OCPP in the spotlight: Threats and countermeasures for electric vehicle charging infrastructures 4.0

Cristina Alcaraz[1], Jesus Cumplido[1], and Alicia Triviño[2]

[2]Computer Science Department, University of Malaga, Spain

[4]Electrical Engineering Department, Unviersity of Malaga, Spain

[1]{alcaraz,cumplido}@uma.es, [2]{atc}@uma.es

Abstract

Undoubtedly, Industry 4.0 in the energy sector improves the conditions for automation, generation and distribution of energy, increasing the rate of electric vehicle manufacturing in recent years. As a result, more grid-connected charging infrastructures are being installed, whose Charging Stations (CSs) can follow standardized architectures, such as the one proposed by the Open Charge Point Protocol (OCPP). The most recent version of this protocol is v.2.0.1, which includes new security measures at device and communication level to cover those security issues identified in previous versions. Therefore, this paper analyzes OCPP-v2.0.1 to determine whether the new functions may still be susceptible to specific cyber and physical threats, and especially when CSs may be connected to microgrids. To formalize the study, we first adapted the well-known threat analysis methodology, STRIDE, to identify and classify threats in terms of control and energy, and subsequently we combine it with DREAD for risk assessment. The analyses indicate that, although OCPP-v2.0.1 has evolved, potential security risks still remain, requiring greater protection in the future.

Keywords: Electric Vehicle Charging infrastructures Industry 4.0 OCPP Microgrid Cybersecurity Risk management.

1 Introduction

Governments and institutions are supporting the Electric Vehicle (EV) market since they are aware of the environmental advantages of this mode of transport. Due to the limitations of the battery capacity, EV owners are expected to charge their vehicles in multiple locations (including their home, work place or with public infrastructure) [26]. The research community is analyzing in depth where to place and how to operate EV Charging Stations (CSs), as uncontrolled charging of these vehicles poses a technological challenge for Smart Grids [41]. From these studies, it is recommended that future power systems must incorporate advanced control algorithms to ensure reliability, safety and security while coping with the relevant changes affecting the grid.

Guaranteeing reliability, safety and security in power systems with high power levels and an increasing number of assets (e.g., EVs) is becoming complex. Current research efforts propose dividing the power system into smaller interconnected units, known as Microgrids (MGs) in order to simplify the control and to make it more robust. In the context of Industry 4.0, an MG employs advanced information technologies, communication networks, protocols and sophisticated information processing to monitor and control power generation, distribution and consumption processes in more efficient and robust way [13]. To do so, it is necessary to optimize the management of electrical, communication and control elements, which are tightly coupled resulting in cyber-physical MGs. As a Cyber-Physical System (CPS), an MG is susceptible to cyber-attacks which may compromise its performance, maintainability and integrity. Specifically, an attacker can maliciously exploit its components and interdependence to damage the MG, degrade its performance and even interfere with the external power network. In fact, the MG's voltage and frequency stability, power balance, and dispatch are highly dependent on secure and healthy cyber-systems to ensure that the MG assets are controlled correctly [47].

Previous works have already studied the vulnerabilities of MGs focusing on some of their components. For example, some studies have already identified the threats to voltage source converters and their controls [42] [30]. However, there are still many security issues to consider in the MGs. Due to the impact of EVs on MGs and the stress their charging may generate, numerous research works conclude that the Charging Infrastructure (CI) could provoke high risks with a high probability, as they are easily accessible for the public [11], [44]. Consequently, it is necessary to study the new CIs required in the future from a cybersecurity point of view. Academia and industry have already identified vulnerabilities in the communication between the EV and the CS, the EV operator interfaces, the Internet and the maintenance interface of the CS [22], but a deeper analysis is fundamental to consider the communication and information processing done by these elements in the context of Industry 4.0.

In this paper, we identify the threats and risks posed to EV public CSs in MGs corresponding to the new generation of Industry 4.0, including those risks related to the communication infrastructure, Information Technologies (ITs) involved in the control, and the MG power assets. Due to its popularity, we assume that CSs use the Open Charge Point Protocol (OCPP) for the Charging Transactions (CTs). Specifically, we analyze OCPP-v2.0.1 [36], which includes new functions not analyzed and covered in its previous versions [8]. Some of these functions are: device management, improved transaction handling, support for ISO 15118 (related to incorporate the communication between the EV and the CS) [1, 2], display and messaging support, smart charging functions, and even new security functions compared to OCPP-v1.6 [35] that need to be assessed with respect to possible security and safety risks. To identify these risks, we use a common risk management approach for the analysis, extending it according to the methodology also applied in [24]. Namely, we study the threats using a formal method to detect how attackers can compromise both control and energy assets. In this sense, we adapted the STRIDE methodology to contemplate two relevant aspects: (i) the inclusion of energy hazards, and (ii) the combined use of STRIDE with the DREAD assessment model to deepen the analysis process by contemplating possible risks [3].

STRIDE is a simple method, originally conceived to classify threats according to the aim of the attack in software (SW) developments [25]. Specifically, the STRIDE model identifies six categories of threat: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege (defining the acronym for STRIDE). Some recent works have already applied the STRIDE methodology in monitoring systems and in cyber-physical energy systems, but mainly focus their approaches on the consequences of the control processes [46] [51]. Since MGs have both SW and energy system components, we also apply the STRIDE model to comprise energy-specific threats as also considered in [16]. This related work includes a recent survey on security issues in OCPP. The main difference between our work and that of [16] lies in the level of study and depth of the OCPP-v2.0.1 protocol by computing risks through two well-known risk management methodologies, STRIDE+DREAD. The comprehensive view that we get with this combination of methodologies even allows us to identify which types of threats require greater attention in the future, especially now with the new technological currents of Industry 4.0 spreading within the sector.

Regarding the combined use of STRIDE+DREAD, it is important to note that DREAD classifies security threats according to five characteristics: Damage, Reproducibility, Exploitability, Affected Users and Discoverability (which defines the acronym DREAD). Thus, our research aims to combine both approaches (STRIDE+DREAD) to evaluate a set of risks in control (c) and energy (e) assets, referring this combination to as STRIDE-DREAD$^{\mathrm{c+e}}$ (henceforth SD$^{\mathrm{c+e}}$). This grouping facilitates us to later provide a set of countermeasures, considering the particularities of the MG in the context of Industry 4.0. Therefore, **the main contributions** of this work are:

- Adaptation of the threat analysis method STRIDE to a system with control and energy assets. In particular, we consider a scenario with public EV Charging Infrastructure (EVCI) and a MG-based control. In the context of Industry 4.0, we extract a specific taxonomy of threats related to the OCPP protocol, v2.0.1, demonstrating the susceptibility of the protocol to multiple types of attacks.

