smart cities

MDPI

Article

Communication Vulnerabilities in Electric Mobility HCP Systems: A Semi-Quantitative Analysis

Robert Basmadjian

Department of Informatics, Clausthal University of Technology, Julius-Albert-Str. 4, 38678 Clausthal-Zellerfeld, Germany; robert.basmadjian@tu-clausthal.de

Abstract: An electric mobility ecosystem, which resembles a human-centred cyber physical (HCP) system, consists of several interacting sub-systems that constantly communicate with each other. Cyber-security of such systems is an important aspect as vulnerability of one sub-system propagates to the entire system, thus putting it into risk. Risk assessment requires modelling of threats and their impacts on the system. Due to lack of available information on all possible threats of a given system, it is generally more convenient to assess the level of vulnerabilities either qualitatively or semi-quantitatively. In this paper, we adopt the common vulnerability scoring system (CVSS) methodology in order to assess semi-quantitatively the vulnerabilities of the communication in electric mobility human-centred cyber physical systems. To this end, we present the most relevant sub-systems, their roles as well as exchanged information. Furthermore, we give the considered threats and corresponding security requirements. Using the CVSS methodology, we then conduct an analysis of vulnerabilities for every pair of communicating sub-systems. Among them, we show that the sub-systems between charging station operator (CSO) and electric vehicle supply equipment (charging box) as well as CSO and electric mobility service provider are the most vulnerable in the end-to-end chain of electric mobility. These results pave the way to system designers to assess the operational security risks, and hence to take the most adequate decisions, when implementing such electric mobility HCP systems.

Keywords: vulnerability; communication infrastructure; smart cities; electric mobility; sustainable transport; electric vehicles

Citation: Basmadjian, R. Communication Vulnerabilities in Electric Mobility HCP Systems: A Semi-Quantitative Analysis. *Smart Cities* **2021**, *4*, 405–428. https://doi.org/10.3390/smartcities4010023

Academic Editor: Pierluigi Siano

Received: 10 March 2021
Accepted: 18 March 2021
Published: 20 March 2021

1. Introduction

A cyber physical system (CPS) is a collection of sub-systems, which are interconnected with each other by means of information and communications technology (ICT). In [1], the author describes CPSs as the integration of computation and physical processes such that the embedded computers (e.g., information) and networks (e.g., communication) monitor and control those physical processes through feedback loops. In a human-centred cyber physical system (HCPS), human beings (e.g., operators) are involved in certain decision-making. Consequently, there is a mutual dependence of humans and such systems on each other: the system reacts on the human interventions and vice versa. To this end, An electric mobility ecosystem is a typical example of an HCPS, where such a system consists of generally five relevant sub-systems (e.g., actors/stakeholders) of electric vehicles (EV), electric vehicle supply equipment (EVSE), electric mobility service provider (eMSP), charging station operator (CSO) and distribution system operator (DSO) [2,3]. As it can be noticed, in addition to the cyber physical system in place, human beings (e.g., EV drivers, grid or charging station operators) are involved in such a system. This involvement necessitates a constant feedback loop which can be realised thanks to the information commutation and communication between the different sub-systems.

Cyber-security of such HCPS has received considerable attention in the recent years, due to the fact that the vulnerability of one sub-system brings the whole HCPS system

into risk. To this end, several works in the literature targeted analysing the vulnerability of different HCPSs. For instance, it was shown in [4] that the vulnerabilities in the Ukrainian power system allowed attackers to exploit them. Furthermore, as DSO and CSO sub-systems are interconnected, then CSOs could also become the target of cyber attackers. Hence, by gaining control to the CSO's infrastructure, it would be possible to manipulate the power station connected to the corresponding charging station. This could lead to imbalance in the power demand and supply, and hence endangers the stability of the power system, which then causes power outages. The impact would be even greater when for example smart charging solutions are in place at the charging station: cyber attackers could compel those charging stations to use more power than reserved to them, which could damage transformers and feeder lines (e.g., a sort of denial of service attacks). In [5], the authors investigated and reviewed the cyber-security attacks, counter measures, and challenges of the communication protocols used within the context of human-centred cyber physical systems (e.g., SCADA). They showed that several vulnerabilities present in SCADA systems were exploited successfully, such as the attacks carried in 2008 on the public tram system in Lodz (Poland), and in 2000 on the Maroochy Water Services (Australia).

To assess the level of risk present in such HCPSs, the underlying risk needs to be modelled. However, modelling risk is a complex and tedious process. Basically, accepted risk models involve some basic concepts such as assets, threats (e.g., damaging events putting assets in danger), impacts (e.g., the potential outcome of threats causing damage to the assets) and vulnerabilities (e.g., weaknesses of the system allowing threats to exploit assets, and causing impacts). For risk assessment, analysing the threats quantitatively is unrealistic for most systems. This is because in most cases access to important and security-relevant information is not available. As a matter of fact, assessing the vulnerabilities and the associated impact is far more simpler and realistic, since those are within the control of system operators and designers [6]. Thus, risk assessment methodologies in human-centred cyber physical systems focus on assessing these aspects (e.g., vulnerabilities and impacts), usually qualitatively (e.g., low, medium, high) or semi-quantitatively (e.g., score range between 0 and 10). Furthermore, each pair of communicating entities has its own particular threats and vulnerabilities, and the corresponding impact(s) on the system. Those need to be analysed and assessed separately, so that the end-to-end security of the whole human-centred cyber physical systems can be addressed adequately.

Given the importance and relevance of the topic, in this paper we study semi-quantitatively the vulnerabilities on the communicating entities within the context of electric mobility HCP systems. To this end, we first identify all the relevant sub-systems (e.g., actors/stakeholders) that are involved in the communication of such type of human-centred cyber physical systems. We then adopt the common vulnerability scoring system (CVSS) methodology in order to assess semi-quantitatively the vulnerabilities present between every pair of communicating sub-systems. To achieve this, we carry out an exhaustive literature review [7–18] leading us to consider assumptions and giving clear justifications on our choices. Based on those assumptions, CVSS overall vulnerability score is calculated. Our carried out analysis and assessment show that among the different communicating pair of sub-systems, the ones between CSO and EVSE as well as CSO and eMSP are the most vulnerable sub-systems. To the best of our knowledge, this is the first paper in attempting to provide an end-to-end semi-quantitative assessment of the vulnerabilities within the context of electric mobility HCP systems.

The remainder of this paper is structured as follows: In Section 2, we first describe the human-centred cyber physical system under study by giving details about the involved sub-systems, their corresponding roles, as well as the information communicated between them. We then define the attack types and the security requirements that need to be consider. In Section 4, the CVSS methodology is introduced, its three groups are detailed by specifying the different metrics for each group, and the model to compute the overall vulnerability score is given. Evaluation and assessment of vulnerabilities between each

pair of communicating sub-systems are presented in Section 5. The paper is concluded in Section 6.

2. Preliminaries

In this section, we first describe the different actors of the electric mobility HCP system and specify their respective roles. Then based on the considered actors, we state the exchanged information and the underlying standard data models. Lastly, we define different types of attacks pertinent to the electric mobility context and specify the most relevant security requirements necessary to face against the described attack types.

2.1. System Description

In [19], the electric mobility system architecture (EMSA) model and framework were introduced. Such a framework is based on the smart grid architecture model (SGAM) [20]; however for the context of electric mobility. Thus, its four domains were selected carefully to represent the corresponding cyber physical system (see Figure 1): energy conversion (e.g., DSO), energy transfer to and from EV (e.g., CSO), electric vehicle and EV user premises (e.g., eMSP and EV users). In addition to its four domains, EMSA also consists of–like SGAM–6 zones of process, field, station, operation, enterprise and market. Process is the smallest power generating or consuming entity (e.g., EVSE, EV), whereas field is the concatenation of one or more processes (e.g., charging box providing two or more charging connectors or EVSEs). Station is the aggregation of one or more fields (e.g., a charging station consisting of several charging boxes), whereas operation, enterprise and market are the respective concatenations of lower level entities (e.g., an operation zone can present the aggregation of one or more charging stations). It is worthwhile to mention that starting from operation upwards, the realisation of each zone is done through a software implementation (e.g., charging station management system). Finally, such a model has 5 interoperability layers of business, function, information, communication and component. In business layer, all the actors together with their business goals and high level uses cases are specified. In the function layer, all the necessary functions/methods are defined for the realisation of the goals specified in the business layer. In the information layer, the necessary data models are detailed which are used by the functions specified in the function layer. Communication layer specifies the different communication protocols used for the exchange of information between different functions. The physical infrastructure with its constituent entities are detailed in the component layer.

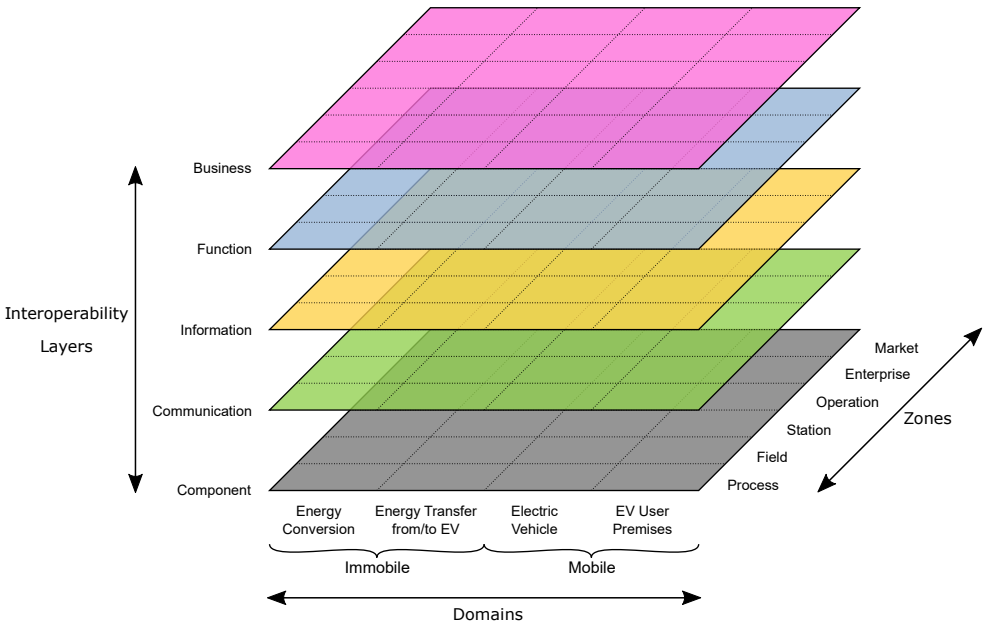

Figure 1. The E-Mobility Systems Architecture (EMSA) model of [19].

