the future development of charging hubs, causing hot spots with significantly large numbers of CPs.

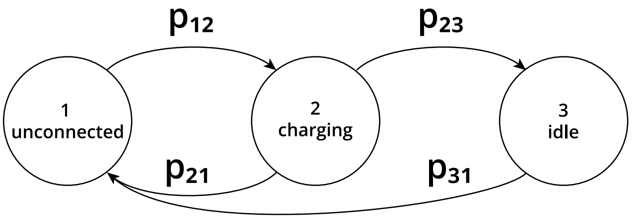


FIGURE 5. Markov chain diagram for EV charging, representing the different states of a CP.

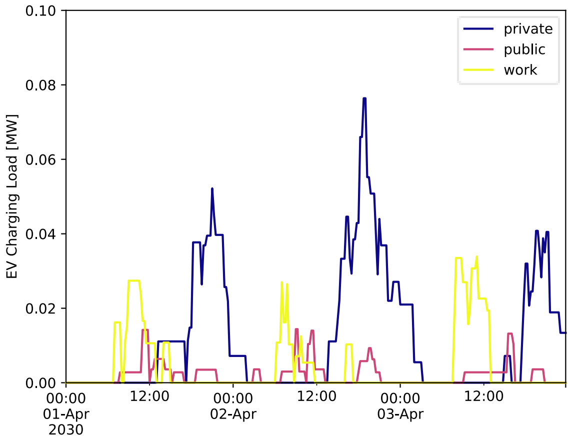


FIGURE 6. Example load profile for a single transformer for **T = 288, *t* = 15 minutes, t_0 = April 1st 2030 00:00, t_T = April 3rd 2030 23:45, *I* = 1.**

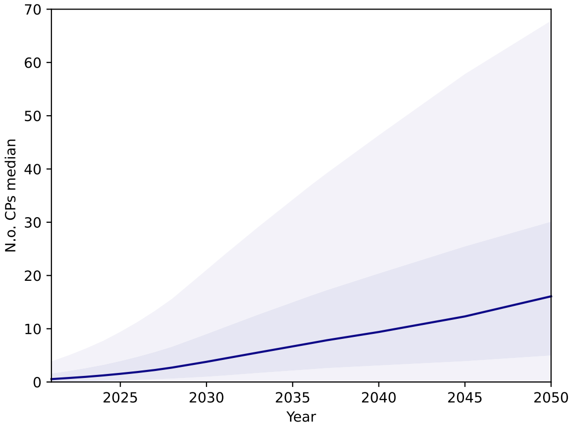


FIGURE 7. Development of number of CPs per MV-LV transformer (median), including interquartile (25-75%) spread and lowerand upper bound.

Simulations are run for T timesteps t, from t_0 to t_T. Then let $\alpha_{cp\,t}$ *and* $\beta_{cp\,t} \in \{0, 1\}$ be the occupied, respectively charging state per CP for any given timestep. The number of iterations is set to I.

Figure 6 shows an example output of the algorithm for a random transformer in a grid model supplied by a Dutch DSO. The figure shows a single iteration of 3 days (288 timesteps of 15 minutes). Evident from the figure is that the specific transformer is in a residential area, considering the high load originating from private CPs. Moreover, the peaks coincide with peaks found in [1] which are in the evening (around 19:00) and morning for private and work related charging respectively. The public charging shows less of a pattern, resulting from their more diverse usage. Finally, the model also accounts for change in charging behavior between weekdays and weekend. The simulation ran from Monday up to and including Wednesday, therefore including work-related charging. Figure 6 shows the results from a single iteration. When more iterations are run and the results averaged, the plots approximate the ones presented in [1].

VII. SIMULATION RESULTS

Simulation results of cyber attacks based on the EV charging load profiles described in the previous chapter are presented. The object of the simulation study is to show the potential impact an cyber attack on EVCI might have on the power system. Considering the probabilistic nature of EV charging behaviour, special examination of stochasticity must be addressed. Thus, a cyber attack scenario is designed where an attacker would conduct a cyber attack to disrupt the grid. Consequently, it is most likely an attacker would target either a CPO's CPMS or a CP protocol (see Section IV). Namely, the effects on the grid of an attack would be mainly dependent on the amount of load collectively controlled in the affected EVCI. This in turn is dependent not only on the number of CPs, but also their outlet power and the presence and energy demand of EVs. As these variables are highly time dependent, a stochastic approach was chosen to model the EV charging behaviour (see Section VI). Thus, a large number of iterations was run to prevent experimental bias. In order to demonstrate the effect the cyber attack would have on the grid, voltage stability was chosen the main indicator. A number of assumptions were made in designing the cyber attack scenario:

- Assumption 1: the vulnerabilities described in Sections IV-C and IV-D are exploited to gain access to CP operation.
- Assumption 2: remote attacks on CPMSs and MitM attacks on OCPP and OSCP are used to eventually elevate hacker privileges to remotely operate CPs.
- Assumption 3: all CPs in the analysed grids are connected to a CPO back-end. By combining the fleet of CPs of different CPOs the attack is scaled up to cover private, public and workplace CPs.
- Assumption 4: the attacker controls enough computational power and network bandwidth to simultaneously execute an attack across the entire attack vector.
- Assumption 5: the attacker has deep knowledge of the energy system, using market insights in supply and demand to time the attack.

The attack scenarios described above are often referred to as load altering attacks (LAAs). A cyber attack exploiting a vulnerability in a charging protocol is modelled, resulting in the worst case scenario, i.e. the largest possible affected collective load. In terms of power system operations these LAAs can affect a power grid's frequency, rotor and voltage stability [219]. Of those, the latter is chosen as focal point. Namely, frequency stability is often the responsibility of transmission system operators (TSOs) who are not responsible for distribution networks. Moreover, rotor stability requires the presence of synchronous machines, which are not as prevalent in MV distribution networks (DNs) as they are in transmission networks (besides inverter-based generators). As a result, voltage stability is chosen as the starting point for impact analysis. As an indication for voltage stability, the effect of the cyber attack scenario on voltage levels is reported on in this work.

TABLE 7. Facts and figures of the studied MV distribution grid.

#	Variable
External grid voltage	50 kV
Number of HV transformers	4
MV nominal voltage	10.5 kV
Number of MV busbars	151
Number of MV loads	119

For our experimental setup, a MV grid models is supplied by a Dutch DSO. A schematic overview in the form of a single line diagram is given in Figure 8. The most important facts and figures are given in Table 7.

The power flow analysis is conducted through DIgSILENT PowerFactory's Python API. Disturbance event dates are generated based on a random week- or weekend day, depending on the experiment. Simulated times are 8:45, 12:45 and 18:00, coinciding with regular morning, afternoon and evening peaks in distribution grids. The attack scenario is based on the attacker's knowledge to coincide with ancillary services markets. As such, the CPs are assumed to be in the idle state (see Figure 5) as part of a congestion management service to the DSO. The attack is executed by simultaneously switching the CPs to charging state during congested power grid conditions, further straining operational limits. The attack is simulated in PowerFactory using Parameter Event Objects (.EvtParam, hereafter PEOs) inside the Quasi-Dynamic Simulation (QDS, "ldfsweep" inside PowerFactory. ComStatsim simulation module object) events module (IntEvtqds). The PEOs target the MV loads objects (.ElmLodmv) and sets their "scale" parameter. Before the attack the loads are scaled down to their base, non-charging load, simulated delayed or smart charging. At the time of the attack the loads are scaled to 1.0, i.e. fully considering loads of all connected and charging CPs.

To minimize statistical bias, experiments are repeated 30 times, generating new EV load profiles each time. EV charging load profiles are generated for the entirety of the simulation date, resulting in a statistically relevant EV load at the time of the disturbance. For each simulated disturbance event a base simulation is run on top of the disturbed state simulation. For each bus, voltage magnitude (in p.u. based