- Combination of methodologies STRIDE+DREAD to determine the level of severity of each attack on control and energy assets.

- Identification of a set of mitigation actions, prioritizing each action according to the analysis made by SD$^{\mathrm{c+e}}$ to reduce possible consequences and impact.

The paper is structured as follows: Section 2 proposes a formal architecture of the MG components, highlighting the role of CSs and their control. Section 3 presents SD^{c+e} for EVCIs, describing how we apply the extended STRIDE methodology together with the DREAD model for threat assessment. Section 4 analyzes the influence of mitigation solutions, while Section 5 outlines the conclusions and future work.

2 Architecture and stakeholders

A MG is a local power system formed by Distributed Energy Resources (DERs) and based on multiple stakeholders: suppliers, customers (as EVs), technical operators and engineers [27, 40]. The implementation of a MG involves considering one of the following three main operational approaches: (i) to operate as an independent power system during its lifetime; (ii) to be fully connected to another power system and use it to complement energy from local DERs and storage systems; and (iii) to switch from the isolated and connected modes in order to rely on the external power system when local resources cannot satisfy local demand. In the next subsections, we first analyze the architecture of a MG with EVs considering these three operational modes. Then, we will describe the role of the stakeholders for the aforementioned operational conditions.

2.1 Architecture

In [45] and [39], the authors present the fundamental components of a MG, which mainly consists of three layers: (i) physical layer containing electrical devices; (ii) communication layer; and (iii) cyber layer. A set of ITs runs in these three layers, and they are responsible for controlling operations through the different processing and decision-making techniques of a Central Control System (CCS). These ITs must converge with existing Operational Technologies (OTs), introducing the benefits of Industry 4.0 (better automation, autonomy, access and control) into EVCIs [7]. This CCS is able to manage the control signals from the controllers and actuators in order to optimize energy production levels and the MG stability. The installation of the Energy Management System (EMS) is within the CCS. Its main purpose is to monitor, control and optimize the performance of the MG operations. It performs a set of control functions to maintain safety, reliability, economy, resilience, sustainability, and efficiency in the system [34]. Another main component of the CCS is the CS Management System (CSMS), which is responsible for efficiently managing the collection transactions requested by end users in all its CSs (usually deployed in public places). A communication network composed of various wireless and wired network devices, communication infrastructures and industrial communication protocols allows the data flows collected by the sensors and the transmission of the operations sent by the CCS. OCPP corresponds to an open application protocol that establishes communication between the CSs and the CSMS, and even the EMS [36].

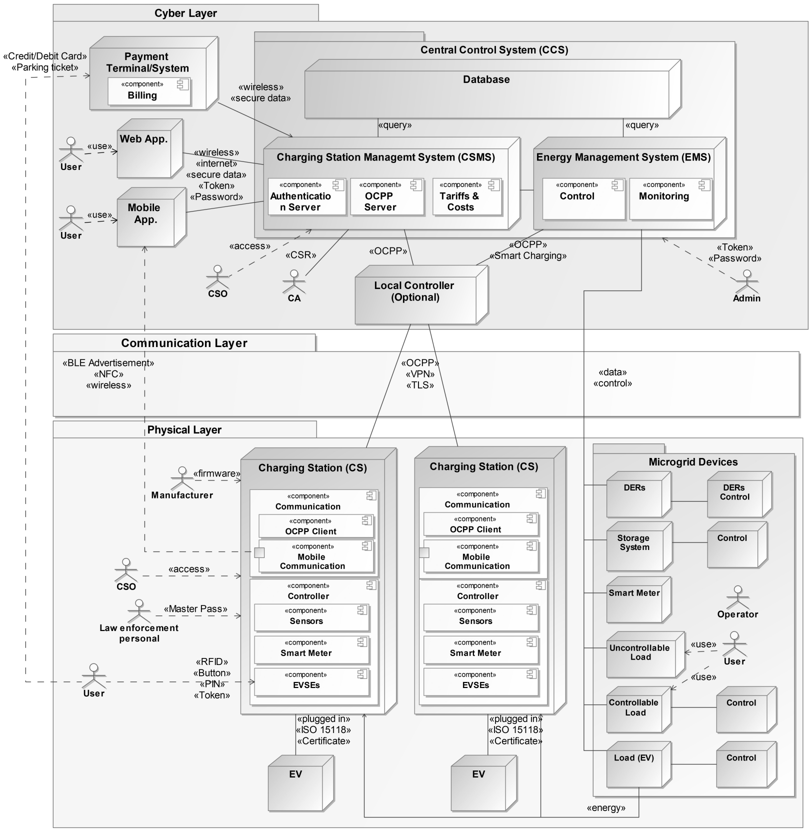

Figure 1: A charging stations-based microgrid architecture under the OCPP-v2.0.1 conceptualization

The architecture that we follow in this paper aims to model an advanced EVCI in an MG operating with an electricity market where users pay for electricity consumption to charge their EVs. In this architecture, users can reserve power at a predetermined CS connector, and the connection may be initiated automatically, with no manual intervention. The system can, therefore, activate a connector and start to charge the EV battery. This request is managed in two ways, depending on the scenario implemented. The first allows the user to start a CT via a mobile, web application or a payment terminal/system (using a credit/debit card or a parking ticket), where the CSMS manages the transaction request. To do so, the CSMS is responsible for authenticating the user and sending the transaction operation to the corresponding CS. The second way to request CTs allows the user to authenticate himself/herself using the authentication resources of the CSs and the resources supported by the OCPP protocol, such as an RFID tag, button (no authentication required), PIN, EV certificate or unique token. The CS forwards the request to the CSMS which accepts or denies the user's request and authorizes the CS to start the CT. Note that the CS is also able to handle the request without previously communicating with the CSMS if it is in offline mode. In the following sections, we will discuss these authentication modes in more detail.