2.1.1. Role of Each Actor

Figure 2 presents the relevant actors of electric mobility considered in this paper and their respective roles. Please note that the corresponding figure captures both the function and component layers of EMSA. This is because the function layer specifies all the necessary functions (e.g., payment method) needed by the corresponding HCP system. Furthermore, functions of each sub-system exchange information with each other through communication. Consequently, Figure 2 clarifies the need for the communication between different sub-systems. The following actors (e.g., sub-systems) and their corresponding roles are considered in this paper:

- EV User: is the one who uses the electric vehicle (EV). The owner and user should not necessarily point to the same person.
- EV: is the transportation mean which is powered by an electric battery system.
- EVSE: EV supply equipment, also known as the charging connector, is responsible for providing electricity drawn from the power system to the EV to charge its battery. The EVSE communicates with the EV to negotiate the charging parameters, manage power delivery, and to handle the payment.
- eMSP: electric mobility service provider grants EV Users access to a variety of EVSEs, facilitates payment services with different methods, and helps in searching for available charging stations. For this purpose, eMSP normally makes an agreement with CSOs to get the data of charging sessions of their customers. One entity could also play the role of CSO and eMSP for the same purpose.
- CSO: charging station operator is responsible for managing the different charging boxes (e.g., a collection of EVSEs) located at one or more charging stations. Furthermore, it is responsible for technical operations and maintenance of EVSEs (public and semi-public). Its revenue comes mainly from providing electrical energy to EVs, and it has the information for authorising EV Users for using its EVSEs.
- CH: clearing house, also known as roaming, enables EV Users to be able to charge their EVs at EVSEs that belong either to a different country or contracted CSO.
- DSO: distribution system operator, also known as the grid operator, has the main responsibility of maintaining the stability of the grid and hence the constant flow of electricity.
- Energy Supplier: is responsible for supplying energy to the utility companies and DSOs. In certain cases, energy supplier and DSO can be the same entity.

It is important to note that the above-mentioned sub-systems present the abstract description of the HCP system under study. As a matter of fact, in this paper whenever we analyse every pair of the communicating sub-systems (see Section 5), this is realised at this level of abstraction. More precisely, it is possible that more than one instance of the corresponding sub-system exploits the vulnerability of one or more instances of the other sub-system (e.g., relationship is m:n and not 1:1). To clarify more, in case of a vulnerability that exists at the EVSE (e.g., charging boxes), this vulnerability can be exploited by more than one electric vehicle and at different charging boxes.

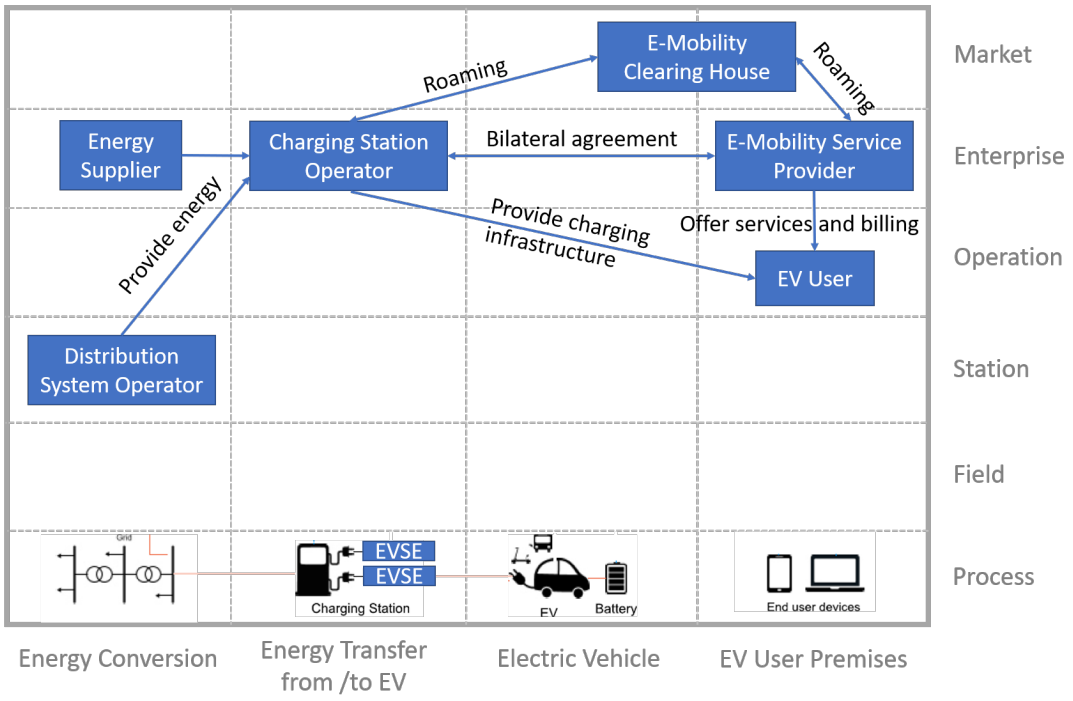

Figure 2. The most relevant sub-systems (e.g., actors/stakeholders) involved in electric mobility cyber physical system inspired by [19]. The red-coloured links demonstrate the electrical connections, whereas the blue-arrowed links illustrate the underlying role of one sub-system with respect to the other.

2.1.2. Information Commutation

Figure 3 gives an overview of the standard data models used for the interaction between pairs of actors (e.g., sub-systems) described in Section 2.1.1. Currently, the electric mobility ecosystem is vigorously fragmented, where mostly open protocols pre-dominate the information commutation. The de-facto standards specify the relevant data formats.

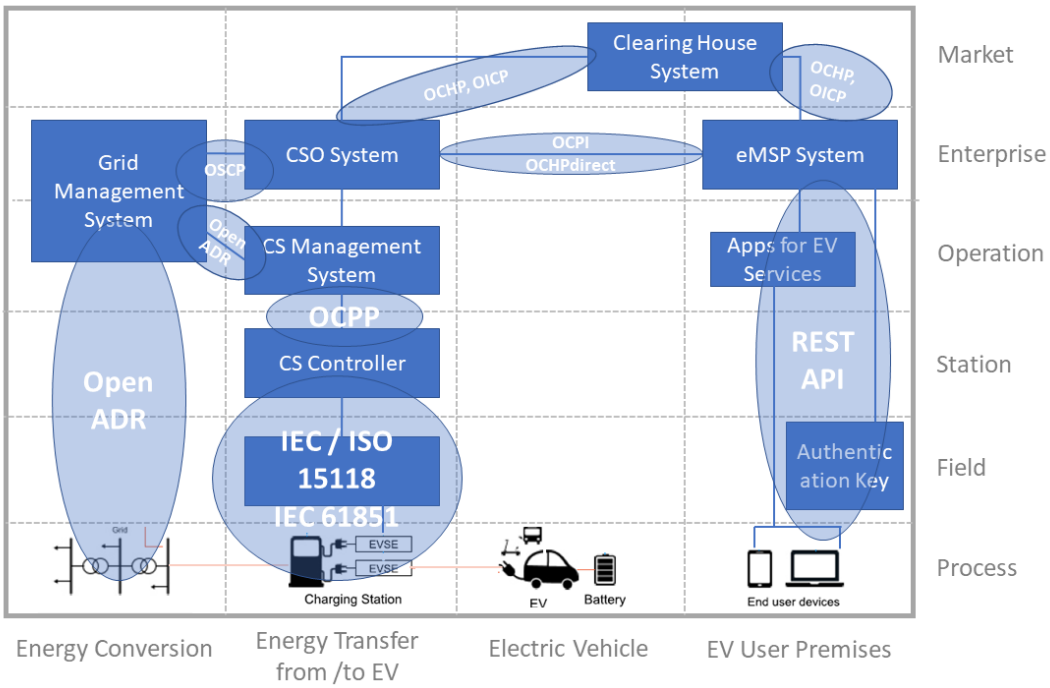

Figure 3. The most dominant standard data formats used for information exchange between pairs of actors/stakeholders involved in electric mobility cyber physical systems inspired by [19].

In the zones of market and enterprise, protocols for clearing house-based (e.g., roaming purposes) such as open clearing house protocol (OCHP [21]) and open inter charge procotol (OICP [22]), or peer-to-peer information exchange such as the open charge point interface (OCPI v2.2 [23]) dominate. Those protocols are used to exchange information between the actors of eMSP, CH and CSO. For the exchange of information between the actors of DSO and CSO, the open smart charge protocol (OSCP [24]) stands over the others.