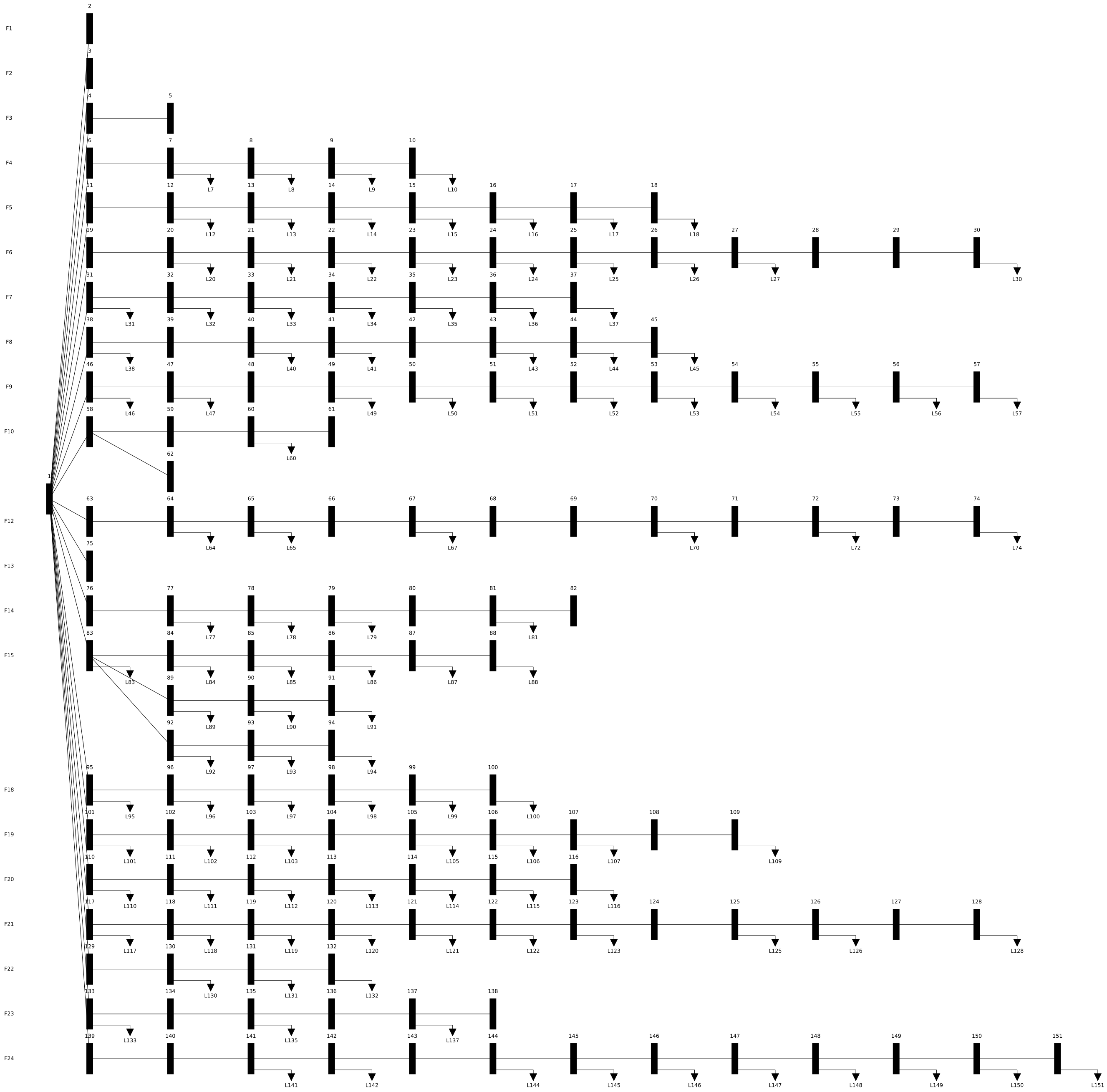

F1 2
F2 3
F3 4 5
F4 6 7 8 9 10
L7 L8 L9 L10
F5 11 12 13 14 15 16 17 18
L12 L13 L14 L15 L16 L17 L18
F6 19 20 21 22 23 24 25 26 27 28 29 30
L20 L21 L22 L23 L24 L25 L26 L27 L30
F7 31 32 33 34 35 36 37
L31 L32 L33 L34 L35 L36 L37
F8 38 39 40 41 42 43 44 45
L38 L40 L41 L43 L44 L45
F9 46 47 48 49 50 51 52 53 54 55 56 57
L46 L47 L49 L50 L51 L52 L53 L54 L55 L56 L57
F10 58 59 60 61
L60
62
1
F12 63 64 65 66 67 68 69 70 71 72 73 74
L64 L65 L67 L70 L72 L74
F13 75
F14 76 77 78 79 80 81 82
L77 L78 L79 L81
F15 83 84 85 86 87 88
L83 L84 L85 L86 L87 L88
89 90 91
L89 L90 L91
92 93 94
L92 L93 L94
F18 95 96 97 98 99 100
L95 L96 L97 L98 L99 L100
F19 101 102 103 104 105 106 107 108 109
L101 L102 L103 L105 L106 L107 L109
F20 110 111 112 113 114 115 116
L110 L111 L112 L113 L114 L115 L116
F21 117 118 119 120 121 122 123 124 125 126 127 128
L117 L118 L119 L120 L121 L122 L123 L125 L126 L128
F22 129 130 131 132
L130 L131 L132
F23 133 134 135 136 137 138
L133 L135 L137
F24 139 140 141 142 143 144 145 146 147 148 149 150 151
L141 L142 L144 L145 L146 L147 L148 L149 L150 L151

FIGURE 8. Single line diagram of MV distribution network.

on nominal bus voltage), and active power flow (in MW) are collected. These are then used to determine the delta between base and cyber attack scenario.

A. STATISTICAL SPREAD

Figure 9 shows the change in active power flow for buses on feeder 9 (see Figure 8). The figure is used to visualize the statistical spread in the results. Each observation in the box-plot represents one iteration of a cyber attack event compared to the base simulation for that datetime. In other words, the ΔP is formed by the combined loads of the affected CPs connected to the bus number on the x-axis. The ΔV is calculated by subtracting the bus voltage under cyber attack from the bus voltage in the base case. The reason there are box and whiskers is due to the probabilistic nature of the EV charging behaviour model and repeated simulation iterations. It can be concluded that the statistical spread is smaller for buses with fewer connected CPs. This is to be expected, due to the stochastic nature of EV arrival at CPs. More connected EVs will result in a higher difference in active load due to a cyber attack. The differences in the number of CPs connected to each bus bar, notably between

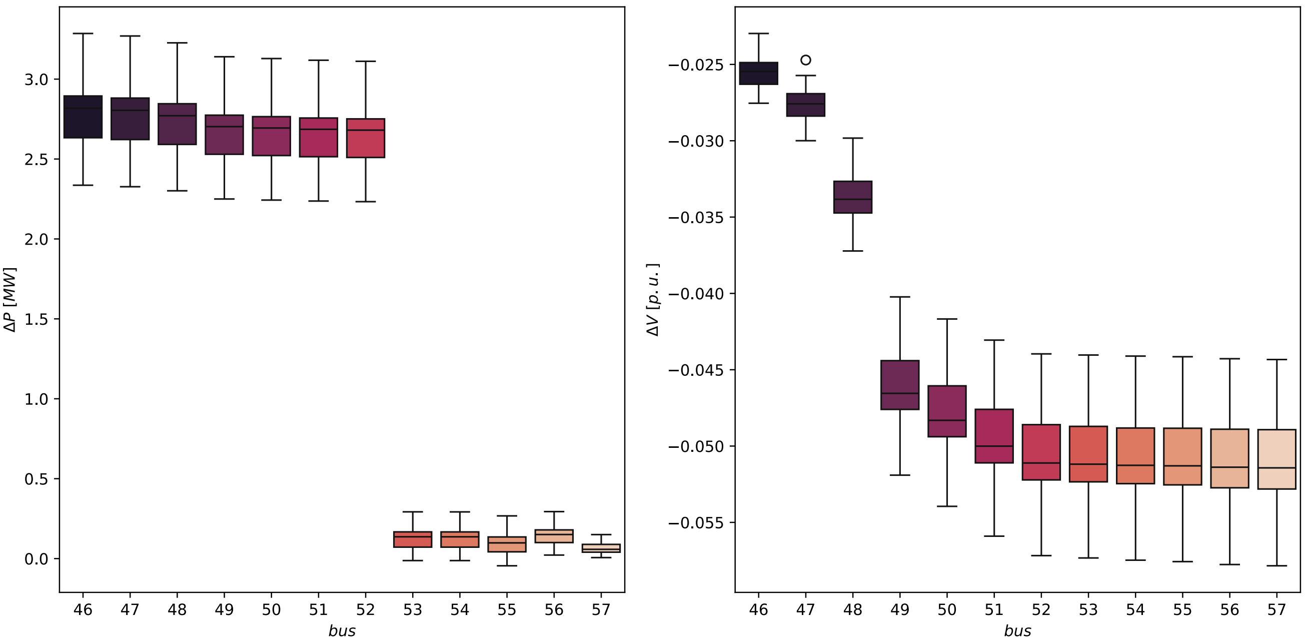
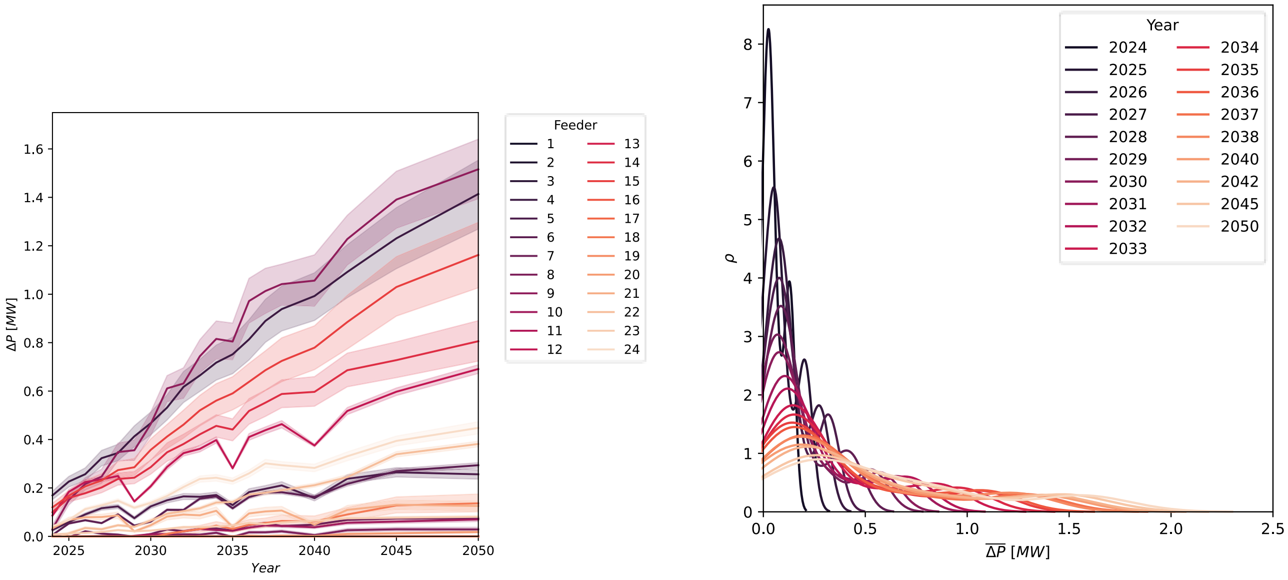


FIGURE 9. Box plot of difference in active power flow [MW]and voltage [p.u.] in feeder 9 (F9) for 2050 at 8:45.