As can be seen in Figure 1, the architecture counts with a set of distributed CSs that operate and communicate with the CSMS, included in the CCS, via the specialized OCPP protocol, which provides a secure interaction with users and EVs as controllable loads. In addition, the MG powers the CSs and the CCS control and manage the CSs. Each CS relies on different SW and hardware (HW) modules, which enable intelligent operability and secure communication between the internal devices. These modules have been classified into two parts: communication assets and the controller. In the communication part, it is possible to find (i) the OCPP communication, where the OCPP client is able to connect to the OCPP server in the CSMS, but also (ii) different ways to connect with the end user such as Bluetooth Low Energy (BLE) advertisements or Near-Field Communication (NFC) to display the nearby CSs to the user. Thanks to the communication elements, the user can visualize the status of the connectors and send a new request to the CSMS. On the other hand, the controller part of the CS contains three main components. The first component constitutes telemetry elements working as "sensors". These sensors are devoted to collecting information on the electrical state of the CS, temperature, and other measures of energy consumption per CS. In this case, the "smart meters" are electronic devices with the capacity to compute information records such as consumption of electric energy, voltage levels, current and power factor. These devices are responsible for metering the total energy consumed in each CT, in order to facilitate user billing in the CSMS and real-time control demand in the EMS. The last main components of the controller part are the EV Supply Equipments (EVSEs), which include actuators in charge of activating/deactivating the connection and communication with the EVs.

2.2 Stakeholders

The CSMS is in charge of sending regularly the energy consumption and reserve data of all CSs to the EMS. Subsequently, this information is processed and analyzed by the EMS to monitor and control the DERs according to the energy consumption and demand in the MG. Since EVs are controllable loads within the MG, the EMS would be responsible for monitoring the loads and their safe storage, and for supplying power to the CS connectors when needed. These functionalities are largely controlled by the OCPP protocol [36], corresponding to the smart charging functional block. This functional block describes all the functionality that enables the CS operator (or indirectly a third party, like the EMS) to influence the charging current/power of a CT, or set limits on the amount of power/current of a CS that can be supplied to an EV. It is feasible to negotiate these current and power limits in the CSs during the CTs with the EVs through a bidirectional communication standard ISO 15118 [1,2]. Moreover, OCPP offers the possibility to use a local controller, which is deployed between the CSMS (or the EMS) and any number of CSs creating a local group. It is located close to the CSs (and may even be wired to the CSs), and works so that the CSMS and the EMS are not aware if the CS is connecting to it directly, or via the local controller.

In addition to the users requesting CTs from the CSMS or directly from the CS with their EVs connected to the CS connectors, there are other possible parties involved in a CS-based MG, as shown in Figure 1. For example, the MG may adapt the power levels of the CIs as a consequence of a relevant growth of controllable/uncontrollable loads. If at certain hours these customers demand high energy from DERs, this may have repercussions for the current/power charging limits of the CSs. Other involved stakeholders are (i) the manufacturers of the firmware installed in each CS; (ii) the operators who have full access to the DERs; and (iii) the CS Operators (CSOs), who have the possibility to interact by performing OCPP operations and configurations on the system through the CSMS or directly on the CSs. Moreover, OCCP-v2.0.1 incorporates two new actors: (i) law enforcement personal, who could stop any ongoing transaction via a Master Pass ID (e.g., a Master Pass RFID tag) with the intention of disconnecting any EV that has to be towed away; and (ii) Certificate Authorities (CAs), which have the function of validating and signing certificates generated by the CSMS. Finally, IT administrators can have access to the CSMS and EMS processes and configuration variables, as well as having full access to databases, containing telemetry values, control data or security configurations/data. We subsequently consider all these actors as possible malicious agents in the threat analysis presented in the following sections.

With the incorporation of new ITs, multiple communications infrastructures and the wide set of actors, it is essential to consider the diverse security risks posed by the new generation of MGs. As can be seen from the architecture, the OCPP protocol bears a major responsibility in the communication processes between the CSMS and CSs, and between the EMS and CSs. In [8], the same cybersecurity issues were already discussed, but focused on OCPP-v1.6.

Table 1: STRIDE threat model based on [32]

Property	Threat	Definition
Authentication	**S**poofing	Unlawful access and illicit use of another user's authentication information
Integrity	**T**ampering	Deliberate modification of data, configurations and source codes
Non-repudiation	**R**epudiation	Claiming to have not performed an action
Confidentiality	**I**nformation Disclosure	Exposing information to someone not authorized to see it
Availability	**D**enial of Service (DoS)	Denial or degradation of requested services, resources or data
Authorization	**E**levation of Privilege	Gaining capabilities without proper authorization to access resources, data or services

Now, OCPP has upgraded its version to v2.0.1, which includes new security functionalities such as device management using certificates x.509, support for ISO 15118, secure firmware updates and encrypted communication via Transport Layer Security (TLS). But even so, a security analysis is still necessary to identify the new security issues in this new version of OCPP. For that reason, the following sections aim to extract a set of threats that may be found in OCPP-enabled CSs, considering STRIDE+DREAD.

3 SD^{c+e}: Threat model and analysis

To identify vulnerabilities and threats, we apply the STRIDE threat model proposed by Microsoft [31, 32].

3.1 Main STRIDE phases and related work

As stated above, STRIDE classifies the threats into six categories (cf. Table 1). This model is widely used due to its straightforward methodology, which is simple and easy to apply, where threats are analyzed and identified manually in each of the system components [20]. For example, in work [25], the STRIDE methodology is applied for CPS-based applications using five steps; while work in [24] applies one more step (see also Figure 2) in order to assess the effect of the threats for cyber-enabled ships and establish mitigation actions. Considering the mentioned six-step approach [3], we then apply it to provide a more complete picture of threats and risks associated with CIs in a MG.

For the sake of clarity, the operation of the adapted methodology is described as follows. Step 1 consists in *decomposing the system into logical or structural components*. These can be internal or external processes or assets that interact and communicate with the system. Subsequently, a *Data Flow Diagram (DFD) is plotted* (Step 2) for each of the components, in order to visualize the functionalities inside and outside the system. Each DFD shows four standard symbols: (i) External Entity (EE), (ii) Data Flow (DF), (iii) Process (P), and (iv) Data