In the zones of operation, station, field and process, the open charge point protocol (OCPP [25]) is used for the information exchange between the charging station management system (e.g., back-end system) and the charging station controllers giving access to the EVSEs. For the cross-domain information exchange with grid management system, open automated demand-response (OpenADR [26]) is available. This data model is used for the realisation of demand-response such that the relevant information is exchanged with charging station management system and the grid infrastructure through monitoring devices (e.g., smart meters). Finally, the direct communication between the actors of EV and EVSE as well as between the charging station controller and different charging boxes (e.g., collection of EVSEs) are realised thanks to the standards ISO 15118 [27] and IEC 61851 [28].

2.2. Cyber Security

In this section, we first give the definition of the different types of cyber attacks considered in this paper, and then specify the corresponding security requirements.

2.2.1. Types of Attacks

Inspired by [5,29,30], in this paper we consider the following six different types of cyber attacks that can be executed within the context of electric mobility HCP systems:

- Man-in-the-Middle (MiM): includes the insertion of unauthentic information and spoofing by intervening the communication between two entities through a forged party. During the exchange of messages, the attacker might counterfeit the message and send the wrong information to the endpoint. This can decrease the availability of communicating entities and damage their reputation.
- Impersonation: the theft of another entity's identity by a malicious party. To this end, this latter uses the victim's credentials during the identification and authentication processes, so that it pretends to be the authentic entity. This can lead to various harmful effects on the system.
- Eavesdropping: the illegal scan of the conversation between two entities by a malicious party. This is done in order to capture sensitive information about the system (e.g., credentials). This attack can lead EV Users, CSOs, and other actors (e.g., sub-systems) of electric mobility HCP systems to financial damage depending on the significance of the captured information. For instance, the loss of personally identifiable information (PII) can create privacy issues, and chances for impersonation become significant.
- Denial-of-Service (DoS): too many requests on communication channels and services may delay message delivery. Furthermore, disruption can also be realised by deleting messages/actions/processes which can make the services inaccessible to authentic users. This could cause unavailability of the service for a temporary period of time, which can damage the reputation and integrity of service providers (e.g., DSO, CSO, eMSP).
- Tampering of messages: is the act of deliberately modifying (e.g., destroying, manipulating, or editing) information that belongs to some other entity. It could cause harmful effects to the system. For instance, the fabrication of tariff information or metering data may lead to energy theft in EV charging infrastructure.
- Repudiation: systems, services, or processes can deliberately or unintentionally stop executing their proper actions, such as message transmission or data storage, etc. For instance, EV Users can claim to have received less energy than stated on the billing record. Likewise, the DSO may claim to have delivered more energy to the CSO.

2.2.2. Security Requirements

The following five security requirements are considered in this paper, for the context of electric mobility HCP systems, which are inspired by [31]:

- Confidentiality: is the protection of information from any unauthorised disclosure. To face eavesdropping attacks, the confidentiality of sensitive information such as charging request messages, control messages for payments, etc. should be protected.
- Authentication: is the process of verification in order to ensure that the communicating entity is the one that it claims to be. To face impersonation attacks and to provide a fair billing with an EV roaming support, strong entity identification and mutual authentication services should be realised.
- Authorisation: is the process of granting authorised users legitimate access to resources (e.g., system, data, application, etc.). It is beneficial to minimise the chances of successful impersonation attacks.
- Integrity: ensures that the original message being sent has not been altered or changed during the transmission. To face tampering attacks, the integrity of the messages should be ensured.
- Availability: is the property of a system or a resource of the system being accessible and usable upon demand by authorised entities. DoS attacks impose a threat to this property. Measures (e.g., gateway filtering) must be in place to ensure that important service entities can resist DoS attacks.

It is important to note that the National Institute of Standards and Technology (NIST) has defined several security requirements for Smart Grid (see Table 3-3 in [32]). Thus, the above mentioned requirements present a subset and not an exhaustive list of security requirements

3. Literature Review

In this section, we present the results of the carried out literature review. We classify them based on the involved pair of communicating sub-systems.

3.1. EV-EVSE

It was shown in [29] that MiM attacks are possible that can manipulate the energy provisioning path. This is realised by using its own fake charging spot implanted between EV and authorised EVSE. To this end, the attacker routes the communication between honest EV user and EVSE. This leads to partial theft of energy, whereas the authorised EV gets the fraction of its purchased energy. In [29,31], the authors demonstrated that by eavesdropping sensitive authentication and authorisation information (e.g., vehicle identification number stored in internal storage of EV) can be stolen, which can lead to impersonation attacks. In [11], the authors show that the authentication process between EV and EVSE could be eavesdropped. Thus, by inserting fake card reader devices on remote EVSE or using NFC-enabled phones and cloning the cards, it is possible to eavesdrop on the data communication (e.g., ID number) of RFID cards. Lee et al. in [16] showed that an attacker can use two ways to intrude the system by stealing either valid certificate, private key or by using expired or revoked certificates. Furthermore, they demonstrated that fraud and harm may also be committed by tampering of messages exchanged between EV and EVSE. For instance, by modifying "metering status" or "power delivery" messages, an EV user can be provided with less energy than the requested amount. The charging fee can also be fabricated by changing the parameters of "payment details" messages. Regarding DoS attacks, it was shown in [29,31] that such type of attacks could make the EVSE inaccessible by delaying or dropping some messages related to charge metering. Furthermore, the authors illustrated that repudiation (e.g., transaction falsification) could also take place either deliberately or unintentionally, where EV user can claim to have received less energy than stated on the billing record. Similarly, the utility may claim to have delivered more energy to the customers.

3.2. EVSE-CSO

The authors in [15,17] showed that the communication between EVSE and CSO is vulnerable to eavesdropping which may lead to impersonation attacks. Distortion (e.g., fake data insertion, spoofing) could lead to MiM attacks which could easily disturb communication. Furthermore, they illustrated that disruption is also possible by deleting some messages from the conversation or by replaying some selective messages in the communication. Variants of this threat can be those related to DoS. To this end, attackers could take advantage of the interception, so that other subsequent attacks can be carried out such as denial of power resources and services, energy theft and overload (e.g., variation of power levels at particular points in the system such as substations). In all of these cases, attackers inject fake OCPP transactions to cause serious local effects and/or reduce network stability.

3.3. CSO-eMSP

The authors in [18] studied the communication between those two sub-systems. They showed that dishonest CSO employees or even eavesdroppers could theft the static credentials used in protocol setup phase that can lead to MiM attacks and spoofing. Furthermore, the authors claim that it could be possible the creation of false charging plans and manipulate the smart charging processes. Due to insufficient security provided by TLS, professional hackers could get into the network and alter the data in transit between the several subsystems that the eMSP communicates with. Finally, the authors demonstrated that DoS attacks on channels and services could delay message deliveries and make services inaccessible to legitimate users. This could cause shutting down services. For instance, a malware in a system can compromise the ability of the eMSP to create charging plans or handling sensitive data in a secure manner. The authors in [14] illustrated that the CSO is capable of reading the data transmitted between EVSE and EVs such as the contract ID of EV user and energy rates at that particular time or location. This insufficient end-to-end security can cause the security issues of private data. In case of messages tampering attacks, eMSP cannot verify that the data received from CSO is authentic as it was originally generated by EVSE.

3.4. DSO-CSO and -eMSP

In [33], the authors demonstrated that it is possible for professional hackers/other third parties to intrude the data collected by the DSO and potentially alter it. Furthermore, viruses and/or malware could potentially be a danger to the system by altering or tapping into specific parts of the power grid. Dishonest employees of the DSO or eMSP can also find ways to manipulate forecast capacity and communication.

4. Methodology to Assess Vulnerabilities

Basically, risk can be assessed either quantitatively [34] or qualitatively [35]. The former is realised when significant amount of information is available and derives assessments in the form of numerical values, whereas the latter derives assessments based on some qualitative levels (e.g., high, medium, low) which might be sometimes subjective. Each of those two approaches has its own advantages and inconveniences. Semi-quantitative approaches such as Microsoft's Dread [36] and FIRTS's CVSS [37] are proposed in order to benefit from advantages of both quantitative and qualitative assessment approaches. Briefly, the principles and methods used in this approach are based on numerical representative in the form of bins or scales. The values and meanings of those scales are specified for particular context. Once the assessment is generated in the form of bins (e.g., 0–15, 16–35, 36–70, 71–85, 86–100) or scales (e.g., 0.1–10), those can be converted into qualitative metrics and communicated with decision-makers. Table 1 summarises the most relevant quantitative, qualitative and semi-quantitative approaches that have been proposed in the literature. Please note that the last two entries (e.g., MIL-STD-882E and ASIL) of this table deal with assessing risks for safety-critical systems. For instance ASIL models risk as the

probability of a dangerous event to happen multiplied by its impact and takes into account parameters such as exposure, severity, controllability of the dangerous event.

Table 1. The most relevant quantitative, qualitative and semi-quantitative approaches proposed in the literature.

Approach	Type	Parameters	Reference
NIST Special Publication 800-30	Qualitative and semi-quantitative	Likelihood and impact	[35]
Common Vulnerability Scoring System	Semi- quantitative (0–10)	Attack vector, attack complexity, privilege required, user interaction, CIA impact, exploit code maturity, remediation level, report confidence, and security requirements	[37]
Microsoft's DREAD	Semi- quantitative (1–10)	Damage, reproducibility, exploitability, affected users, discoverability	[36]
OWASP Risk Rating Methodology	Qualitative and semi-quantitative (0–9)	Likelihood based on threat agent and vulnerability factors, impact based on technical and business factors	[38]
MIL-STD-882E System Safety	Qualitative	Severity and probability	[39]
Automotive Safety Integrity Level (ASIL)	Qualitative	Probability, severity, controllability	ISO 26262

In this paper, we adopt the common vulnerability scoring system (CVSS) methodology for the assessment of the vulnerabilities. As mentioned previously, this methodology provides a semi-quantitative approach for the derivation of the underlying metrics for assessment. Our choice is based on the fact that among the different methodologies, CVSS considers numerous parameters for the assessment (see Table 1). Consequently, it is suitable for the analysis of vulnerabilities of complex sub-systems and their interactions, which is the case for the electric mobility human-centred cyber physical systems. Next, we briefly describe the corresponding methodology and highlight how the different metrics are derived.