(a) Per feeder

(b) Kernel density plot of yearly increase over all buses

FIGURE 10. Yearly increase of affected load (a) per feeder (b) over allbuses in the MV network.

the two groups 46-52 and 53-57, can be explained by the expected adoption of electric mobility. For instance, it may be that buses 46-52 feed a higher-income demographic area or business park, while buses 53-57 cover less densely populated or developed areas, or areas with fewer possibilities for installing new grid connections c.q. CPs.

B. IMPACT ANALYSIS

Due to the expected accelerated adoption of electric mobility, the affected load by a possible cyber attack is set to increase. This is shown in Figure 10. In (a) the yearly increase in affected load is shown per feeder. The statistical spread, indicated by the shaded area around the different line plots, is caused by differences in the number of connected CPs per feeder bus. A bigger shaded area may mean large deviations in the number of connected CP per bus, or a smaller number of buses in the feeder, resulting in a bigger spread. Overall the impact of possible cyber attacks is shown to increase over the years. Cumulatively, the maximum load altered approximates 16 MW towards 2050. The resulting voltage

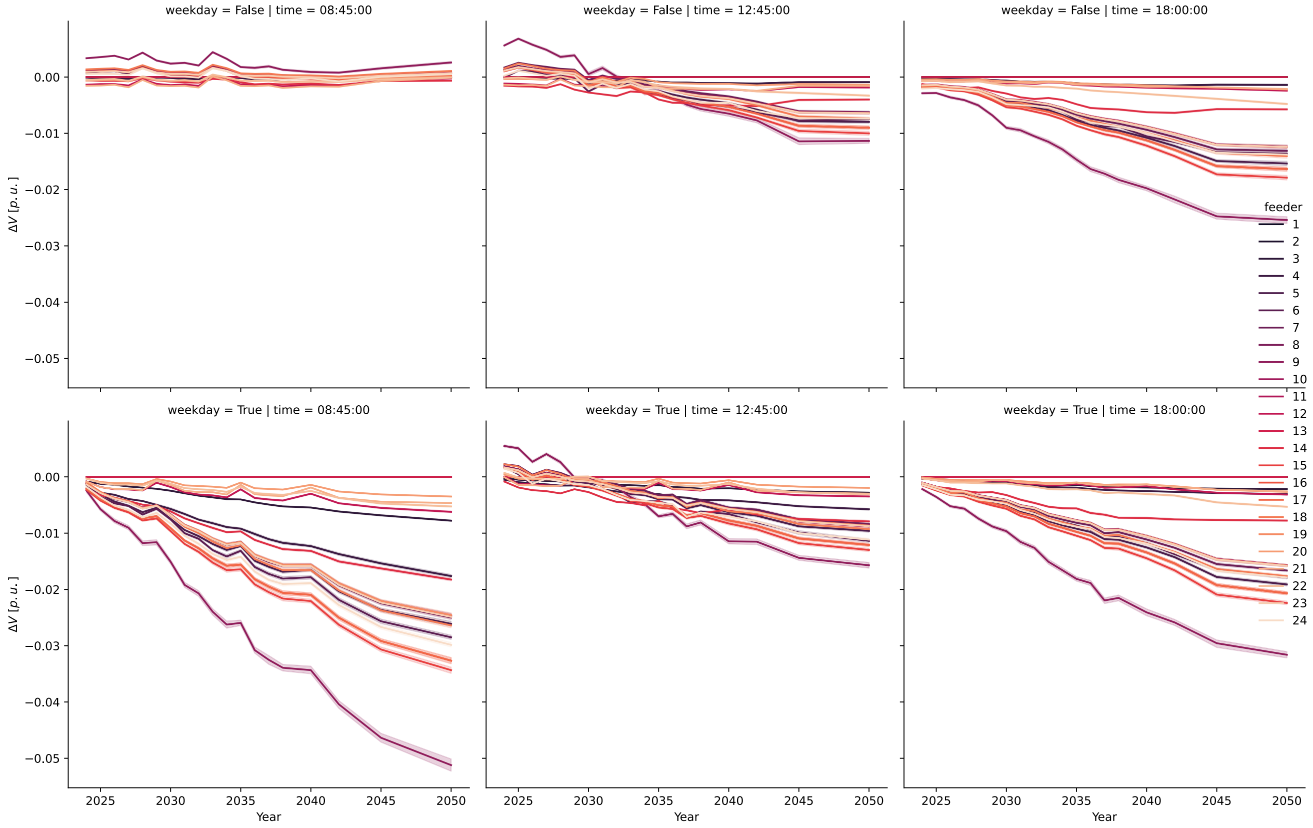


FIGURE 11. Impact of cyber attacks over the years, split by time of the attack and week/weekend.

drop at the end of the feeder approximates 0.05 p.u. (see Figure 9). In Figure 10(b) the kernel density plot (KDE) shows the distribution of delta P, averaged over all buses, per year. A KDE may be used to show smoothened PDFs, for instance by smoothening out a histogram. In this case they are used to visualise the relative occurrence of the sum of affected load by the cyber attack. Namely, affected load is stochastic and continuous. A simple histogram would show it discretised and incur loss of information. Furthermore, a KDE is used to show the stochasticity over a large number of buses and iterations. The affected load is evident from the figure. Namely, while a sharp peak around 0.1 MW is visible for the first years, the peak decreases over the years, giving way to a slightly smaller, but more impactful peak around 1.5 MW. Conclusively, over the years the absolute impact per bus will increase. It should be noted that in the construction of this figure, buses with few or no connected CPs (also visible as feeders in the bottom of Figure 10(a)) are ignored. These skewed the graph towards 0, drawing away attention from the main conclusion: how impact will grow over the years. Moreover, KDE plots apply a smoothening function, resulting in negative values (not shown in the figure). It should be noted that the true negative ΔP were non-present or negligible. In Figure 11 the effects are visible separately for weekends (top) and weekdays (bottom).

In radially operated distribution networks, it is expected that voltages drop along the line. This is a result of resistance and reactance of the cables as well as the loads in the network, in line with Ohm's law. This is evident from Figure 9, where voltages drop along feeder 9. Even though the affected load is lowest at the end of the feeder, ΔV is biggest. Because of this, the impact of cyber attacks is addressed by looking at the final bus in each feeder. This concept is applied in Figure 10. It shows how the impact of the cyber attack will develop over the years. Each line plot shows how the voltage is affected at the last bus in each feeder in Figure 10a. The rows distinguish between week- and weekend days, while the columns show the different times of the simulated cyber attack. Curves in the different plots may appear less smooth. This is because of lower number of CPs, increasing the effect of stochasticity. Plots tend to smooth out towards 2050, as the number of CPs increases.

Large differences are seen between cyber attack times and day of the week. Overall the effects of a potential cyber attack in this specific distribution grid will be biggest during the week in the morning. This is because the grid is dominated by work-related charging. This is even more apparent from Figure 12. A sharp peak can be seen on weekdays at the beginning of the work day (8:45). While the public charging peak at the beginning of the evening (18:00) is much less pronounced.