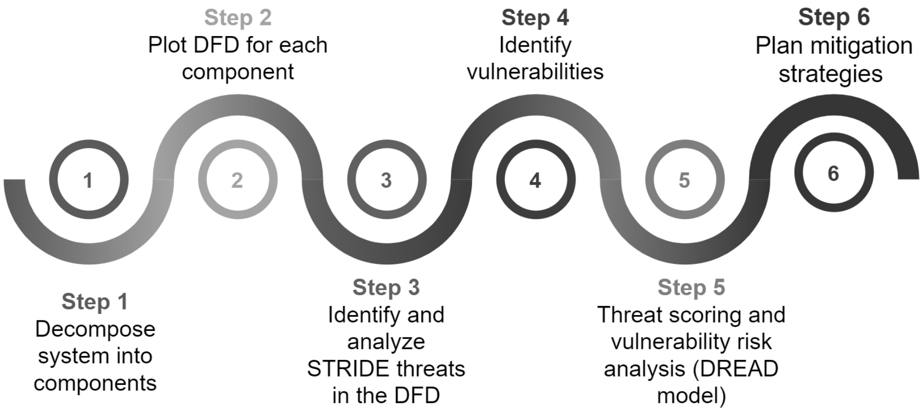
Step 2
Plot DFD for each component
Step 4
Identify vulnerabilities
Step 6
Plan mitigation strategies
1
2
3
4
5
6
Step 1
Decompose system into components
Step 3
Identify and analyze STRIDE threats in the DFD
Step 5
Threat scoring and vulnerability risk analysis (DREAD model)

Figure 2: STRIDE+DREAD methodology based on 6 steps, recommended by [3]

Table 2: DREAD approach to threat assessment

Procedure	To prioritize the threats, each threat is ranked from 1 to 10 following the five DREAD evaluation criteria, and then the scores are summed and divided by 5 (the number of criteria). The result is a numerical score between 1 and 10 for each threat. High scores indicate serious threats.
Criteria	**Description**
Damage	Data loss, HW or media failure, reduction of operational performance, or any similar damage
Reproducibility	How often a specified type of attack or threat is successful
Exploitability	The effort and expertise required to mount an attack or exploit a threat
Affected users	The number of users that could be affected by a threat
Discoverability	The likelihood that a threat will be exploited. This is difficult to estimate accurately

Table 3: Related work on security frameworks and approaches in cyber-physical (power) systems

Related work	Threat analysis	Risk assessment	Counter-measures	Based on power systems	Physical threats	CSs threats	OCPP threats	Energy threats
[25] (2017)	STRIDE			✓				✓
[37] (2019)	STRIDE		Proposed mitigations		✓			
[48] (2012)	STRIDE		Proposed mitigations					
[24] (2020)	STRIDE	DREAD	NIST guide to ICS security					
[29] (2020)	STRIDE	Likelihood and impact-based		✓	✓	✓		✓
[23] (2013)	STRIDE	Resistance, likelihood and impact-based	Proposed mitigations	✓		✓		
[18] (2021)	STRIDE	x	Proposed solution	✓		✓		✓
[51] (2021)	MITRE ATT&CK for ICS	Hybrid approach		✓	✓			✓
[10] (2013)	V2GP and V2GC threats		Proposed mitigations	✓	✓	✓		✓
[9] (2020)	Home and public CSs-based		Literature-based	✓		✓	✓	
[8] (2017)	OCPP-based			✓		✓	✓	
[40] (2018)	OCPP-based		Proposed solution	✓		✓	✓	
[38] (2021)	Domestic CS-based		Proposed solution	✓		✓	✓	
[44] (2022)	Public CS-based		Proposed electrical monitoring	✓		✓	✓	
[17] (2022)	OCPP-based	Reduced use cases				✓	✓	
[16](2022)	OCPP and literature-based		Literature-based	✓	✓	✓	✓	✓
SD^{c+e} (Our approach)	OCPP-based and STRIDE	DREAD	Proposed mitigations	✓	✓	✓	✓	✓

Store (DS). This subdivision facilitates the manual process of *identifying and analyzing STRIDE threats* (Step 3) in each asset of the DFD (STRIDE-per-asset) and in each interaction between assets (STRIDE-per-interaction). Once threats on control and energy assets are identified, the system *vulnerabilities are detected manually* (Step 4) by analyzing the possible causes and sources of the identified threats. After this, potential threats must be evaluated according to certain established criteria, in order to prioritize and mitigate their effects. This evaluation process coincides with Step 5 through the *DREAD model* proposed by Microsoft in [3]. DREAD prioritizes threats, managed by STRIDE, by simply calculating the risk that their effects may have in terms of damage, reproducibility, exploitability, affected users and discovery (cf. Table 2). With this information, it is now possible to more appropriately select mitigation strategies (Step 6) according to each threat score and risk prioritization.

With respect to the state of the art, STRIDE is one of the most widely used threat models in energy applications and CPSs. Khan *et al.* apply it to identify threats in a real synchrophasor-based synchronous islanding testbed [25], while Orellana *et al.* and Yampolskiy *et al.* adapt STRIDE and security tactics for designing secure CPS architectures in [37] and [48], respectively. There are other related works that combine STRIDE with other existing methodologies to (i) calculate risks using DREAD [24] or according to likelihood and impact [23,29], and (ii) to detect and mitigate attacks through neural networks [18]. Also, other threat models have been used for CPSs, such as STPA-sec, HAZOP, OCTAVE, PASTA, Abuser stories, Attack Trees, T-MAP and CORAS [20,25]. It is also possible to classify threats using the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework developed by MITRE Corporation in [15]. Related to this framework, Zografopoulos *et al.* provide an overview of the security of cyber-physical energy systems using the MITRE ATT&CK for Industrial Control System (ICS) repository [51]. There are also authors that manages the threats considering the specific CPS scenarios [8–10,38,40]. In [10], Atlantic and Ra describe two types of threats to the security of plug-in

EVs: Vehicle-to-Grid (V2G) physical threats (V2GP) and V2G communication threats (V2GC), and propose several mitigation strategies. In [9], Antoun *et al.* present a security assessment of the EVCI by analyzing cyber threats to home and public charging systems. Likewise, [8] and [40] identify the threats and key security properties of the OCPP-v1.6 protocol in power systems. With a perspective of the impact on the power system, Sayed *et al.* analyze some vulnerabilities of the protocols involved in the management of public charging infrastructures [44]. This includes the identification of vulnerabilities in the IEC protocols, the firmware, the ISO 15118 and the OCPPv-1.6. The analysis is performed without a risk assessment methodology, is based on simulating the variation of the active and reactive power of loads (associated to EVs) and evaluating the impact on the grid stability and performance. The authors propose monitoring the electrical performance of the CSs and the reactive power and the harmonic distortion of the grid as feasible countermeasures.

In [17], a penetration test considering three attack scenarios (erroneous data, long values and user interface manipulation) is performed for OCPP-v1.6, while the papers [38] and [16] include in their study the OCPP-v2.0.1 protocol. Indeed, in [38], a general vulnerability and mitigation analysis on domestic CSs is also provided according to some of the current protocols and standards, including OCPP-v2.0.1. However, the analysis is at a very high level, covering the fundamental differences with the previous version and several security challenges and recommendations. In [16], a recent survey about security issues and countermeasures in the OCPP protocol is found, stressing the main affected assets (EV, EVSE, CS, EMS, CSMS, data or grid). These three last studies differ from ours in the way in which OCPP is evaluated. Our work focuses on providing a comprehensive threat analysis of OCPP-v2.0.1, following the traditional STRIDE+DREAD methodology and enumerating a set of countermeasures.