4.1. Common Vulnerability Scoring System

CVSS assesses the vulnerability of a system by dividing the considered metrics into three groups: base, temporal, and environmental (see Figure 4). Base group consists of metrics related to CIA (Confidentiality, Integrity and Availability) impact, access vector and complexity as well as authentication. Temporal group comprises of metrics related to exploitability, remediation level and report confidence. Finally, environmental group consists of metrics related to CIA requirement, potential of collateral damage and target distribution.

The methodology assigns to each of the above-mentioned metrics certain numerical values, which are derived based on the recommendations of the standardised information gathering (SIG questionnaire) repository [40] with the collaboration of Deloitte and Touche LLP [41]. The overall vulnerability score of each system under study is calculated with the help of mathematical models. Based on the derived scores, those can then be qualitatively categorised into low, medium, high, and critical levels, as shown in Table 2. Next, we detail the metrics of each group and then give the overall mathematical models for the assessment of the vulnerability, which are proposed by [37].

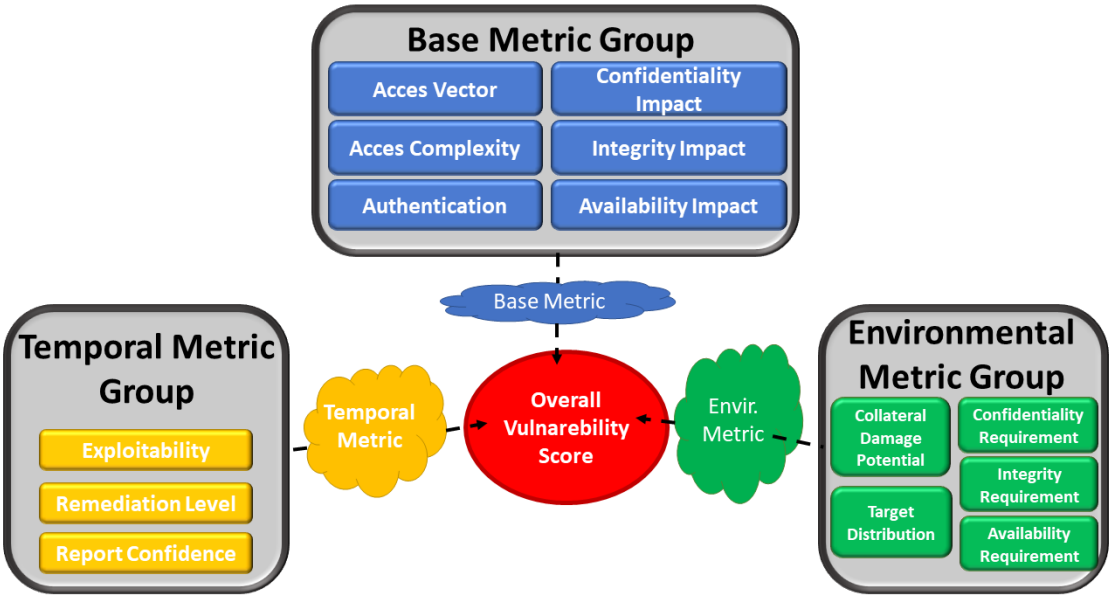

Figure 4. Different metric groups of CVSS Version 2.

Table 2. Qualitative risk severity rating scale for different categories based on [37].

Category	CVSS Score Range
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10

4.1.1. Base Metric Group

This group demonstrates the characteristics of vulnerabilities of a system that remain constant with respect to time and the user's environment. It consists of the following parameters:

- Access Vector: represents either the fact that the vulnerability is remotely exploitable or up to what extent the attacker needs access to get into the system. For this purpose, it has three possibilities of network, adjacent and local. Network describes that vulnerability is remotely exploitable and has the highest value of 1. Adjacent is used when attacker requires physical or logical access to the network (e.g., local IP, Bluetooth) and has a value of 0.646. Local indicates that the attacker needs either local or physical access to vulnerable entities for their manipulation, and has a value of 0.395.
- Access Complexity: illustrates the level of complexity in carrying out attacks on a system. The more complex the attack is, the least vulnerable the system becomes. It has three possibilities of high, medium and low. High shows that the vulnerable configuration is seen very rarely in practice, and has a value of 0.35. Medium indicates that access depends on some factors such as authentication, special configuration and/or knowledge about the system, and has a value of 0.61. Low denotes that the attack can be performed easily, and has the highest value of 0.71.
- Authentication: shows that either the attacker needs to be authorised by the system or does not need to be, in order to successfully compromise the system. It has three possibilities of none, single and multiple. None is used when the attacker is unauthorised and does not require privilege to access system resources, and has the highest value of 0.704. Single shows that the attacker needs to be authorised at least

once and must have privilege up to non-sensitive resources, and has a value of 0.56. Multiple denotes that the attacker is authorised and has privilege up to administrative level or the attack depends on user interaction, and has a value of 0.45.

- Impact Metric: describes the level of CIA (Confidentiality, Integrity, Availability) of the system impacted by an attack. It has three possibilities of complete, partial and none. Complete illustrates that there is a complete loss of CIA, and has the highest value of 0.660. Partial is used when there is loss of CIA up to some extent, and has a value of 0.275. None indicates that there is no impact on CIA and has a value of 0.

Based on the aforementioned parameters, the score for the base group metric is calculated by considering the following mathematical model [37]:

$$Base_{score} = (0.6Impact + 0.4Exploitability - 1.5)1.176 \quad (1)$$

where $Impact$ and $Exploitability$ are given as:

$$Impact = 10.41(1 - (1 - Imp_C Req_C)(1 - Imp_I Req_I)(1 - Imp_A Req_A))$$

$$Exploitability = 20 Access_{Vector} Access_{Complexity} Authentication$$

where Imp_X and Req_X denote respectively the impact and requirement of the element X, such that X can be one of the three parameters of Confidentiality (C), Integrity (I), or Availability (A). Furthermore, authentication, access vector and complexity are modeled in $Exploitability$. For the worst case scenario, $Impact$ and $Exploitability$ can take values of 10.41 and 6.6 respectively. Consequently, replacing those values in Equation (1) results in a score of 8.7 for the base group metrics when considering the worst case scenario.

4.1.2. Temporal Metric Group

This group represents the reported information about vulnerabilities, and shows to what extent the attacks against a particular vulnerability are known. New patch releases and advancement in system security as well as attack methods make this metric varying with respect to time and user environment. It consists of the following parameters:

- Exploitability: represents the severity in exploiting the vulnerabilities of the system. To this end, it has four possibilities: high, functional exploitation, PoC code, and unproven. High indicates that attack is possible by commonly available codes, remotely deliverable viruses or by manual trigger, and has the highest value of 1. Functional exploitation shows that exploitation techniques along with code are available that can be functional in case of vulnerability, and has a value of 0.95. Proof-of-concept (PoC) code demonstrates that exploitation techniques do not work for all situations, where extensive modifications are required by a skilled attacker, and has a value of 0.9. Unproven illustrates that no exploitable code is available, and only theoretical concept of exploitability can be found, and has a value of 0.85.
- Remediation Level: measures the level of effort realised to remedy the effected components of the system by attacks. Like the previous metric, this one too has four possibilities: unavailable, workaround, temporary and official fixes. Unavailable demonstrates that there is currently no available solution, and has the highest value of 1. Workaround indicates that solutions might be available through third-parities, and has a value of 0.95. Temporary fix shows that the official vendors provide a temporary solution, and has a value of 0.9. Official fix shows that a complete solution is available by official vendors, and has a value of 0.87.
- Report Confidence: this metric measures the level of assurance on the existence of vulnerabilities by authorised vendors. This metric has three possibilities: confirmed, reasonable, and unknown. Confirmed shows that the corresponding vulnerability is acknowledged by vendors, and has the highest value of 1. Reasonable indicates that the vulnerability is confirmed by unofficial vendors such as researchers or security analysts, and has a value of 0.95. Finally, unknown demonstrates that only the impact

indicates the presence of vulnerability, where the reason of the vulnerability is not known, and has a value of 0.9.

Taking into account the above-mentioned parameters, the score for the temporal group metric is calculated by considering the following mathematical model [37]:

$$Temporal_{score} = Base_{score} Exploitability Remediation_{Level} Report_{Confidence} \quad (2)$$

where $Base_{score}$ is given in Equation (1) and the other three parameters are described in this section respectively. For the worst case scenario, the temporal metric group has the same score of 8.7 as that of the base metric group. Please note that the temporal score produces a score no higher than the base one, and no greater than 33% lower than the base score.