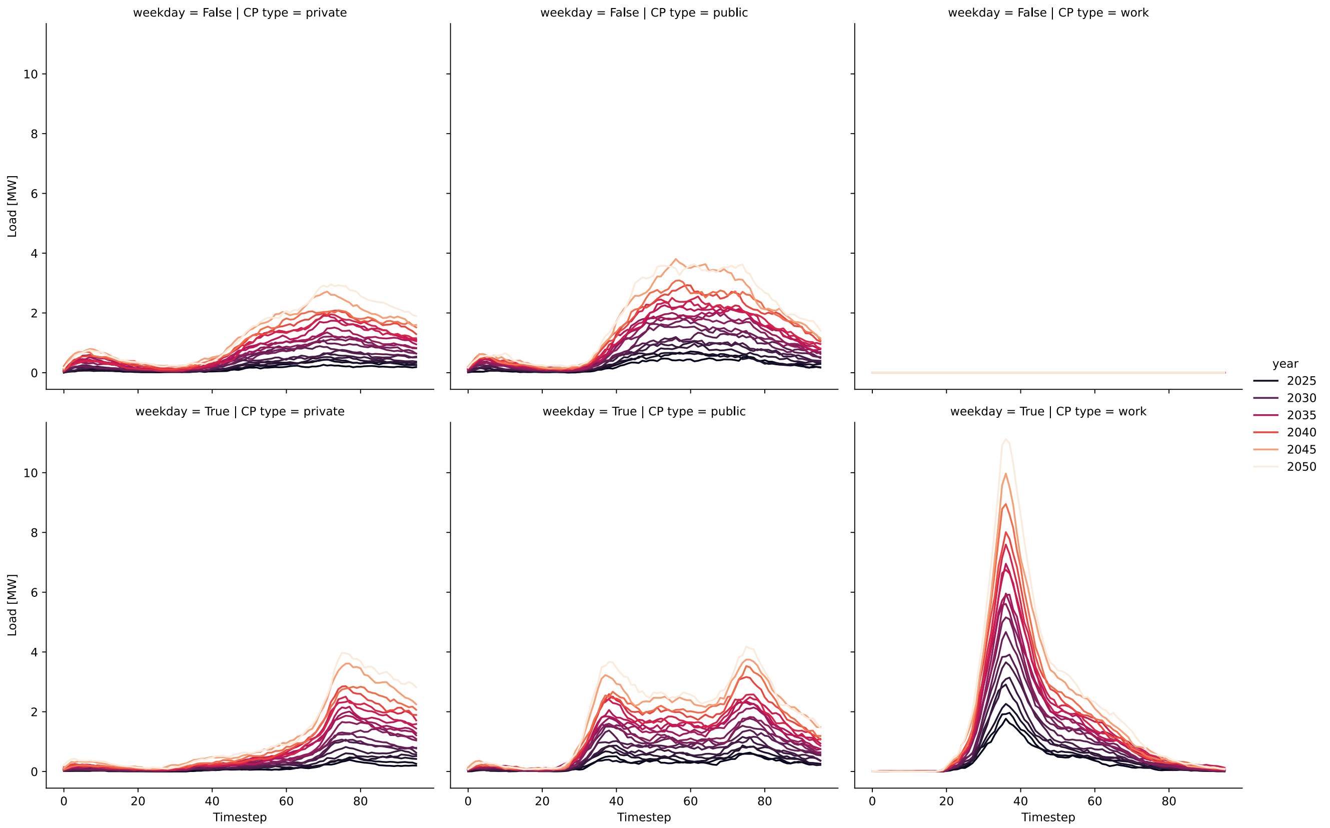


FIGURE 12. Single iterations over years of load related to EV-charging.

C. DISCUSSION AND FUTURE WORK

In general the effects of this type of cyber attack seems to be limited on voltage levels in this specific distribution grids. Even considering the worst-case scenario, a cyber attack covering the entire EVCI would not incur unstable grid operation. This is most likely due to the highly stochastic behaviour of EV users, which is also visible in Figure 9 as the length of boxes and whiskers. While the number of CPs drastically increases, the maximum occupancy remains relatively low. It is assumed that charging behaviour will not drastically change over time [220]. Therefore, this behaviour may be expected in the future scenarios. From the simulations we conclude that no significant impact may arise for this specific MV distribution grid. However, several opportunities for future research have presented themselves:

- The effect of cyber attacks on other MV distribution grids.
- As the cyber attack crosses network and even country borders, the aggregated effect of multiple MV distribution grids on HV distribution grids or even transmission grids.
- The current study was conducted using quasi dynamic simulations, thus showing the steady state response. A study towards dynamic behaviour, for instance in combination with different inverter-based DERs, is crucial for a deeper understanding of the impact.
- Different combinations of grid conditions and cyber attacks may be possible. For instance the effect of a cyber attack on a grid with congestion. The grid already under stress may exhibit a much larger impact due to an cyber attack. On top of that, different DERs, such as rooftop PV may influence the impact both positively and negatively (from a power system stability perspective).

VIII. CONCLUSION

In this survey paper we addressed a combination of two topics: cyber security in electric vehicle charging infrastructure (EVCI) and power system (cyber) resilience. We conclude that numerous vulnerabilities are present in both physical and digital systems of electric vehicles (EVs), charge points (CPs) and related systems – for instance CP management systems (CPMSs). The existing vulnerabilities may lead to cyber attacks on significant portions of the infrastructure. Considering the physical interdependency, cyber attacks on EVCI may have a profound effect on power systems. From our survey on power system resilience we conclude the latter has not been thoroughly addressed. Therefore we have presented a method to model stochastic EV charging behaviour to analyse the impact a cyber attack on EVCI may have on a MV distribution grid. We show that although the effects may not be severe in static analysis, much is unknown about dynamic responses. Therefore we propose directions for future research into combinations of EVCI cyber attacks and power system resilience.

REFERENCES

[1] N. Refa, D. Hammer, and J. van Rookhuijzen. (2021). *Elektrisch Rijden in Stroomversnelling; Elektrificatie Van Personenauto's Tot 2050*. ElaadNL. [Online]. Available: https://www.elaad.nl/uploads/files/2021Q3_Elaad_Outlook_Personenautos_2050.pdf

[2] S. Acharya, Y. Dvorkin, H. Pandžic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[3] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[4] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[5] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[6] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[7] 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.

[8] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging," *IEEE Trans. Ind. Electron.*, vol. 68, no. 1, pp. 478–487, Jan. 2021.

[9] 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, Nov. 2018.

[10] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP protocol: Security threats and challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2452–2459, Sep. 2017.

[11] 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*, vol. 12, no. 5, pp. 4377–4388, Sep. 2021.

[12] M. Panteli and P. Mancarella, "Modelling and evaluating the resilience of critical electrical power infrastructure to extreme weather events," *IEEE Syst. J.*, vol. 11, pp. 1733–1742, 2015.

[13] D. Ronanki and H. Karneddi, "Electric vehicle charging infrastructure: Review, cyber security considerations, potential impacts, countermeasures, and future trends," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 12, no. 1, pp. 242–256, Feb. 2024.

[14] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP)," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1504–1533, 3rd Quart., 2022.

[15] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, "Electric vehicle attack impact on power grid operation," *Int. J. Electr. Power Energy Syst.*, vol. 137, May 2022, Art. no. 107784, doi: 10.1016/J.IJEPES.2021.107784.

[16] S. Shirvani, Y. Baseri, and A. Ghorbani, "Evaluation framework for electric vehicle security risk assessment," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 1, pp. 33–56, Jan. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10247152/

[17] V. S. R. Tappeta, B. Appasani, S. Patnaik, and T. S. Ustun, "A review on emerging communication and computational technologies for increased use of plug-in electric vehicles," *Energies*, vol. 15, no. 18, p. 6580, Sep. 2022.

[18] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6695–6709, Dec. 2023.

[19] N. Bhusal, M. Abdelmalak, M. Kamruzzaman, and M. Benidris, "Power system resilience: Current practices, challenges, and future directions," *IEEE Access*, vol. 8, pp. 18064–18086, 2020.

[20] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266, Jul. 2017.

[21] B. Chen, J. Wang, X. Lu, C. Chen, and S. Zhao, "Networked microgrids for grid resilience, robustness, and efficiency: A review," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 18–32, Jan. 2021.

[22] M. Hamidieh and M. Ghassemi, "Microgrids and resilience: A review," *IEEE Access*, vol. 10, pp. 106059–106080, 2022.

[23] M. Mahzarnia, M. P. Moghaddam, P. T. Baboli, and P. Siano, "A review of the measures to enhance power systems resilience," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4059–4070, Sep. 2020.

[24] F. Mujjuni, T. R. Betts, and R. E. Blanchard, "Evaluation of power systems resilience to extreme weather events: A review of methods and assumptions," *IEEE Access*, vol. 11, pp. 87279–87296, 2023.

[25] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access*, vol. 8, pp. 87592–87608, 2020.

[26] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley, and J. Barnett, "On vulnerability and resilience of cyber-physical power systems: A review," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2367–2378, Jun. 2022.

[27] A. Serrano-Fontova, H. Li, Z. Liao, M. R. Jamieson, R. Serrano, A. Parisio, and M. Panteli, "A comprehensive review and comparison of the fragility curves used for resilience assessments in power systems," *IEEE Access*, vol. 11, pp. 108050–108067, 2023.

[28] V. B. Venkateswaran, D. K. Saini, and M. Sharma, "Approaches for optimal planning of energy storage units in distribution network and their impacts on system resiliency," *CSEE J. Power Energy Syst.*, vol. 6, no. 4, pp. 816–833, Dec. 2020.

[29] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1604–1613, Mar. 2016.

[30] S. Acharya, H. A. U. Khan, R. Karri, and Y. Dvorkin, "MaDEVIoT: Cyberattacks on EV charging can disrupt power grid operation," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2024, pp. 1–5.

[31] U. D. Department of Energy. *Alternative Fueling Station Locator*. Accessed: May 28, 2024. [Online]. Available: https://tinyurl.com/3hnm3xby

[32] S. R. Fahim, R. Atat, C. Keçeci, A. Takiddin, M. Ismail, K. Davis, and E. Serpedin, "Graph autoencoder-based power attacks detection for resilient electrified transportation systems," *IEEE Trans. Transport. Electrific.*, vol. 10, no. 4, pp. 9539–9553, Jan. 2024.

[33] G. Benysek and M. Jarnut, "Electric vehicle charging infrastructure in Poland," *Renew. Sustain. Energy Rev.*, vol. 16, no. 1, pp. 320–328, Jan. 2012, doi: 10.1016/j.rser.2011.07.158.