To summarize, Table 3 shows a comparison of the frameworks and approaches used in the related work on CPS, and particularly on CS infrastructures. As the table shows, some related research work focus on threats to CIs such as [8–10, 23, 29, 40], but only some of them consider threats to the OCPP communication protocol such as [8, 9, 16, 17, 40]. From the table, we also highlight that none of the related work applies a STRIDE+DREAD-based threat and risk assessment model for specific CIs integrating OCPP. It is also true that reference [24] contemplates this combination of methodologies, but only focused for CPSs deployed on ships and not for power applications. Therefore, this paper introduces SD^{c+e} for energy scenarios. This new approach analyzes both cyber threats in control processes (c) and energy threats (e) caused in power system environments; thus, covering cyber, physical and energy assets. This also provides a clear understanding of the vulnerability impact of each component using DREAD for the assessment, and helps to ensure the security of the power system. These threats will be discussed in detail in the following section.

Table 4: Main assets of a CS-based MG

EE	DF	DS	P
CSMS - Application server - OCPP server **EMS** - Control - Monitoring **Charging Station** - OCPP client - Mobile communication - Sensors - Smart meter - Connectors **Microgrid** - DERs - Storage system - Controllers - EV load - Controllable load - Uncontrollable load **Mobile/Web App.** **Measurement components**	**Wireless** - HTTPS - BLE - NFC - OCPP - RFID **Wire** - Modbus TCP - Ethernet	**Database** **RFID tags** **Variables**	**- CS communication** **- BLE/NFC publication** **- Mobile/Web requests** **- User requests** **- User authentication** **- Charging transaction** **- Metering consumption** **- Smart charging control** **- Microgrid control**

3.2 Main threats and vulnerabilities

Observing Figure 2, the first action to perform within the SD^{c+e} model would be to identify the main assets of the application scenario such as control, communication, HW and SW components, and power. Based on these assets, it is possible to classify them according to their functions, and subsequently into EE, DF, DS and P. Table 4 shows this characteristic, contemplating additionally those main assets illustrated in Figure 1. After this, the second step requires plotting the DFDs to see the potential relationships between assets. But since the data flows and relationships between these elements can easily be derived from Figure 1, this step is omitted from the paper.

To continue with SD^{c+e}, we analyze the phases established by Step 3 and

Table 5: Susceptibility of system assets to STRIDE threats (based on [25])

Asset	S	T	R	I	D	E
EE	✓		✓			
DF		✓		✓	✓	
DS		✓	✓	✓	✓	
P	✓	✓	✓	✓	✓	✓

Table 6: Threat consequences in an EVCI installed in an MG

Code	Description	Impact
TC-1	Inability to manage or configure CSs	I-1, I-2, I-3
TC-2	DoS to the CCS	I-1, I-3
TC-3	DoS to the CSs	I-1, I-3
TC-4	Disclosure of sensitive information	I-3, I-4
TC-5	Unauthorized use of CSs for charging	I-2, I-3
TC-6	Inability to start/stop OCPP charging transactions	I-3
TC-7	Fraud on energy consumption	I-3
TC-8	Desynchr. of system parameters	I-1, I-2, I-3
TC-9	Revert energy to the grid	I-1, I-2, I-3
TC-10	Inefficient operation of the MG	I-3

Impact codes: I-1: overload/blackout, I-2: equipment damage, I-3: economic damage and energy theft, I-4: industrial secrets

Step 4 of Figure 2, both focused on the identification and analysis of vulnerabilities. Each type of asset is susceptible to various threats specific to the STRIDE model, as shown in Table 5 and detailed in [25]. This methodology states that before analyzing the threats and vulnerabilities, it is necessary to first extract a list of possible consequences that may affect the system. For that reason, Table 6 establishes a set of possible Threat Consequences (TCs) associated with EVCIs deployed in MGs. Each of these TCs is associated with a pre-determined code, and may result in greater or lesser impact on a part of the system or on the overall system (I-1, I-2, I-3 and I-4). This type of analysis allows us to later manage the risks in the DREAD model and rating according to threats.

From Table 6, we determine that all TCs have an impact on the economy of the MG system owners or their customers, due to (i) energy losses, (ii) inability to meet energy demand at the CS, or (iii) possible fraud in energy consumption. For example, through information disclosure (TC-4), attackers could first intend to leak sensitive information (such as configurations, SW codes, user consumption data, etc.) to subsequently corrupt the reputation of the organization or carry out other subsequent attacks against the control or distribution of energy. TC-1 and TC-8 also present high risk consequences, which lead to a lack of control and deconfiguration of the MG, thereby destabilizing the energy load parameters and even causing overloads, blackouts, physical damage to DER and CS equipment, and possible human injuries. Likewise, TC-9 also has a high impact on the system, since this TC refers to the possibility of an unnatural or massive reversion of energy to the MG. In turn, this may affect the stability of electrical components, which could be overloaded and damaged, leading to energy losses and economic costs.

For clarity, all these threats are further described in the following sections,

Table 7: Comparison of OCPP security features
(based on [36] and [35])

Security	OCPP-v1.6	OCPP-v2.0.1
Encrypted communication	**Poor** (SSL/TLS is only recommended)	**High** (TLS in security profiles, but still HTTP option)
Certificate Management	**X**	✓
Security logs and events	**X**	✓
ISO 15118 support	**X**	✓
Secure upload firmware	**X** (no firmware verification)	**High** (but still non-secure option)
Digital signatures	**X**	**Poor** (only for meter values, optional)
Secure data transfer	**Medium** (HTTP(S) and FTP(S)) (FTP(S) is recommended)	**Medium** (HTTP(S) and FTP(S)) (FTP(S) is recommended)
Identity and Access Management (IAM)	**Poor** (only by an idTag) (susceptible to S and E threats)	**Poor** (new authentication methods) (susceptible to S and E threats) (no authentication options)
Store CVs securely	**X** (Disclosure of credentials) (CVs could be tampered)	**X** (Disclosure of credentials) (More CVs can be tampered)
Limited remote access	**Medium** (CSOs, CSMS and manufacturers)	**Poor** (new possible malicious external entities: EMSs, CAs, web/mobile apps, law enforcement personal)
Secure charging profiles	**Medium** (susceptible to T threats) (charging profiles controlled by CSMS, CSs and CSOs	**Poor** (susceptible to T threats) (charging profiles tampered by EMS, CSMS, CSs (its CVs), CSOs and EVs)
Endpoint DoS protection	**Poor** (measures only for CSs, using the offline mode)	**Poor** (measures only for CSs, using the offline mode)
Physical protection	**X** (Accessible public CSs) (No applied measures)	**X** (Accessible public CSs) (No applied measures)