4.1.3. Environmental Metric Group

This group represents metrics that capture characteristics of a vulnerability that are associated with a user's environment. It consists of the following parameters:

- Collateral Damage Potential: this parameter measures the possible loss of (1) physical assets of an organisation, and (2) life through damage caused by an attack. It has six possibilities: low, low-medium, medium-high, high, and undefined with values of 0.1, 0.3, 0.4, 0.5 and 0 respectively. In this paper, as we consider the information and communication layers of EMSA without analysing its component layer, then we consider the possibility of undefined (e.g., value of 0) for this parameter.
- Target Distribution: it measures the percentage of systems that could be affected by the vulnerability. This parameter has five possibilities: none, low, medium, high, and undefined with values of 0, 0.25, 0.75, 1.0, and 1.0 respectively. For the same reason as explained in the previous parameter, this one too we select the value of zero (e.g., none) to skip this metric in the equation.
- Security Requirements: this metric measures the effect that an organisation or individuals could have by loss of confidentiality, integrity, and availability (CIA). Thus, it consists of three sub-metrics of Req_C,Req_I, and Req_A. Furthermore, each such sub-metric has four possibilities: low, medium, high and undefined with values of 0.5, 1.0, 1.51, and 1.0 respectively.

Considering the above-mentioned parameters, the score for the environmental group metric is calculated by considering the following mathematical model [37]:

$$Environmental_{score} = (Temporal_{score} + (10 - Temporal_{score}) Collateral_{DamagePotential}) Target_{Distribution} \quad (3)$$

where $Temporal_{score}$ is given in Equation (2) and the other two parameters are described in this section respectively. For the worst case scenario, the environment metric group has a score of 9.35.

5. Evaluation

In this section, we evaluate and assess the vulnerabilities using the CVSS methodology presented in Section 4. To this end, we consider the communication between every pair of actors (e.g., sub-systems) given in Section 2.1, together with the type of attacks described in Section 2.2.

5.1. EV-EVSE

The communication between EV and EVSE happens whenever an EV is willing to be supplied with electricity (e.g., to charge its battery) from the EVSE (see Figure 2). To compute the overall vulnerability score of this communication, we considered assumptions and gave justifications to them, which are explained next.

5.1.1. Base Metric Group

This communication might be vulnerable to attacks whenever the EV user's ID, private keys, and/or certificates are compromised. This can be only realised if the attacking entity

is located locally (e.g., no remote access) at the charging station. Hence, the *Access Vector* is set to "local". Since end-to-end security has already been considered by ISO 15118 standard, as well as transport layer security is implemented, then we assume *Access Complexity* to be "medium" (e.g., it cannot be "low"). Please note that it also cannot be considered "high" since the EV user ID is the only factor on which the complete authentication to back end system depends. We consider *Authentication* to be "single", because it is possible to obtain the unique ID of the EV user through fake RFID reader devices. Regarding *Impact Metrics*, since the vulnerabilities in access control give user-level access, we consider confidentiality and integrity to be "partial". Similarly, the successful attacks can cause user-level access issues in the form of denial of service, then we assume also availability to be "partial".

5.1.2. Temporal Metric Group

We assume *Exploitability* to be "functional exploitation", since exploit code is available. This is because, it can be implemented in most of the situations where the vulnerability exists (e.g., ATM skimming). Although the encryption-based RFID cards are used in banking systems; however their use is not considered in the scope of ISO 15118 yet. Since official vendors do not report the vulnerabilities or attacks related to authentication, the solutions are explained by non-official sources such as research organisations or security companies. Consequently, we consider *Report Confidence* and the *Remediation Level* to be "reasonable" and "workaround" respectively.

5.1.3. Environmental Metric Group

Since the disclosure of identification data or charging related messages can have limited adverse effects on individuals in the form of energy theft, we consider that the *Security Requirements'* confidentiality to be "low". Furthermore, the tampering of messages can cause serious damage to the system. Hence, we assume integrity to be "medium". For instance, by modifying 'metering status' messages or 'power delivery' messages, an EV user can be provided with less energy than the requested amount. Charging fees can also be fabricated by changing the parameters of 'payment details' messages. Unavailability of EVSEs can be problematic, on one hand to the EV users, and on the other hand to EVSE vendor's reputation. Thus, we suppose the availability to be "medium".

5.1.4. Overall Score

Based on the above-mentioned justifications on the different considered metrics, we calculated the overall score for the vulnerability between EV and EVSE. The obtained results is shown in Table 3, indicating a low overall vulnerability score of 3.0.

5.2. EVSE-CSO

The communication between EVSE and CSO happens whenever a charging or management related information are required (e.g., new charging process starts, payment, maintenance). As it can be seen in Figure 3, this communication is realised through the OCPP protocol. To compute its overall score, we identified three different vulnerabilities related to the OCPP protocol: transport layer security, local authentication, system maintenance methods. Furthermore, for each of these three types of vulnerabilities, we considered assumptions and gave justifications to them, so that the overall score is computed.

Table 3. Summary of the vulnerability analysis for the EV-EVSE sub-systems communication. The parameter values indicate our choice to the different metrics of the CVSS methodology.

Base Metrics	**Parameter Values**
Access Vector	local
Access Complexity	medium
Authentication	single
Confidentiality Impact	partial
Integrity Impact	partial
Availability Impact	partial
Temporal Metrics	**Parameter Values**
Exploitability	functional exploitation
Remediation Level	workaround
Report Confidence	reasonable
Environmental Metrics	**Parameter Values**
Confidentiality Requirement	low
Integrity Requirement	medium
Availability Requirement	medium
Overall vulnerability score	**3.0**

5.2.1. Base Metric Group

Vulnerability V_1: Transport Layer Security

OCPP is implemented based on web-based services using the HTTP and FTP protocols over older versions of TLS, which are vulnerable to attacks. In this paper, we assume that the implementation of OCPP is updated with all the latest patches installed. Despite those assumptions, any vulnerability due to required TLS configurations could be remotely exploitable. Thus, we assume that *Access Vector* has a value of "network". Furthermore, we consider that *Acess Complexity* is "medium". This is because the number of attacks are possible even for TLS v1.3 [42]. The *Authentication* metric is "none" because exploiting any TLS or OpenSSL-related vulnerability, the attacker does not need user interaction to launch a successful attack such as by JavaScript or Applet injection, etc. Regarding *Impact Metrics*, we assume the confidentiality to be "partial". This is because in TLS-related attacks, 'data in transit' can only be on the risk of disclosure; however, saved data remain secure. We consider that integrity and availability have a value of "complete" because entire modification of information would be possible by exploiting this vulnerability, leading to total unavailability of the EVSE and CSO.

Vulnerability V_2: Local Authentication

For this type of vulnerability, we consider *Access Vector* to be "network" since, according to the OCPP protocol, CSO sends the updated local authentication list (LAL) to EVSEs and removes its cached memory to allow EVSEs to authenticate users in offline mode. Attackers can exploit this feature remotely by enforcing EVSEs to remain offline through any DoS attack. Furthermore, we assume *Access Complexity* to be "low". Since user interaction is not required in this type of attacks, then we give *Authentication* a value of "none". Regarding *Impact Metrics*, we assume confidentiality and integrity to be both "none", whereas we consider that availability to have a value of "complete".

Vulnerability V_3: System Maintenance Methods

According to the OCPP protocol, the CSO is required to send a request to EVSE in order to download the firmware updates or to upload the diagnostic files. This feature can be exploited by forcing the EVSE to accept the request with a fake URL to download the firmware updates from malicious hosts. By changing the parameters of this request, an attacker can upload its diagnostic files to that particular EVSE. This vulnerability can

be exploited through the communication channels since most of the messages of OCPP are transferred by web-services using the HTTP and FTP protocols over SSL. Hence, we consider *Access Vector* to be "network". Furthermore, we assume *Access Complexity* to be "medium". This is because exploiting this vulnerability requires modification of commands. As the attack depends on the acceptance of fake requests from the target system, thus we give *Authentication* a value of "multiple". Finally, regarding *Impact Metrics*, we assume the integrity, availability and confidentiality to be "partial". This is because to inject fake commands with modified parameters into the system, disclosure of a few commands could be required to get the actual format. By exploiting this vulnerability, some of system's functions instead of the whole can be comprised. Moreover, this exploit can reduce the system performance because of some injected viruses or malware bugs.

5.2.2. Temporal Metric Group

Vulnerability V_1: Transport Layer Security

For this type of vulnerability, we consider *Exploitability* to be "functional exploitation". This is because various types of attacks are published related to TLS versions. Since the official vendors recommend using TLS v1.1 and above, then we assume *Remediation* to be "official fix". Regarding the *Report Confidence* metric, we give it a value of "confirmed". This is because vendors acknowledged such type of vulnerability. Consequently, improved versions were introduced (e.g., TLS v1.1, v1.2, v1.3).

Vulnerability V_2: Local Authentication

We consider *Exploitability* to be "PoC code" because exploitation techniques do not work for all situations, such that extensive modifications are required by skilled attackers. Non-official vendors explain this type of OCPP vulnerability and different solutions are also provided by them. Thus, we assume *Remediation Level* to be "workaround". As sufficient details are published about this vulnerability and possible attacks on OCPP-based communication, we give *Report Confidence* a value of "reasonable".

Vulnerability V_3: System Maintenance Methods

We assume that *Exploitability* has a value of "PoC code", because the exploitation technique does not work for all situations, where extensive modifications are required by skilled attackers. Since the aforementioned vulnerability of OCPP is explained by non-official vendors and solutions are also provided by them, then we consider *Remediation Level* to be "workaround". Finally, we give *Report Confidence* a value of "reasonable", as sufficient details are published about the vulnerabilities and possible attacks on OCPP-based communication.

5.2.3. Environmental Metric Group

Vulnerability V_1: Transport Layer Security

Since the disclosure of identification-related information or charging-related messages can have limited adverse effects on individuals in the form of energy theft, then we consider confidentiality of the *Security Requirements* metric to be "medium". The tampering of messages can cause a considerable damage to the system. For this purpose, we assume that integrity has a value of "high". For instance, by amendment of messages, attackers might intercept and perform many successive attacks such as a denial of power resources and services, energy theft, and overload the system. In such situations, attackers can inject fake OCPP transactions to cause serious local effects or reduce the system's stability. Unavailability of EVSE and/or CSO can be problematic at the user- and system-level. This is because denial of service attacks can make CSO unable to respond to EVSE, eMSP, DSO, and CH. Thus, we consider the availability to be "medium".