[34] P. Rademakers and P. Klapwijk. (2017). *Ev Related Protocol Study*. ElaadNL. [Online]. Available: https://www.elaad.nl/research/ev-related-protocol-study/

[35] (2021). *Wetsvoorstel Energiewet—Versie Uht (17, Nov. 2021) Conceptvoorstel*. [Online]. Available: https://www.rijksoverheid.nl/documenten/publicaties/2021/11/26/wetsvoorstel-energiewet-uht

[36] R. voor Ondernemend Nederland. (2021). *Laden Van Elektrische Voertuigen; Definities En Toelichting*. [Online]. Available: https://www.rvo.nl/sites/default/files/2021/06/LadenvanElektrischeVoertuigen-DefinitiesenToelichtingjanuari2021.pdf

[37] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Trans. Ind. Informat.*, vol. 7, no. 3, pp. 381–388, Aug. 2011.

[38] J. M. Carrasco, L. G. Franquelo, J. T. Bialasiewicz, E. Galvan, R. C. PortilloGuisado, M. A. M. Prats, J. I. Leon, and N. Moreno-Alfonso, "Power-electronic systems for the grid integration of renewable energy sources: A survey," *IEEE Trans. Ind. Electron.*, vol. 53, no. 4, pp. 1002–1016, Jun. 2006.

[39] ElaadNL and E. N. Cyber Security. (2019). *Security Architecture for Electric Vehicle Charging Infrastructure*. [Online]. Available: https://encs.eu/documents

[40] M. van Eekelen, E. Poll, E. Hubbers, B. Vieira, and F. van den Broek, "An end-to-end security design for smart ev-charging for enexis and elaadnl," ElaadNL, Arnhem, The Netherlands, 2014.

[41] S. Gopacs. *Hoe Werkt Gopacs?*. Accessed: Jan. 30, 2024. [Online]. Available: https://www.gopacs.eu/hoe-werkt-gopacs/

[42] Shapeshifter. *UFTP*. Accessed: Jan. 30, 2024. [Online]. Available: https://github.com/shapeshifter/shapeshifter-specification

[43] Equigy. (2020). *A Multi-tso Initiative to Catalyse the Cost-effective Use of Balancing Potential Provided By Flexible Distributed Energy Resources*. Accessed: Feb. 13, 2024. [Online]. Available: https://equigy.com/

[44] Open Charge Alliance. *OSCP 1.0, Protocols, Home—Open Charge Alliance*. Accessed: Jul. 22, 2021. [Online]. Available: https://www.openchargealliance.org/protocols/oscp-10/

[45] GreenFlux. *Learn About Charging Protocols OCPI, OCPP and OSCP—Greenflux*. Accessed: Jul. 22, 2021. [Online]. Available: https://www.greenflux.com/spotlights/open-protocols/

[46] Open Charge Alliance. *Downloads—Open Charge Alliance*. Accessed: Jul. 22, 2021. [Online]. Available: https://www.openchargealliance.org/downloads/

[47] *Openadr 2.0—Profile Specification B Profile*, OpenADR Alliance, San Ramon, CA, USA, 2015.

[48] OpenADR Alliance. *Openadr—Product Database*. Accessed: Jul. 22, 2021. [Online]. Available: https://products.openadr.org/

[49] IEEE Standards Association. *IEEE 2030.5-2018—IEEE Standard for Smart Energy Profile Application Protocol*. Accessed: Jul. 28, 2021. [Online]. Available: https://standards.ieee.org/standard/2030_5-2018.html

[50] International Electrotechnical Commission. *IEC TR 61850-90-8:2016 | IEC Webstore | LVDC*. Accessed: Jul. 28, 2021. [Online]. Available: https://webstore.iec.ch/publication/24475

[51] ElaadNL Smartlabs. *Open Clearing House Protocol (OCHP) | The Free International Standard for E-Mobility Interoperability*. Accessed: Feb. 2, 2024. [Online]. Available: https://www.ochp.eu/

[52] M. van der Kam and R. Bekkers, "Mobility in the smart grid: Roaming protocols for EV charging," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 810–822, Jan. 2023.

[53] ElaadNL. *Interoperability, Research—Elaad NL*. Accessed: Jul. 22, 2021. [Online]. Available: https://www.elaad.nl/research/interoperability/

[54] E. Foundation. *OCPI Downloads | Evroaming Foundation*. Accessed: Jul. 28, 2021. [Online]. Available: https://evroaming.org/downloads/

[55] *Emip Protocol Implementation Guide*, GIREVE, Sèvres, France, 2019.

[56] Hubject. *Hubject/oicp: Open Intercharge Protocol*. Accessed: Feb. 2, 2024. [Online]. Available: https://github.com/hubject/oicp/tree/master

[57] Open Charge Alliance. *Ocpp 2.0.1, Protocols, Home—Open Charge Alliance*. Accessed: Jul. 22, 2021. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/

[58] *OCPP 2.0.1 Part 0—Introduction*, Open Charge Alliance, Arnhem, The Netherlands, 2020.

[59] *IEC Webstore*, Standard IEC 63110-1:2022, I. E. Commission, 2022. [Online]. Available: https://webstore.iec.ch/publication/60000

[60] *IEC Webstore*, IEC Standard 61851-1:2017, 2017. [Online]. Available: https://webstore.iec.ch/publication/33644

[61] *Road vehicles—Vehicle to grid communication interface—Part 1: General information and use-case definition*, ISO Standard 15118-1:2019, 2019. [Online]. Available: https://www.iso.org/standard/69113.html

[62] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern.-A, Syst. Hum.*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[63] T. M. Overman, R. W. Sackman, T. L. Davis, and B. S. Cohen, "High-assurance smart grid: A three-part model for smart grid control systems," *Proc. IEEE*, vol. 99, no. 6, pp. 1046–1062, Jun. 2011.

[64] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[65] M. Wen, S. Chen, R. Lu, B. Li, and S. Chen, "Security and efficiency enhanced revocable access control for fog-based smart grid system," *IEEE Access*, vol. 7, pp. 137968–137981, 2019.

[66] A. Sundararajan, T. Khan, A. Moghadasi, and A. I. Sarwat, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *J. Modern Power Syst. Clean Energy*, vol. 7, no. 3, pp. 449–467, May 2019.

[67] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," *IEEE Access*, vol. 8, pp. 177447–177470, 2020.

[68] X. Liu, J. Ospina, and C. Konstantinou, "Deep reinforcement learning for cybersecurity assessment of wind integrated power systems," *IEEE Access*, vol. 8, pp. 208378–208394, 2020.

[69] T. S. Ustun and S. M. S. Hussain, "An improved security scheme for IEC 61850 MMS messages in intelligent substation communication networks," *J. Modern Power Syst. Clean Energy*, vol. 8, no. 3, pp. 591–595, May 2020.

[70] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1942–1976, 3rd Quart., 2020.

[71] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021.

[72] A. Pal, A. Jolfaei, and K. Kant, "A fast prekeying-based integrity protection for smart grid communications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5751–5758, Aug. 2021.

[73] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[74] S. M. Farooq, S. M. S. Hussain, T. S. Ustun, and A. Iqbal, "Using ID-based authentication and key agreement mechanism for securing communication in advanced metering infrastructure," *IEEE Access*, vol. 8, pp. 210503–210512, 2020.

[75] Y. M. Khaw, A. A. Jahromi, M. F. M. Arani, S. Sanner, D. Kundur, and M. Kassouf, "A deep learning-based cyberattack detection system for transmission protective relays," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2554–2565, May 2021.

[76] D. Mashima, P. Gunathilaka, and B. Chen, "Artificial command delaying for secure substation remote control: Design and implementation," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 471–482, Jan. 2019.

[77] C.-C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021.

[78] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat, and B. Kroposki, "A multidimensional holistic framework for the security of distributed energy and control systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 17–27, Mar. 2020.

[79] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 886–899, Mar. 2018.

[80] V. K. Singh and M. Govindarasu, "A cyber-physical anomaly detection for wide-area protection using machine learning," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3514–3526, Jul. 2021.

[81] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[82] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5405–5415, Sep. 2019.

[83] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1092–1102, Jun. 2014.

[84] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020.

[85] S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: Applications and challenges," *IEEE Access*, vol. 9, pp. 50961–50981, 2021.

[86] S. Acharya, Y. Dvorkin, and R. Karri, "Causative cyberattacks on online learning-based automated demand response systems," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3548–3559, Jul. 2021.

[87] D. K. Molzahn and J. Wang, "Detection and characterization of intrusions to network parameter data in electric power systems," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3919–3928, Jul. 2019.

[88] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[89] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[90] T. S. Sreeram and S. Krishna, "Managing false data injection attacks during contingency of secured meters," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6945–6953, Nov. 2019.

[91] A. Abusorrah, A. Alabdulwahab, Z. Li, and M. Shahidehpour, "Minimax-regret robust defensive strategy against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2068–2079, Mar. 2019.

[92] H. E. Brown and C. L. Demarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5854–5866, Nov. 2018.

[93] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.

[94] P. Lau, W. Wei, L. Wang, Z. Liu, and C.-W. Ten, "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4403–4414, Sep. 2020.

[95] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[96] T. G. Machado, A. A. Mota, L. T. M. Mota, M. F. H. Carvalho, and C. C. Pezzuto, "Methodology for identifying the cybersecurity maturity level of smart grids," *IEEE Latin Amer. Trans.*, vol. 14, no. 11, pp. 4512–4519, Nov. 2016.

[97] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting stuxnet-like attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020.

[98] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707–1721, Jul. 2015.