Table 8: Overview of OCPP security profiles in [36]

Profile	**CS Auth.**	**CSMS Auth.**	**Comm. Security**
1. Unsecured Transport with Basic Auth.	HTTP Basic Auth.	-	-
2. TLS with Basic Auth.	HTTP Basic Auth.	TLS auth. using certificate	TLS
3. TLS with Client Side Certificates	TLS auth. using certificate	TLS auth. using certificate	TLS

Authentication (auth.). Communication (comm.)

but classified according to the STRIDE category set out in [32], and analyzed taking into account the main OCPP-v2.0.1 features. To provide a preview of these features, Tables 7-10 detail the main functionalities of the protocol. For instance, Table 7 shows the main differences related to security issues of v2.0.1 [36] with respect to v1.6 [35]. Similarly, Table 8 outlines the three possible security profiles according to the OCPP client-server model: (i) "*Unsecured Transport with Basic Authentication*" (with the "*Identity*" and "*BasicAuthPassword*" Configuration Variables (CVs)), which does not include encryption and is recommended only in secure networks, such as a Virtual Private Network (VPN); (ii) "*TLS with Basic Authentication*" where the CSMS authenticates itself using a TLS server certificate, while the CSs are authenticated using "*HTTP Basic Authentication*"; and (iii) "*TLS with Client Side Certificates*", where both the CSMS and CSs authenticate themselves using certificates. Meanwhile, Table 9 summarizes the OCPP Use Cases (UCs), grouped by functional blocks, and Table 10 lists the CVs that are susceptible to attack if they are disclosed or tampered with. For reasons of space, only a subset of UCs and CVs, mainly susceptible to STRIDE threats, have been collected, and are identified in more detail in the following subsections.

3.2.1 Spoofing

Any impersonation involves first illicitly obtaining the security credentials or identity (ID) of legitimate users to (i) gain unauthorized access to CS resources (TC-5) or (ii) commit other subsequent attacks such as energy fraud (TC-7). If, additionally, we explore the capabilities of OCPP-v2.0.1 to authenticate users in the system, we note that in the authorization UCs (*C* functional block), it collects the different authentication methods in a previous phase, before authorizing the user to start the transaction in the CS. These authentication phases are still susceptible to impersonation threats such as: (i) RFID tag cloning/theft as also mentioned in [8], [16] and [38]; (ii) physical theft of the credit/debit card or the parking ticket; (iii) disclosure or brute-force attack of a PIN-code; and (iv) disclosure of the security credentials through malware infection in personal

Table 9: Some potential threats to OCPP-v2.0.1 use cases

UC ID	UC Name	Description	Attack/Consequences	STRIDE
A	Security	Security requirements		
A01	Update Basic Authentication Password	CSMS may send a new value for the BasicAuthPassword Configuration Variable	Disclosure of the new credentials	SI
			Tampering the credentials	ST
A02	Update CS Certificate by CSMS	CSMS may start a certificate update procedure	Malicious CA sets an expiration date very close to the current date (DoS to CS)	D
A03	Update CS Certificate by CS	CS initiates the process to update its key when it detects that the certificate will expire in one month	Malicious CA sets an expiration date very close to the current date (DoS to CS)	D
B	Provisioning	Functionalities for provisioning CSs		
B01	Cold Boot CS	Connect a CS which is powering up to a CSMS and provide the right state information	A CS connect to a malicious CSMS	SE
			A malicious CS connect to the CSMS	SE
			A malicious CS forces continuous reboots (DoS to CSMS)	D
B02, B03	Cold Boot CS - Pending/Rejected	*Pending/Rejected* status with the time interval the CS must wait to resend the request.	Setting a high time interval value (DoS to CS)	TD
B05	Set Variables	CSMS may change variables in the CS	Tampering the configuration variables	T
B06	Get Variables	CSMS may retrieve the value of an attribute for one or more variables of one or more components	Disclosure of configuration variables	I
B08	Get Custom Report	CSMS requests a CS to send all the configuration variables	Disclosure of configuration variables	I
B10	Migrate to new CSMS	CS reboots and connects to a new CSMS	Connect to a malicious CSMS and may be deliberate configured by a malicious CSO	SE
B11, B12	Reset - With(out) Ongoing Transactions	CSMS requests a CS to reset itself	Malicious CSMS or CSO continously requests a restart of the CSs (Dos to CS)	D
C	Authorization	Ways to authorize a user		
C01-06	Authorization methods	Using a RFID tag	Cloning or stealing a RFID tag	SE
		Starts with a button	There is no authentication	SE
		Using a credit/debit card	Stealing a credit/debit card	SE
		Using a PIN-code	Brute-force attack	SE
		Using an APP	Injecting a malware	SIDE
		Using a parking ticket	Stealing a parking ticket	SE
C10, C11, C12	Authorization Cache	Authorize an EV driver by using the Authorization cache while the CS is offline	Tampering the cache and forcing the offline mode	TE
			CSO requests to clear the cache and forces offline mode	TD
C13, C14, D01	Local Authorization List	Authorize an EV driver by using the Local Authorization List while the CS is offline	Adding an entry with a malicious ID and forcing the offline mode	TE
			Clearing the entries of the list and forcing offline mode	TD
C15	Offline authorization of unknown ID	Allow automatic authorization of any unknown EV driver while the CS is offline	Unauthorized access forcing offline mode	TE
C16	Stop Transaction with a Master Pass	Enable stopping of transactions by use of a Master Pass	Stealing the Master Pass and stopping the unauthorized transactions	SDE
F	Remote Control	Remote control management from the CSMS		
F03	Remote stop transaction	CSMS may stop an ongoing transaction of a CS	Stopping remotely the transactions	D
G	Availability	CS informs the CSMS of its current availability		
G02	Heartbeat	CS sends a heartbeat after a configurable time interval. It is also used for time synchronization	Setting an incorrect date to desynchronize the time	TD
G04	Change Availability CS	CSMS may change the availability of a CS to *operative* or *inoperative* mode	Disabling the CSs	D
H	Reservation	Enable an EV driver to make a reservation of a CS		
H01	Reservation	An EV driver reserve an EVSE until a certain expiry time	Setting a high expiry datetime at ReserveNowRequest message (DoS to CS)	TD
I	Tariff and Cost	It provides tariff and cost information to a driver		
I02, I06	Show Total Cost / Tariff Information	It shows an EV Driver the running total cost / tariff information during the charging	Lying about the total cost/tariff information to the user	T
J	Meter Values	CS sends periodic clock-aligned MeterValues		
J02	Sending transaction related Meter Values	CS sends energy meter information about its transaction to the CSMS (meter values are signed optionally)	Tampering meter values to desynchronize the energy monitoring (if they are not signed)	TR
K	Smart Charging	A third party (like EMS) influences the charging current/power transferred, or set limits		
K01	Set Charging Profile	CSMS may change the power/current limits of a CS	Tampering the energy limits	TD
K10	Clear charging profile	CSMS may clear some or all the charging profiles that were sent to a CS	Deconfiguring the charging profiles	TD
L	Firmware Management	CS operator updates the firmware of a CS		
L02	Non-Secure Firmware Update	CS can download and install a Non-Secure firmware update from CSMS	Installing a malicious firmware in a CS (e.g., backdoor, spyware, ransomware...)	STRIDE
M	ISO 15118 Certificate Management	Support of certificate-based authentication between EV and CS bidirectional communication		
M04	Delete Certificates	CSMS requests the CS to delete its certificate	Insider requests to delete all certificates	D
M05	Install Certificates	CSMS requests the CS to install a new certificate	A malicious CA installs the certificates	S
N	Diagnostics	Enabling remote diagnostics of problems with a CS		
N03-N06	Set/Remove Monitoring	CSO can configure the monitoring parameters, such as thresholds to events, level security...	A malicious CSO tampers the variables to produce malfunction or DoS	TD