Vulnerability V_2: Local Authentication

Loss of availability of EVSEs can have limited adverse effects on the individual level or to the reputation of the company. Thus, we consider availability of the *Security Requirements* metric to be "low". No modification or disclosure of other system information can happen because of this particular vulnerability. Consequently, we assume the integrity and confidentiality requirements to be "undefined".

Vulnerability V_3: System Maintenance Methods

Exploitation of this vulnerability can have limited adverse effects on individuals or organizations. Thus, we assume integrity, availability and confidentiality of the *Security Requirements* metric to be "low".

5.2.4. Overall Score

Based on the above-mentioned justifications on the different considered metrics, we calculated the overall score for the three vulnerabilities V_1, V_2 and V_3 separately for the communication between EVSE and CSO. The obtained results are given in Table 4, indicating an overall vulnerability score of 7.7 (high), 4.4 (medium) and 3.9 (low) for V_1, V_2 and V_3 respectively.

Table 4. Summary of the vulnerability analysis for the EVSE-CSO sub-systems communication. The parameter values indicate our choice to the different metrics of the CVSS methodology. Three different types of vulnerabilities V_1, V_2, and V_3 are identified for this communication.

Base Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**	**Parameter Values for V_3**
Access Vector	network	network	network
Access Complexity	medium	low	medium
Authentication	none	none	multiple
Confidentiality Impact	partial	none	partial
Integrity Impact	complete	none	partial
Availability Impact	complete	complete	partial
Temporal Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**	**Parameter Values for V_3**
Exploitability	functional exploitation	PoC code	PoC code
Remediation Level	official fix	workaround	workaround
Report Confidence	confirmed	reasonable	reasonable
Environmental Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**	**Parameter Values for V_3**
Confidentiality Requirement	medium	undefined	low
Integrity Requirement	high	undefined	low
Availability Requirement	medium	low	low
Overall vulnerability score	**7.7**	**4.4**	**3.9**

5.3. CSO-eMSP

CSO and eMSP communicate and exchange messages with each other for the sake of facilitating and providing numerous services to the EV users. It can be noticed from Figure 3 that the corresponding communication is realised through the OCPI protocol. To compute its overall vulnerability score, we identified three different vulnerabilities related to the OCPI protocol: static credentials for authentication, transport layer security, and application layer security. Furthermore, for each of these three types of vulnerabilities, we assumed certain facts with justifications, so that the overall score is computed.

5.3.1. Base Metric Group

Vulnerability V_1: Static Credentials for Authentication

Stated by the OCPI protocol, the exchange of static tokens in the initial setup phase of the protocol is outside its scope. This can be realised for instance by email exchanges. However, many attacks could remotely exploit this vulnerability. As a matter of fact, we assign *Access Vector* a value of "network". Moreover, we assume *Access Complexity* to be "low". This is because security of static credentials depends on TLS or any email service. We consider *Authentication* to be "none", since if the attacker successfully gets the static credential, he/she could act as a legitimate entity, and the system will be completely disclosed to him/her. Regarding *Impact Metrics*, we give availability a value of "none", because according to the types of attacks considered in this paper, if the attacker enters into the system either as CSO or eMSP, he/she will not disconnect the connection between CSO and eMSP. Instead, he/she would rather go for other advantages of authorisation such as energy theft. For integrity and confidentiality, we consider to have both a value of "complete".

Vulnerability V_2: Transport Layer Security

OCPI protocol relies on transport layer security and it refers to TLS as SSL, which is an older version and is vulnerable to attacks. Therefore, the communication between CSO and eMSP could be remotely exploited. Consequently, we assume *Access Vector* to be "network". In this paper, we consider that the implementation is realised using the latest versions of TLS (e.g., version 1.2 or 1.3). Furthermore, OCPI considers the use of TLS as an option and does not describe the security features of the communication in detail, such as which cipher suits or certificates should be used. Hence, we give *Access Complexity* a value of "medium". In case of insufficient transport layer configurations, an attacker would not be required to be authenticated to exploit the vulnerability. This is because various attacks can bypass the authentication mechanisms. As a matter of fact, we assume *Authentication* to be "none". Concerning *Impact Metrics*, we give confidentiality a value of "complete", since CSO acts as a mediator for the delivery of information from EVSE to eMSP. Furthermore, CSO remains capable of reading or modifying the exchanged information, such that eMSP has no means of verifying that the data received from CSO is the same as the one generated by EVSE. We assume that integrity is "partial", because the attacker can have limited control over modifications or compromised components. Finally, we consider availability to be "partial". This is because, the denial of service attacks can reduce the system performance, such that the resources of the impacted component might get delayed but not fully unavailable.

Vulnerability V_3: Application Layer Security

Due to the lack of inherent end-to-end security at the application layer, this vulnerability can be remotely exploited. Thus, we consider *Access Vector* to be "network". Also, *Access Complexity* is "low", whenever any legitimate entity acts as an attacker. Furthermore, we give *Authentication* a value of "none". This vulnerability is a sort of uncertainty of a system to verify whether the received information is correct or not. Therefore, we assign to the *Impact Metrics*' confidentiality and availability a value of "undefined". However, since modified information can be sent and received by victim eMSP or CSO, then integrity has a value of "partial".

5.3.2. Temporal Metric Group

Vulnerability V_1: Static Credentials for Authentication

We assume *Exploitability* to be "functional exploitation", as numerous exploitation techniques exist. Because this vulnerability type of OCPI can cause issues, which can be temporarily fixed by official vendors, then we assign *Remediation Level* a value of "temporary fix". Moreover, as sufficient details are published about the vulnerabilities and possible attacks on OCPI-based communications, we consider *Report Confidence* to be "reasonable".

Vulnerability V_2: Transport Layer Security

For this type of vulnerability, we consider *Exploitability* to be "PoC code", because exploitation techniques do not work for all situations such that extensive modifications are required by skilled attackers. For the same reasons as the ones of the vulnerability of V_1, we give *Remediation Level* and *Report Confidence* a value of "temporary fix" and "reasonable" respectively.

Vulnerability V_3: Application Layer Security

We give *Exploitability* a value of "PoC code", since exploitation techniques do not work for all situations, such that extensive modifications are required by skilled attackers. As protocols for the communication between CSO and eMSP do not consider end-to-end security as a priority, then we consider *Remediation Level* to be "workaround". Because sufficient information are published about this vulnerability and possible attacks on OCPI-based communication, then we give *Report Confidence* a value of "reasonable".

5.3.3. Environmental Metric Group

Vulnerability V_1: Static Credentials for Authentication

When an attacker intrudes inside the system, the disclosure of customer's identification information and charging-related messages can have limited adverse effects on the system or on individuals in the form of energy theft or privacy issues. For this reason, we consider confidentiality of the *Security Requirements* metric to be "low". Since tampering of messages can create a problem for the system to maintain the correctness of its records, then integrity is "medium". As the loss of availability of communication between CSO and eMSP cannot happen in this vulnerability, therefore we assign availability a value of "undefined".

Vulnerability V_2: Transport Layer Security

Due to the same reasons as the ones for the vulnerability V_1, we assume confidentiality and integrity of the *Security Requirements* metric to be "low" and "medium" respectively. As the loss of availability could have limited adverse effects on the system, we set availability to be "low".

Vulnerability V_3: Application Layer Security

Since modification of business-related information could have a limited effect on the overall system, then we assume confidentiality and availability to be "undefined", and integrity to be "low".

5.3.4. Overall Score

Based on the above-mentioned justifications on the different considered metrics, we calculated the overall score for the three vulnerabilities V_1, V_2 and V_3 separately for the communication between CSO and eMSP. The obtained results are shown in Table 5, indicating an overall vulnerability score of 7 (high), 6.2 (medium) and 3.0 (low) for V_1, V_2 and V_3 respectively.

5.4. DSO-CSO and -eMSP

The communication between DSO and CSO as well as eMSP takes place in order to realise demand-side integration through the advanced metering infrastructure (AMI). It can be observed from Figure 3 that the corresponding communication is achieved through the OpenADR and OSCP protocols. To compute its overall vulnerability score, we identified two different vulnerabilities related to those protocols: lack of key management system, and vulnerabilities in AMI. Furthermore, for each of these two type of vulnerabilities, we considered assumptions and gave justifications to them, so that the overall score is computed.

Table 5. Summary of the vulnerability analysis for the CSO-eMSP sub-systems communication. The parameter values indicate our choice to the different metrics of the CVSS methodology. Three different types of vulnerabilities V_1, V_2, and V_3 are identified for this communication.

Base Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**	**Parameter Values for V_3**
Access Vector	network	network	network
Access Complexity	low	medium	low
Authentication	none	none	none
Confidentiality Impact	complete	complete	undefined
Integrity Impact	complete	partial	partial
Availability Impact	none	partial	undefined
Temporal Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**	**Parameter Values for V_3**
Exploitability	functional exploitation	PoC code	PoC code
Remediation Level	temporary fix	temporary fix	workaround
Report Confidence	reasonable	reasonable	reasonable
Environmental Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**	**Parameter Values for V_3**
Confidentiality Requirement	low	low	undefined
Integrity Requirement	medium	medium	low
Availability Requirement	undefined	low	undefined
Overall vulnerability score	**7**	**6.2**	**3.0**

5.4.1. Base Metric Group

Vulnerability V_1: Lack of Key Management System

Since this vulnerability can be remotely exploitable, we assume that *Access Vector* has a value of "network". Furthermore, we consider *Access Complexity* to be "low" as a legitimate entity can act as an attacker. We give *Authentication* a value of "none" because such an action is not required by attackers. Consequently, the attackers can have full access to the device, which can violate confidentiality and integrity requirements of user-related data. Hence, we assign to both of those metrics a value of "partial", and to availability a value of "undefined".