[99] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[100] S. Ahmad, I. Raza, M. H. Jamal, S. Djuraev, S. Hur, and I. Ashraf, "Central aggregator intrusion detection system for denial of service attacks," *Comput., Mater. Continua*, vol. 74, no. 2, pp. 2363–2377, 2023.

[101] S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, "Deep transfer learning based intrusion detection system for electric vehicular networks," *Sensors*, vol. 21, no. 14, p. 4736, Jul. 2021.

[102] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf, and D. Kundur, "A survey on cyber-physical security of active distribution networks in smart grids," *IEEE Access*, vol. 12, pp. 29414–29444, 2024.

[103] M. Bharathidasan, V. Indragandhi, V. Suresh, M. Jasiński, and Z. Leonowicz, "A review on electric vehicle: Technologies, energy trading, and cyber security," *Energy Rep.*, vol. 8, pp. 9662–9685, Nov. 2022, doi: 10.1016/j.egyr.2022.07.145.

[104] R. Aghapour, M. Zeraati, F. Jabari, M. Sheibani, and H. Arasteh, *Cybersecurity and Data Privacy Issues of Electric Vehicles Smart Charging in Smart Microgrids*. Cham, Switzerland: Springer, 2022, pp. 85–110, doi: 10.1007/978-3-031-05909-4_4.

[105] S. Abedi, A. Arvani, and R. Jamalzadeh, *Cyber Security of Plug-in Electric Vehicles in Smart Grids: Application of Intrusion Detection Methods*. Singapore: Springer, 2015, pp. 129–147, doi: 10.1007/978-981-287-299-9.

[106] P. Razmjoui, A. Kavousi-Fard, T. Jin, M. Dabbaghjamanesh, M. Karimi, and A. Jolfaei, "A blockchain-based mutual authentication method to secure the electric vehicles' TPMS," *IEEE Trans. Ind. Informat.*, vol. 20, no. 1, pp. 158–168, Jan. 2023.

[107] J. Yi, H. An, Y. Xing, J. Li, G. Zhang, O. Bamisile, K. Yang, and Y. Xu, "A cyber attack detection strategy for plug-in electric vehicles during charging based on CEEMDAN and broad learning system," *Energy Rep.*, vol. 9, pp. 80–88, May 2023, doi: 10.1016/j.egyr.2022.12.094.

[108] A. Kavousi-Fard, T. Jin, W. Su, and N. Parsa, "An effective anomaly detection model for securing communications in electric vehicles," *IEEE Trans. Ind. Appl.*, vol. 9994, pp. 1–1, 2020.

[109] O. Avatefipour, A. S. Al-Sumaiti, A. M. El-Sherbeeny, E. M. Awwad, M. A. Elmeligy, M. A. Mohamed, and H. Malik, "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning," *IEEE Access*, vol. 7, pp. 127580–127592, 2019.

[110] V. S. R. Kosuru and A. K. Venkitaraman, "A smart battery management system for electric vehicles using deep learning-based sensor fault detection," *World Electr. Vehicle J.*, vol. 14, no. 4, p. 101, Apr. 2023.

[111] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 3, pp. 2010–2022, Sep. 2021.

[112] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber-physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.

[113] U. Bazazi and S. N. Ravadanegh, *Evaluation of Cyberattacks in Distribution Network With Electric Vehicle Charging Infrastructure*. Cham, Switzerland: Springer, 2022, pp. 111–128, doi: 10.1007/978-3-031-05909-4_5.

[114] S. I. Jeong and D.-H. Choi, "Electric vehicle user data-induced cyber attack on electric vehicle charging station," *IEEE Access*, vol. 10, pp. 55856–55867, 2022.

[115] M. Ali, G. Kaddoum, W.-T. Li, C. Yuen, M. Tariq, and H. V. Poor, "A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5258–5271, 2023.

[116] M. Mohammadi and J. B. Mohasefi, "Availability-based and risk-less optimization model for electric vehicles optimal itinerary planning in smart grid," *Sustain. Energy, Grids Netw.*, vol. 30, Jun. 2022, Art. no. 100642, doi: 10.1016/j.segan.2022.100642.

[117] H. Feng, R. Tavakoli, O. C. Onar, and Z. Pantic, "Advances in high-power wireless charging systems: Overview and design considerations," *IEEE Trans. Transport. Electrific.*, vol. 6, no. 3, pp. 886–919, Sep. 2020.

[118] A. C.-F. Chan and J. Zhou, "Cyber-physical device authentication for the smart grid electric vehicle ecosystem," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1509–1517, Jul. 2014.

[119] A. C.-F. Chan and J. Zhou, "A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 3367–3376, Dec. 2015.

[120] S. Islam, S. Badsha, S. Sengupta, I. Khalil, and M. Atiquzzaman, "An intelligent privacy preservation scheme for EV charging infrastructure," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1238–1247, Feb. 2023.

[121] S. Acharya, R. Mieth, C. Konstantinou, R. Karri, and Y. Dvorkin, "Cyber insurance against cyberattacks on electric vehicle charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1529–1541, Mar. 2022.

[122] Z. S. Warraich and W. G. Morsi, "Early detection of cyber-physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids," *Sustain. Energy, Grids Netw.*, vol. 34, Jun. 2023, Art. no. 101027, doi: 10.1016/j.segan.2023.101027.

[123] M. Girdhar, J. Hong, H. Lee, and T.-J. Song, "Hidden Markov models-based anomaly correlations for the cyber-physical security of EV charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3903–3914, Sep. 2022.

[124] N. Moghadasi, Z. A. Collier, A. Koch, D. L. Slutzky, T. L. Polmateer, M. C. Manasco, and J. H. Lambert, "Trust and security of electric vehicle-to-grid systems and hardware supply chains," *Rel. Eng. Syst. Saf.*, vol. 225, Sep. 2022, Art. no. 108565, doi: 10.1016/j.ress.2022.108565.

[125] K. Sarieddine, M. A. Sayed, D. Jafarigiv, R. Atallah, M. Debbabi, and C. Assi, "A real-time cosimulation testbed for electric vehicle charging and smart grid security," *IEEE Secur. Privacy*, vol. 21, no. 4, pp. 74–83, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10064175/

[126] P. Li, W. Ou, H. Liang, W. Han, Q. Zhang, and G. Zeng, "A zero trust and blockchain-based defense model for smart electric vehicle chargers," *J. Netw. Comput. Appl.*, vol. 213, Apr. 2023, Art. no. 103599, doi: 10.1016/j.jnca.2023.103599.

[127] T. Z. Nonvignon, A. B. Boucif, and M. Mesfioui, "A copula-based attack prediction model for vehicle-to-grid networks," *Appl. Sci.*, vol. 12, no. 8, p. 3830, Apr. 2022.

[128] M. ElKashlan, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs)," *Electron.*, vol. 12, no. 4, p. 1044, Feb. 2023.

[129] M. Ghafouri, E. Kabir, B. Moussa, and C. Assi, "Coordinated charging and discharging of electric vehicles: A new class of switching attacks," *ACM Trans. Cyber-Phys. Syst.*, vol. 6, no. 3, pp. 1–26, Jul. 2022.

[130] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102511, doi: 10.1016/j.cose.2021.102511.

[131] M. M. Rana, "IoT-based electric vehicle state estimation and control algorithms under cyber attacks," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 874–881, Feb. 2020.

[132] M. Basnet and M. H. Ali, "Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning," *IET Gener., Transmiss. Distrib.*, vol. 15, no. 24, pp. 3435–3449, Aug. 2021.

[133] H. Su, M. Qiu, and H. Wang, "Secure wireless communication system for smart grid with rechargeable electric vehicles," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 62–68, Aug. 2012.

[134] C. Alcaraz, J. Cumplido, and A. Trivinño, "OCPP in the spotlight: Threats and countermeasures for electric vehicle charging infrastructures 4.0," *Int. J. Inf. Secur.*, vol. 22, no. 5, pp. 1395–1421, May 2023. [Online]. Available: https://link.springer.com/10.1007/s10207-023-00698-8

[135] S. M. Farooq, S. M. S. Hussain, S. Kiran, and T. S. Ustun, "Certificate based security mechanisms in vehicular ad-hoc networks based on IEC 61850 and IEEE WAVE standards," *Electronics*, vol. 8, no. 1, p. 96, Jan. 2019.

[136] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack. (2006). *Uncover Security Design Flaws Using the Stride Approach*. MSDN. [Online]. Available: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[137] F. van den Broek, E. Poll, and B. Vieira, "Securing the information infrastructure for EV charging," in *Proc. 7th Int. Conf. Wireless Satell. Syst.*, Jan. 2015, pp. 61–74.

[138] A. Paverd, A. Martin, and I. Brown, *Security and Privacy in Smart Grid Demand Response Systems*, vol. 8448. Cham, Switzerland: Springer, 2014, pp. 1–15. [Online]. Available: https://link.springer.com/10.1007/978-3-319-10329-7_1

[139] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for California's smart inverter functions," in *Proc. IEEE CyberPELS (CyberPELS)*, Apr. 2019, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8925257/

[140] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5," in *Proc. 8th Workshop Model. Simul. Cyber-Phys. Energy Syst. (MSCPES)*, 2020, pp. 1–6.

[141] K. Sarieddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, "Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised EV charging stations," *Int. J. Elect. Power Energy Syst.*, vol. 156, 2024, Art. no. 109735.