UC ID: use case identifier in the OCPP-v2.0.1 specification.
The shaded rows represent the functional blocks where the use cases are grouped

Table 10: Some potential threats to OCPP-v2.0.1 configuration variables

Configuration variable	Use	Attack	Risks/Consequences	STRIDE
RetryBackOffRepeatTimes	Number of connection attempts doubling the previous time	Set a LOW number	DoS to CSMS (TC-2)	TD
RetryBackOffWaitMinimum	Minimum time waiting to reconnect after a connection loss	Set a HIGH number	DoS to CS (TC-3)	TD
WebSocketPingInterval	Number of seconds between pings (only for WebSocket implementations)	Set a LOW number	DoS to CSMS (TC-2)	TD
HeartBeatInterval	Interval of inactivity after the CS sent the last HeartbeatRequest	Set a LOW number	DoS to CSMS (TC-2)	TD
MaxEnergyOnInvalidId	Maximum amount of energy in Wh to an unknown user	Set a HIGH value	Energy fraud (TC-7)	TDE
DateTime	Current datetime, same as CSMS	Set a CS datetime different from CSMS	Desynchronisation (TC-8)	TD
Identity BasicAuthPassword	CS identity and password (read only)	Disclosure credentials	CS spoofing (TC-4)	SI
AuthEnabled	Authorisation is required	Set to FALSE	Start transactions in an unauthorized manner (TC-5, TC-7)	STE
AuthorizeRemoteStart	Allow remote transactions by CSMS	Set to TRUE and spoof the CSMS	Start transactions in an unauthorized manner (TC-5, TC-7)	TD
LocalAuthorizeOffline	Use locally-authorized IDs to start a transaction when CS is offline	Set to FALSE and force the offline mode	Inability to authenticate users (TC-2, TC-3, TC-6, TC-7)	TD
OfflineTxForUnknownIdEnabled	Supports Unknown Offline Authorization	Set to TRUE and force the offline mode	Start transactions in an unauthorized manner (TC-5, TC-7)	STE
AuthCacheLifetime AuthCacheStorage	How long a token expires and maximum number of bytes used	Set a LOW value and force the offline mode	Inability to authenticate users (TC-2, TC-3, TC-6, TC-7)	TD
LocalAuthListEntries LocalAuthListStorage	Maximum number of entries and bytes used by the Local Authorization List	Set a LOW value and force the offline mode	Inability to authenticate users (TC-2, TC-3, TC-6, TC-7)	TD
MasterPassGroupId	IdTokens belonging to the Master Pass Group	Add an entry with a malicious idToken	Stop the transactions in an unauthorized manner (TC-3, TC-5)	STDE
SmartChargingEnabled SmartChargingAvailable ExternalControlSignalsEnabled	Allow external entities to control the charging profiles	Set to TRUE and connect to a malicious external entity	Fraud (TC-7) and destabilize energy resources (TC-3, TC-8, TC-10)	TD
FileTransferProtocols	List of supported file transfer protocols	Set only FTP and HTTP	Disclosure of data (TC-4)	TI
MessageAttemptsTransactionEvent	Number of tries to submit a TransactionEventRequest to the CSMS	Set a HIGH number	DoS to CSMS (TC-2)	TD
MessageAttemptIntervalTransactionEvent	Waiting time of a CS to resubmitting a failed TransactionEventRequest	Set a HIGH value	DoS to CS (TC-3)	TD
MaxEnergyOnInvalidId	Maximum amount of energy delivered when an ID is unauthorized by the CSMS after start a transaction	Set a HIGH value	Energy theft (TC-7)	TE
StopTxOnInvalidId	Stop an ongoing transaction when it is unauthorized	Set to FALSE	Energy theft (TC-7)	TE
SampledDataSignReadings AlignedDataSignReadings	CS include signed meter values	Set to FALSE	Repudiation of transactions (TC-7)	TR
TariffFallbackMessage TotalCostFallbackMessage	Message to be shown to an EV driver	Lie about the tariff and total cost	Fraud to the consumer (TC-7)	T

devices if CT requests are via a web or mobile application.