Vulnerability V_2: Vulnerabilities in AMI

The advance metering infrastructure (AMI) enables the automated collection of metering data from smart meters. Furthermore, it facilitates the realisation of demand-side management through the OpenADR protocol [43]. Therefore, any hardware design flaw or weak encryption modules in smart meters can directly affect the data collection required for billing. Moreover, smart meters do not have high computational capabilities to process powerful encryption algorithms, making them vulnerable to hacking and data leakage. Hence, we assume that *Access Vector* has a value of "network", because attackers can exploit the smart meters through any DoS attack such as collision in the channel, flooding or jamming, etc. Furthermore, we give *Access Complexity* a value of "low", since exploiting this vulnerability does not require any user interaction. Finally, as the user's data can be disclosed and tampering of meter readings is also possible up to certain extent, then we give the *Impact Metrics*' confidentiality and integrity a value of "partial". We assume availability to have a value of "low", since attackers can also make any particular meter unavailable.

5.4.2. Temporal Metric Group

Vulnerability V_1: Lack of Key Management System

We assign *Exploitability* a value of "PoC code" because exploitation techniques do not work for all situations. Extensive modifications are required by a skilled attacker

due to high-level security provided by the OpenADR protocol. Furthermore, we assign *Remediation Level* a value of "temporary fix" whenever the system uses mechanisms to identify false requests. Finally, we assume that *Report Confidence* has a value of "unknown".

Vulnerability V_2: Vulnerabilities in AMI

We consider *Exploitability* to be "PoC code" because the exploitation techniques do not work for all situations: A skilled attacker requires extensive modifications due to the high level of security provided by OpenADR. The aforementioned vulnerability of OpenADR is explained by non-official vendors. However, unavailability of any meter or unexpected meter readings can easily be identified by the system. Consequently, we assume *Remediation Level* to be "temporary fix" by official vendors. As sufficient information are published about these vulnerabilities of smart meters and possible attacks on OpenADR-based communication, we assign *Report Confidence* a value of "reasonable".

5.4.3. Environmental Metric Group

Vulnerability V_1: Lack of Key Management System

Disclosure and modification of data on one or few links in a network could have only a limited effect on the overall system. As a matter of fact, we assign *Security Requirements* metric's confidentiality and integrity a value of "low", and availability a value of "undefined".

Vulnerability V_2: Vulnerabilities in AMI

The loss of smart meter's availability can have limited adverse effects on the individual level or the reputation of the company. Thus, we assign availability requirement a value of "low". On the other hand, since the modification or disclosure of consumer's information can make even adverse effects on the grid or demand-response systems, then we assume that integrity and confidentiality have a value of "medium".

5.4.4. Overall Score

Based on the above-mentioned justifications on the different considered metrics, we calculated the overall score for the two vulnerabilities V_1 and V_2 separately for the communication between DSO with CSO and eMSP. The obtained results are shown in Table 6, indicating an overall vulnerability score of 3.9 (low), and 4.9 (medium) for V_1 and V_2 respectively.

5.5. Summary of the Results

In this section, we present the obtained results in a nutshell by taking into account the following two scenarios:

- Scenario 1: In case more than one vulnerability exist within the communication of a given sub-system (e.g., 3 vulnerabilities for CSO-eMSP), we consider the worst score of the vulnerabilities as the one for the whole sub-system.
- Scenario 2: In case more than one vulnerability exist within the communication of a given sub-system (e.g., 3 vulnerabilities for CSO-eMSP), we consider the average score of those vulnerabilities as the one for the whole sub-system.

Figure 5 summarises the results of the carried out vulnerability analysis of each pair of communicating sub-systems, by considering the above-mentioned two scenarios. It can be noticed that for the considered both scenarios, the communicating pairs of EVSE-CSO and CSO-eMSP sub-systems are the most vulnerable than the remaining ones. More precisely, by considering Scenario 1, both of the sub-systems EVSE-CSO and CSO-eMSP have high vulnerabilities, DSO-CSO and DSO-eMSP have medium vulnerabilities, whereas the sub-system EV-EVSE has the lowest vulnerabilities. This is also the case, when considering Scenario 2, where DSO-CSO has the lowest vulnerabilities, whereas the other sub-systems have medium vulnerabilities.

Table 6. Summary of the vulnerability analysis for the DSO-CSO and DSO-eMSP sub-systems communication. The parameter values indicate our choice to the different metrics of the CVSS methodology. Two different types of vulnerabilities V_1 and V_2 are identified for this communication.

Base Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**
Access Vector	network	network
Access Complexity	low	low
Authentication	none	none
Confidentiality Impact	partial	partial
Integrity Impact	partial	partial
Availability Impact	undefined	low
Temporal Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**
Exploitability	PoC code	PoC code
Remediation Level	temporary fix	temporary fix
Report Confidence	unknown	reasonable
Environmental Metrics	**Parameter Values for V_1**	**Parameter Values for V_2**
Confidentiality Requirement	low	medium
Integrity Requirement	low	medium
Availability Requirement	undefined	low
Overall vulnerability score	**3.9**	**4.9**

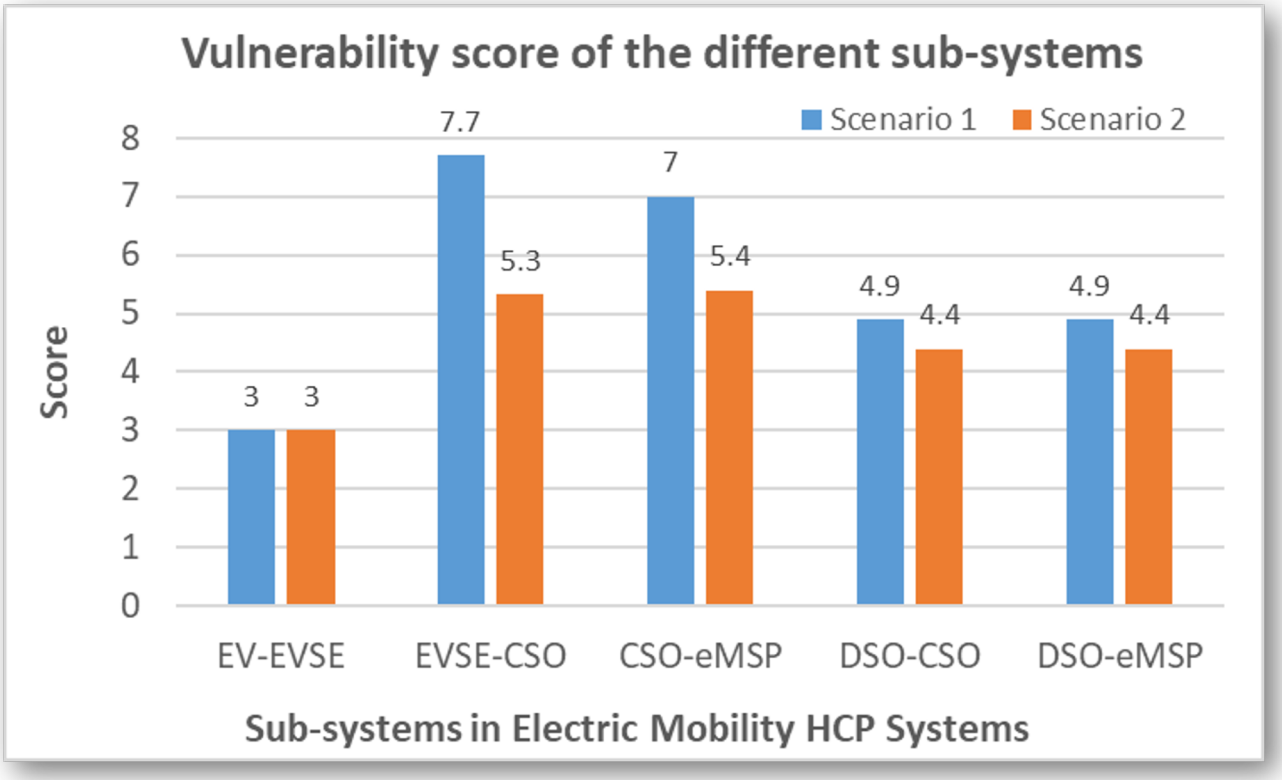

Figure 5. Summary of the vulnerability scores of the different sub-systems by considering two different scenarios. In case more than one vulnerability exist for each communicating sub-system, Scenario 1 and Scenario 2 consider the worst and average values to compute the overall vulnerability score.

6. Conclusions

Cyber-security of human-centred cyber physical systems has lately received considerable attention. This is because such systems consist of several sub-systems which are interconnected with each other through information and communications technology, whereas the vulnerability of one sub-system threatens the whole system. Risk assessment of such complex systems is particularly difficult due to the needed modelling requirements. Usually, it is not possible to quantitatively assess the level of threats as in practice there is a lack of available data. Consequently, the cyber-security risks of real-world systems are assessed by analysing the vulnerabilities of the system under study either qualitatively (e.g., low, medium, high) or semi-quantitatively (e.g., bucket or scoring system).