[142] J. Schmutzler, C. A. Andersen, and C. Wietfeld, "Evaluation of OCPP and IEC 61850 for smart charging electric vehicles," in *Proc. World Electric Vehicle Symp. Exhib. (EVS27)*, Nov. 2013, pp. 1–12.

[143] C. Lopez, A. Sargolzaei, H. Santana, and C. Huerta, "Smart grid cyber security: An overview of threats and countermeasures," *J. Energy Power Eng.*, vol. 9, no. 7, pp. 632–647, Jul. 2015. [Online]. Available: https://www.researchgate.net/publication/281719657

[144] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2518–2542, 3rd Quart., 2018.

[145] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, J. Zhao, and V. Terzija, "A specialized review on outlook of future cyber-physical power system (CPPS) testbeds for securing electric power grid," *Int. J. Electr. Power Energy Syst.*, vol. 136, Mar. 2022, Art. no. 107720, doi: 10.1016/j.ijepes.2021.107720.

[146] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on cyber-physical power system (cpps) testbeds for secure and sustainable electric power grid—Part-II: Classification, overview and assessment of CPPS testbeds," *Int. J. Electr. Power Energy Syst.*, vol. 137, Apr. 2021, Art. no. 107721.

[147] Stedin. *Open Data*. Accessed: Oct. 5, 2023. [Online]. Available: https://www.stedin.net/zakelijk/open-data

[148] Liander. *Open data*. Accessed: Oct. 5, 2023. [Online]. Available: https://www.liander.nl/partners/datadiensten/open-data

[149] Enexis. *Open data*. Accessed: Oct. 5, 2023. [Online]. Available: https://www.enexis.nl/over-ons/open-data

[150] B. van Duijnhoven, M. van der Meer, and H. Nienhuis. *Hoogspanningsnet Netkaart*. Accessed: Oct. 5, 2023. [Online]. Available: https://webkaart.hoogspanningsnet.com/index2.php#7/53.311/2.499

[151] Inside EVs. (2022). *Russian EV Chargers Hacked, Screen Reads*. Accessed: Apr. 9, 2025. [Online]. Available: https://insideevs.com/news/570958/russia-electric-car-chargers-hacked/

[152] Hackread. (2024). *Zero-day Flaws Exposed EV Chargers to Shutdowns and Data Theft*. Accessed: Apr. 9, 2025. [Online]. Available: https://hackread.com/zero-day-flaws-ev-chargers-to-shutdowns-data-theft/

[153] ElaadNL. (2024). *Hacking EV Charging Stations via the Charging Cable*. Accessed: Apr. 9, 2025. [Online]. Available: https://elaad.nl/en/hacking-ev-charging-stations-via-the-charging-cable/

[154] H. Jahangir, S. Lakshminarayana, and H. V. Poor, "Charge manipulation attacks against smart electric vehicle charging stations and deep learning-based detection mechanisms," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 5182–5194, Sep. 2024.

[155] C. S. Holling, "Resilience and stability of ecological systems," *Annu. Rev. Ecol. Systematics*, vol. 4, no. 1, pp. 1–23, Nov. 1973.

[156] C. S. Holling, *The Resilience of Terrestrial Ecosystems: Local Surprise and Global Change*. Cambridge, U.K.: Cambridge Univ. Press, 1986, pp. 292–316.

[157] C. S. Holling, *Engineering Resilience Versus Ecological Resilience*. Washington, DC, USA: National Academy Press, 1996, pp. 31–44.

[158] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Rel. Eng. Syst. Saf.*, vol. 145, pp. 47–61, Aug. 2015.

[159] R. Bhamra, S. Dani, and K. Burnard, "Resilience: The concept, a literature review and future directions," *Int. J. Prod. Res.*, vol. 49, no. 18, pp. 5375–5393, Sep. 2011.

[160] R. Francis and B. Bekera, "A metric and frameworks for resilience analysis of engineered and infrastructure systems," *Rel. Eng. Syst. Saf.*, vol. 121, pp. 90–103, Jan. 2014, doi: 10.1016/j.ress.2013.07.004.

[161] 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, Sep. 2017.

[162] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and quantification of operational and infrastructure resilience in power systems," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4732–4742, Nov. 2017.

[163] D. A. Reed, K. C. Kapur, and R. D. Christie, "Methodology for assessing the resilience of networked infrastructure," *IEEE Syst. J.*, vol. 3, no. 2, pp. 174–180, Jun. 2009.

[164] M. Ouyang and L. Dueñas-Osorio, "Time-dependent resilience assessment and improvement of urban infrastructure systems," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 22, no. 3, Sep. 2012, Art. no. 033122, doi: 10.1063/1.4737204.

[165] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the power grid resilience to extreme weather events using defensive islanding," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2913–2922, Nov. 2016.

[166] M. Ouyang and L. Dueñas-Osorio, "Multi-dimensional hurricane resilience assessment of electric power systems," *Structural Saf.*, vol. 48, pp. 15–24, May 2014, doi: 10.1016/j.strusafe.2014.01.001.

[167] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthq. Spectra*, vol. 19, no. 4, pp. 733–752, Nov. 2003.

[168] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power systems resilience assessment: Hardening and smart operational enhancement strategies," *Proc. IEEE*, vol. 105, no. 7, pp. 1202–1213, Jul. 2017.

[169] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1552–1564, Mar. 2021.

[170] M. Panteli and P. Mancarella, "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electr. Power Syst. Res.*, vol. 127, pp. 259–270, Oct. 2015.

[171] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience," *IEEE Power Energy Mag.*, vol. 13, no. 3, pp. 58–66, May 2015.

[172] S. Espinoza, M. Panteli, P. Mancarella, and H. Rudnick, "Multi-phase assessment and adaptation of power systems resilience to natural hazards," *Electr. Power Syst. Res.*, vol. 136, pp. 352–361, Jul. 2016, doi: 10.1016/j.epsr.2016.03.019.

[173] G. P. Cimellaro, A. M. Reinhorn, and M. Bruneau, "Framework for analytical quantification of disaster resilience," *Eng. Struct.*, vol. 32, no. 11, pp. 3639–3649, Nov. 2010, doi: 10.1016/j.engstruct.2010.08.008.

[174] C. Ji, Y. Wei, and H. V. Poor, "Resilience of energy infrastructure and services: Modeling, data analytics, and metrics," *Proc. IEEE*, vol. 105, no. 7, pp. 1354–1366, Jul. 2017.

[175] S. Poudel, A. Dubey, and A. Bose, "Risk-based probabilistic quantification of power distribution system operational resilience," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3506–3517, Sep. 2020.

[176] S. Espinoza, A. Poulos, H. Rudnick, J. C. de la Llera, M. Panteli, and P. Mancarella, "Risk and resilience assessment with component criticality ranking of electric power systems subject to earthquakes," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2837–2848, Jun. 2020.

[177] D. Luo, Y. Xia, Y. Zeng, C. Li, B. Zhou, H. Yu, and Q. Wu, "Evaluation method of distribution network resilience focusing on critical loads," *IEEE Access*, vol. 6, pp. 61633–61639, 2018.

[178] S. Chanda, A. K. Srivastava, M. U. Mohanpurkar, and R. Hovsapian, "Quantifying power distribution system resiliency using code-based metric," *IEEE Trans. Ind. Appl.*, vol. 54, no. 4, pp. 3676–3686, Jul. 2018.

[179] C. Lin, F. Liu, L. Zhang, G. Li, C. Chen, and Z. Bie, "An online data-driven risk assessment method for resilient distribution systems," *CPSS Trans. Power Electron. Appl.*, vol. 6, no. 2, pp. 136–144, Jun. 2021.

[180] J. B. Leite, J. R. S. Mantovani, T. Dokic, Q. Yan, P.-C. Chen, and M. Kezunovic, "Resiliency assessment in distribution networks using GIS-based predictive risk analytics," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 4249–4257, Nov. 2019.

[181] R. Nateghi, "Multi-dimensional infrastructure resilience modeling: An application to hurricane-prone electric power distribution systems," *IEEE Access*, vol. 6, pp. 13478–13489, 2018.

[182] N. K. Carrington, I. Dobson, and Z. Wang, "Extracting resilience metrics from distribution utility data using outage and restore process statistics," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5814–5823, Nov. 2021.

[183] R. Ghorani, S. Fattaheian-Dehkordi, M. Farrokhi, M. Fotuhi-Firuzabad, and M. Lehtonen, "Modeling and quantification of power system resilience to natural hazards: A case of landslide," *IEEE Access*, vol. 9, pp. 80300–80309, 2021.

[184] D. Shelar, S. Amin, and I. A. Hiskens, "Evaluating resilience of electricity distribution networks via a modification of generalized benders decomposition method," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 3, pp. 1225–1238, Sep. 2021.

[185] G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, "Integration of preventive and emergency responses for power grid resilience enhancement," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4451–4463, Nov. 2017.

[186] M. A. Mohamed, T. Chen, W. Su, and T. Jin, "Proactive resilience of power systems against natural disasters: A literature review," *IEEE Access*, vol. 7, pp. 163778–163795, 2019.

[187] M. Nazemi, M. Moeini-Aghtaie, M. Fotuhi-Firuzabad, and P. Dehghanian, "Energy storage planning for enhanced resilience of power distribution networks against earthquakes," *IEEE Trans. Sustain. Energy*, vol. 11, no. 2, pp. 795–806, Apr. 2020.