In this paper, we considered a human-centred cyber physical system for the context of electric mobility. For this purpose, we studied the vulnerabilities of the end-to-end communicating sub-systems. We adopted the common vulnerability scoring system (CVSS) methodology in order to semi-quantitatively assess the vulnerabilities between every pair of communicating sub-systems. To achieve this, we carried out an exhaustive literature review [7–18], which later helped us in considering well-justified assumptions. Using those assumptions, we assigned values to the different parameters of the three metric groups of the CVSS. Based on those parameters and their corresponding values, we calculated the overall vulnerability score for each pair of communicating sub-systems of (1) EV-EVSE, (2) EVSE-CSO, (3) CSO-eMSP, and (4) DSO-CSO as well as DSO-eMSP. In most of the above-mentioned communicating sub-systems, there exist more than one vulnerability. As a matter of fact, we derived the score for each of the vulnerabilities, and then considered two different scenarios. Scenario 1 always considers the worst vulnerability score, whereas Scenario 2 takes the average to compute the overall score. We showed that among the five different communicating sub-systems, the ones of CSO-eMSP and CSO-EVSE have high vulnerability scores for both scenarios. Consequently, we conjecture that those two sub-systems are the weakest part of the end-to-end communicating chain of electric mobility human-centred cyber physical systems.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study in this paper did not report any data.

Acknowledgments: The author of this paper would like to show his gratitude to Shaista Hussain and the Share&Charge company for their valuable comments especially related to Section 5 of this manuscript.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript.

AMI	advanced metering infrastructure
CIA	confidentiality, integrity and availability
CS	charging station
CSO	charging station operator
CPS	cyber physical system
CVSS	common vulnerability scoring system
DoS	denial-of-service
DSO	distribution system operator
EMSA	e-mobility system architecture
eMSP	e-mobility service provider
EV	electric vehicle
EVSE	electric vehicle supply equipment
HCPS	human-centred CPS

ICT	information and communications technology
MiM	man-in-the-middle
OCN	open charging network
OCPI	open charge point interface
OCPP	open charge point protocol
OICP	open inter charge protocol
OpenADR	open automated demand response
OSCP	open smart charging protocol
SCADA	supervisory control and data acquisition

References

1. Lee, E.A. Cyber Physical Systems: Design Challenges. In Proceedings of the 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008; pp. 363–369. [CrossRef]
2. Eider, M.; Sellner, D.; Berl, A.; Basmadjian, R.; de Meer, H.; Klingert, S.; Schulze, T.; Kutzner, F.; Kacperski, C.; Stolba, M. Seamless Electromobility. In Proceedings of the Eighth International Conference on Future Energy Systems, e-Energy '17, Hong Kong, China, 16–19 May 2017; pp. 316–321. [CrossRef]
3. Basmadjian, R.; Kirpes, B.; Mrkos, J.; CuchÃ½, M. A Reference Architecture for Interoperable Reservation Systems in Electric Vehicle Charging. *Smart Cities* **2020**, *3*, 1405–1427. [CrossRef]
4. Lee, R.; Assante, M.; Conway, T. *Analysis of the Cyber Attack on the Ukrainian Power Grid-Defense Use Case*; Technical Report; Industrial Control System, 2016. Available online: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf (accessed on 10 March 2021).
5. Volkova, A.; Niedermeier, M.; Basmadjian, R.; de Meer, H. Security Challenges in Control Network Protocols: A Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 619–639. [CrossRef]
6. Sherwood, J.; Clark, A.; Lynas, D. *Enterprise Security Architecture: A Business-Driven Approach*; CRC Press: Boca Raton, FL, USA, 2005.
7. Zweistra, M.; Janssen, S.; Geerts, F. Large Scale Smart Charging of Electric Vehicles in Practice. *Energies* **2020**, *13*, 298. [CrossRef]
8. Paverd, A.J.; Martin, A.P.; Brown, I. Security and Privacy in Smart Grid Demand Response Systems. In *Smart Grid Security. SmartGridSec 2014. Lecture Notes in Computer Science*; Cuellar, J., Ed.; Springer: Cham, Switzerland, 2014; Volume 8448, pp. 1–15.
9. Ding, D.; Han, Q.L.; Xiang, Y.; Ge, X.; Zhang, X.M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
10. Vaidya, B.; Mouftah, H.T. Multimodal and Multi-pass Authentication Mechanisms for Electric Vehicle Charging Networks. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 371–376. [CrossRef]
11. Bao, K.; Valev, H.; Wagner, M.; Schmeck, H. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Comput. Sci. Res. Dev.* **2017**, *33*, 3–12. [CrossRef]
12. Morosan, A.G.; Pop, F. OCPP Security-Neural Network for Detecting Malicious Traffic. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, RACS '17, Krakow, Poland, 20–23 September 2017; pp. 190–195. [CrossRef]
13. Alcaraz, C.; Lopez, J.; Wolthusen, S. OCPP Protocol: Security Threats and Challenges. *IEEE Trans. Smart Grid* **2017**, *8*, 2452–2459. [CrossRef]
14. van Aubel, P.; Poll, E.; Rijneveld, J. Non-Repudiation and End-to-End Security for Electric-Vehicle Charging. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania, 29 September–2 October 2019; pp. 1–5. [CrossRef]
15. Rubio, J.E.; Alcaraz, C.; Lopez, J. Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. [CrossRef]
16. Lee, S.; Park, Y.; Lim, H.; Shon, T. Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology. In Proceedings of the 2014 International Conference on IT Convergence and Security (ICITCS), Beijing, China, 28–30 October 2014; pp. 1–4. [CrossRef]
17. Vaidya, B.; Mouftah, H.T. Deployment of Secure EV Charging System Using Open Charge Point Protocol. In Proceedings of the 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 922–927. [CrossRef]
18. Van Keulen, J. *Smart Charging: A Privacy and Security Analysis*; Radboud Universiteit: Nijmegen, The Netherlands, 2014; pp. 1–67.
19. Kirpes, B.; Danner, P.; Basmadjian, R.; de Meer, H.; Becker, C. E-Mobility Systems Architecture: A Framework for Managing Complexity and Interoperability. *Submitt. Energy Inform. (Preprint)* **2019**, *2*, 1–30. [CrossRef]
20. CEN-CENELEC-ETSI Smart Grid Coordination Group. *Smart Grid Reference Architecture*; Technical Report; CEN-CENELEC-ETSI: New Delhi, India, 2012.
21. Open Clearing House Protocol. Available online: http://www.ochp.eu/ (accessed on 17 March 2021).
22. Open Intercharge Protocol. Available online: https://www.hubject.com/en/downloads/oicp/ (accessed on 17 March 2021).

23. Open Charge Point Interface Protocol. Available online: https://ocpi-protocol.org/ (accessed on 17 March 2021).
24. Open Smart Charging Protocol. Available online: https://www.openchargealliance.org/protocols/ (accessed on 17 March 2021).
25. Open Charge Point Procotol. Available online: https://www.openchargealliance.org/protocols/ocpp-20/ (accessed on 17 March 2021).
26. Open Automated Demand Response. Available online: https://www.openadr.org/. (accessed on 17 March 2021).
27. ISO 15118-1:2013. Available online: https://www.iso.org/standard/55365.html. (accessed on 17 March 2021).
28. IEC 61851. Available online: https://www.vde-verlag.de/iec-normen/224263/iec-61851-1-2017.html. (accessed on 17 March 2021).
29. Falk, R.; Fries, S. Electric Vehicle Charging Infrastructure-Security Considerations and Approaches. In Proceedings of the Fourth International Conference on Evolving Internet (INTERNET), Venice, Italy, 24–29 June 2012; pp. 1–7.
30. Lim, H.; Ko, J.; Lee, S.; Kim, J.; Kim, M.; Shon, T. Security Architecture Model for Smart Grid Communication Systems. In Proceedings of the 2013 International Conference on IT Convergence and Security (ICITCS), Macau, China, 16–18 December 2013; pp. 1–4. [CrossRef]
31. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. Smart electric vehicle charging: Security analysis. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24 February 2013; pp. 1–6. [CrossRef]
32. *Guidelines for Smart Grid Cyber Security: Volume 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*; Technical Report; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2010.
33. Dondossola, G.; Terruggia, R. Cyber Security of Smart Grid Communications: Risk Analysis and Experimental Testing. In *Cyber Physical Systems Approach to Smart Electric Power Grid*; Khaitan, S.K., McCalley, J.D., Liu, C.C., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 169–193.
34. Tymchuk, O.; Iepik, M.; Sivyakov, A. Information Security Risk Assessment Model Based on Computing with Words. *MENDEL* **2017**, *23*, 119–124. [CrossRef]
35. NIST; Aroms, E. *NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems*; CreateSpace: Scotts Valley, CA, USA, 2012.
36. Howard, M.; LeBlanc, D. *Writing Secure Code*; Best Practices Series; Microsoft Press: Redmond, WA, USA, 2003.
37. Mell, P.; Scarfone, K.; Romanosky, S. Common Vulnerability Scoring System. *IEEE Secur. Priv.* **2006**, *4*, 85–89. [CrossRef]
38. *OWASP Top 10-2017 The Ten Most Critical Web Application Security Risks*; Technical Report; The Open Web Application Security Project: Annapolis, MD, USA, 2017.
39. *Tailoring for MIL-STD-882E Including SMC Safety Requirements*; Technical Report; US Department of Defense: Washington, DC, USA, 2019.
40. SIG Questionnaire. Available online: https://sharedassessments.org/sig/ (accessed on 17 March 2021).
41. Deloitte. Available online: https://www2.deloitte.com/de/de.html (accessed on 17 March 2021).
42. Open SSL. Available online: https://www.openssl.org/news/vulnerabilities.html (accessed on 17 March 2021).
43. Basmadjian, R. Flexibility-Based Energy and Demand Management in Data Centers: A Case Study for Cloud Computing. *Energies* **2019**, *12*, 3301. [CrossRef]