[188] J. Kim and Y. Dvorkin, "Enhancing distribution system resilience with mobile energy storage and microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4996–5006, Sep. 2019.

[189] S. Yao, P. Wang, X. Liu, H. Zhang, and T. Zhao, "Rolling optimization of mobile energy storage fleets for resilient service restoration," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1030–1043, Mar. 2020.

[190] S. Yao, P. Wang, and T. Zhao, "Transportable energy storage for more resilient distribution systems with multiple microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3331–3341, May 2019.

[191] Z. Yang, P. Dehghanian, and M. Nazemi, "Seismic-resilient electric power distribution systems: Harnessing the mobility of power sources," *IEEE Trans. Ind. Appl.*, vol. 56, no. 3, pp. 2304–2313, May 2020.

[192] P. Jamborsalamati, M. J. Hossain, S. Taghizadeh, G. Konstantinou, M. Manbachi, and P. Dehghanian, "Enhancing power grid resilience through an IEC61850-based EV-assisted load restoration," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1799–1810, Mar. 2020.

[193] S. Lei, C. Chen, H. Zhou, and Y. Hou, "Routing and scheduling of mobile power sources for distribution system resilience enhancement," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5650–5662, Sep. 2019.

[194] B. Zhang, P. Dehghanian, and M. Kezunovic, "Optimal allocation of PV generation and battery storage for enhanced resilience," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 535–545, Jan. 2019.

[195] A. Hussain, V.-H. Bui, and H.-M. Kim, "A proactive and survivability-constrained operation strategy for enhancing resilience of microgrids using energy storage system," *IEEE Access*, vol. 6, pp. 75495–75507, 2018.

[196] S. Biswas, M. K. Singh, and V. A. Centeno, "Chance-constrained optimal distribution network partitioning to enhance power grid resilience," *IEEE Access*, vol. 9, pp. 42169–42181, 2021.

[197] M. E. Parast, M. H. Nazari, and S. H. Hosseinian, "Resilience improvement of distribution networks using a two-stage stochastic multi-objective programming via microgrids optimal performance," *IEEE Access*, vol. 9, pp. 102930–102952, 2021.

[198] F. Teymouri, T. Amraee, H. Saberi, and F. Capitanescu, "Toward controlled islanding for enhancing power grid resilience considering frequency stability constraints," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1735–1746, Mar. 2019.

[199] J. Liu, C. Qin, and Y. Yu, "Enhancing distribution system resilience with proactive islanding and RCS-based fast fault isolation and service restoration," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2381–2395, May 2020.

[200] Y. Xu, C.-C. Liu, K. P. Schneider, F. K. Tuffner, and D. T. Ton, "Microgrids for service restoration to critical load in a resilient distribution system," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 426–437, Jan. 2018.

[201] T. Ding, Z. Wang, W. Jia, B. Chen, C. Chen, and M. Shahidehpour, "Multiperiod distribution system restoration with routing repair crews, mobile electric vehicles, and soft-open-point networked microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 4795–4808, Nov. 2020.

[202] L.-J. Yang, Y. Zhao, C. Wang, P. Gao, and J.-H. Hao, "Resilience-oriented hierarchical service restoration in distribution system considering microgrids," *IEEE Access*, vol. 7, pp. 152729–152743, 2019.

[203] A. Kavousi-Fard, M. Wang, and W. Su, "Stochastic resilient post-hurricane power system recovery based on mobile emergency resources and reconfigurable networked microgrids," *IEEE Access*, vol. 6, pp. 72311–72326, 2018.

[204] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 958–966, Mar. 2016.

[205] I. Linkov and A. Kott, *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. Cham, Switzerland: Springer, 2019, pp. 1–25.

[206] F. Bjrck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber resilience fundamentals for a definition," *Adv. Intell. Syst. Comput.*, vol. 353, pp. 311–316, Jun. 2015.

[207] K. Hausken, "Cyber resilience in firms, organizations and societies," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100204, doi: 10.1016/j.iot.2020.100204.

[208] S. Colabianchi, F. Costantino, G. Di Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Comput. Ind. Eng.*, vol. 160, Oct. 2021, Art. no. 107534, doi: 10.1016/j.cie.2021.107534.

[209] S. Ullah, A. J. Abianeh, F. Ferdowsi, K. Basulaiman, and M. Barati, "Measurable challenges in smart grid cybersecurity enhancement: A brief review," in *Proc. IEEE Green Technol. Conf.*, Apr. 2021, pp. 331–338.

[210] P. Zhao, C. Gu, Y. Ding, H. Liu, Y. Bian, and S. Li, "Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks; cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2253–2263, Apr. 2021, doi: 10.1109/TPWRD.2020.3038065.

[211] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Electr. Power Syst. Res.*, vol. 193, Apr. 2021, Art. no. 107024, doi: 10.1016/J.EPSR.2021.107024.

[212] H. T. Nguyen, J. W. Muhs, and M. Parvania, "Assessing impacts of energy storage on resilience of distribution systems against hurricanes," *J. Modern Power Syst. Clean Energy*, vol. 7, no. 4, pp. 731–740, Jul. 2019, doi: 10.1007/s40565-019-0557-y.

[213] D. A. S. Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Comput. Secur.*, vol. 97, Aug. 2020, Art. no. 101996.

[214] M. Barbeau, F. Cuppens, N. Cuppens, R. Dagnas, and J. Garcia-Alfaro, "Resilience estimation of cyber-physical systems via quantitative metrics," *IEEE Access*, vol. 9, pp. 46462–46475, 2021.

[215] H. Davarikia and M. Barati, "A tri-level programming model for attack-resilient control of power grids," *J. Modern Power Syst. Clean Energy*, vol. 6, no. 5, pp. 918–929, Sep. 2018, doi: 10.1007/s40565-018-0436-y.

[216] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.

[217] Q. A. Al-Gburi and M. A. Mohd Ariff, "Dynamic security assessment for power system under cyber-attack," *J. Electr. Eng. Technol.*, vol. 14, no. 2, pp. 549–559, Mar. 2019, doi: 10.1007/s42835-019-00084-2.

[218] ElaadNL. (2020). *ElaadNL Open Datasets for Electric Mobility Research | Update Apr. 2020*. [Online]. Available: https://platform.elaad.io/analyses/index.php?url=ElaadNL_opendata.php

[219] P. S. Kundur and O. P. Malik, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill, 2022. [Online]. Available: https://books.google.nl/books?id=1-WazgEACAAJ

[220] N. Refa, D. Hammer, P. Broos, J. Janssen, P. Markotic, T. Bos, E. van Zanten, T. van Wel, and R. de Croon. (2024). *Elektrisch Rijden Voor Iedereen, Outlook Personenauto's Update 2024*. [Online]. Available: https://elaad.nl/update-elaad-outlook-personenautos-versnelling-groei-elektrische-autos-na-2030-verwacht/

SJORS HIJGENAAR (Student Member, IEEE) received the B.Sc. degree in systems engineering, policy analysis, and management (energy and industry specialization) and the M.Sc. degree in transport, infrastructure, and logistics from Delft University of Technology, Delft, The Netherlands. He is currently an industrial Ph.D. Student with Stedin Netbeheer B.V. and a Dutch DSO with the Department of Electrical Sustainable Energy (Intelligent Electrical Power Grids Group), Delft University of Technology. His main research interests include the cyber resilience of electric vehicle charging infrastructures, cyber security of electric vehicles, and artificial intelligence for distribution network impact assessment.

ALEXANDRU ŞTEFANOV (Member, IEEE) received the M.Sc. degree from the University Politehnica of Bucharest, Romania, in 2011, and the Ph.D. degree from University College Dublin, Ireland, in 2015. He is currently an Associate Professor of intelligent electrical power grids with TU Delft, The Netherlands. He is the Director of the Control Room of the Future (CRoF) Technology Centre. He holds the professional title of a Chartered Engineer from Engineers Ireland. His research interests include the cyber security of power grids, resilience of cyber-physical systems, and next-generation grid operation.

ARJAN M. VAN VOORDEN received the M.Sc. degree from Delft University of Technology, in 1998, and the Ph.D. degree, in 2008. He is currently an Expert in asset management with a main focus on the development of the integral energy system of the future and has been a Research Fellow with the Intelligent Electrical Power Grids Group, Delft University of Technology, since 2022. His research interests include energy system integration and long-term electricity grid planning.

PETER PALENSKY (Senior Member, IEEE) received the M.Sc. degree in electrical engineering, and the Ph.D. and Habilitation degrees from Vienna University of Technology, Austria, in 1997, 2001, and 2015, respectively. He co-founded Envidatec, a German startup on energy management and analytics, and joined the Lawrence Berkeley National Laboratory, Berkeley, CA, USA, as a Researcher, and the University of Pretoria, South Africa, in 2008. In 2009, he was appointed as the Head of the Business Unit on Sustainable Building Technologies, Austrian Institute of Technology (AIT), and a Principal Scientist of complex energy systems with AIT. In 2014, he was appointed as a Full Professor of intelligent electric power grids with TU Delft. His research interests include energy automation networks, smart grids, and modeling intelligent energy systems. He also serves as an IEEE IES AdCom Member-at-Large in various functions for IEEE. He is an active in international committees, such as ISO and CEN. He is also the Editor-in-Chief of *IEEE Industrial Electronics Magazine*, and an associate editor of several other IEEE publications, and regularly organizes IEEE conferences.