The CCS is another vulnerable access point in the CI analyzed. If an attacker succeeds in spoofing the central system and he/she is capable of gaining access to resources, then he/she may be capable of disabling, manipulating and eavesdropping the communication with CSs (TC-[2-9]), and even controlling EMS operations (TC-1 and TC-10). Another way to attack communication channels from the CCS to CSs is to conduct a Man-in-the-Middle (MitM). An attacker first needs to impersonate the legitimate CSMS through one or several UCs of the OCPP itself; especially, when a CS connects or migrates to a new malicious CSMS (UCs B01 and B10). Once the CSMS has been spoofed, the attacker may be able to remotely start and stop transactions – if this option is enabled ("*AuthorizeRemoteStart*" CV) – in order to deny service to CSs (TC-3). If, addition, the OCPP configuration enables the CV options "*SmartChargingEnabled*", "*SmartChargingAvailable*" and "*ExternalControlSignalsEnabled*", then it is likely that an attacker can impersonate an external entity, such as an external EMS, to connect to legitimate CSs. Consequently, a spoofed EMS might alter energy profiles and limit the amount of current/power of CSs, in order to destabilize energy resources (TC-3, TC-8, TC-10) or consume at a higher power than is permitted (TC-7 – according to the new and corrupted charging profiles).

CSs are also susceptible to attacks due to their high exposure in public areas [16]. Attackers may steal the ID of a victim CS in different ways. For example,

(i) by tampering the CS device and extracting its ID through the OCPP CVs related to "*Identity*" and "*BasicAuthPassword*"; (ii) by stealing the credentials of the client TLS certificate through a physical access to the CS (only if security profile 3 is used and the private key is stored in plain text); (iii) by injecting logic bombs such as spyware or rootkits; and (iv) by stealing or tampering the new password through the A01 UC (see Table 9). A spoofed CS allows the attacker to leak sensitive information managed by the CS itself (e.g., telemetry values, users' IDs, credentials, parameters) and the CSMS (e.g., OCPP transactions), corrupting TC-4. This threat may even favor other subsequent attacks, such as the unauthorized use of the CS and its connectors for charging (TC-5), or change the CS parameters (TC-8 or TC-9). Moreover, legal stakeholders may also stop any OCPP transaction if they use a Master Pass. This Master Pass consists in a unique token (e.g., a master RFID tag) used by law enforcement personnel to stop any (or all) ongoing transactions – e.g., to stop any ongoing transaction when an EV has to be towed away. If this Master Pass is theft or cloned, attackers may gain access to these critical operations, and could deny service or the charging to users (TC-3 and TC-7).

3.2.2 Tampering

This threat refers to the attacker's capacity to violate the integrity of OCPP communication messages, databases or process of a CS. The first and most obvious way to attack the OCPP protocol is to physically or remotely access the OCPP client module of a CS in order to manipulate its CVs. Table 10 shows a set of CVs that can be manipulated (except for "*Identity*" and "*BasicAuthPassword*" which are read-only) to cause either a DoS (e.g., by decreasing the heartbeat interval) or to gain unauthorized access to the system (e.g., by activating "*OfflineTxForUnknownIdEnabled*" to access as a "legitimate" user when the CS is in offline mode due to a previous DoS attack).

Another way to attack is through a MitM [8, 16]. OCPP messages may be manipulated from different standpoints. For example, attackers might: (i) change the "*meterValues*" variable during a transaction (JO2 UC) to mislead the CSMS about the total amount of energy consumed in a transaction, causing fraud (TC-7); (ii) modifying a charging profile (K01 UC) to consume at higher power and desynchronize energy parameters (TC-8); or (iii) alter the tariff and cost messages during a transaction (I02 UC) to cheat the end user about the total cost – making the victim pay more or less than expected (TC-7). To avoid this situation, TLS-based peer-to-peer protection could help encrypt such transactions. In this way, an attacker would first need to overcome this issue considering the TLS weaknesses against MitM threats [43], [8].

Finally, energy-related threats have to be taken into account in MG systems. Attackers can manipulate DERs for the purpose of misconfiguring installations in order to extract energy from renewable energy sources, for example, by modifying the inclination of photovoltaic panels or turbine blades, leading to energy inefficiency (TC-1, TC-8). As a consequence, storage systems may be overused, causing their performance to degrade prematurely (TC-10). In addition, if the attacker varies the control set-points associated with voltage or frequency regulations, the electrical signal in the MG bus would be unable to comply with international restrictions on voltage levels and/or operational frequency. This may cause electrical damage to the CS components and even some computational problems (the frequency of the electrical signal may cause some timing problems in the micro-processors). Smart meters, such as phasor measurements, may also provide wrong measurements, which may lead to incorrect control commands. These attacks may render the CS unable to meet the energy demand of the users, thereby causing an impact on the real health of the power assets that make up the MG. Any misconfiguration of the MG may even interfere with the external power system, provoking further consequences.

3.2.3 Repudiation

Traditional repudiation attacks are triggered when a malicious entity claims not to have performed an action that it did in fact perform, and the victim entity is unable to verify the truth of the claim. To avoid this problem, the system should contemplate the use of digital signatures to ensure the provenance of the actions.

Thanks to the ISO 15118, CSs can manage digital signatures with information related to metering in the EV part. Unlike OCPP-v1.6, the new version also manages signed meter values when CSs need metering information exchange to th CSMS (in OCPP security profiles 2 and 3). However, OCPP does not force to the use of digital signatures, what repudiation attacks may arise. For example, malicious customers may lie about the real metering values in the transactions as stated in [8]. Also, if messages between the CSMS and CSs, and between the EMS and CSs are not properly audited, when an error occurs in a CS due to poor control of energy and charging profiles, the system may not determine the responsible entity (e.g., the EMS or other external EMSs), or even the origin of the error. Therefore, it is essential to use secure communications under digital signature schemes to ensure accountability, traceability and authentication.

3.2.4 Information disclosure

Adversaries may exploit security breaches to steal sensitive information (TC-4) and gain more detailed knowledge of the system, in order to subsequently prepare more elaborated attacks. In CS, it is possible to lead this type of attack not only at communication level but also in a compromised CS (e.g., through a physical attack or a physical manipulation during the installation/maintenance tasks), corrupting databases, registers and logs. From these information assets, it is possible to extract or derive user IDs, security credentials, telemetry data, energy consumption and cumulative power data, and vulnerabilities inherent in the CS firmware − even if many of these are encrypted [21].

To launch a MitM attack on the OCPP security profiles (as also shown in Table 8), the attacker must gain access to the private network. To do so, if TLS (especially when the version is lower than 1.3) is applied (security profiles 2 and 3), then the attacker must obtain the shared session key through the already discovered vulnerabilities such as protocol downgrades, connection renegotiation and session resumption. The work in [43] reflects these weaknesses, which compiles a list of vulnerabilities found in the SSL/TLS protocols, while the work [8] states several examples of threats in the TLS-based OCPP-v1.6. Other data flows that may be threatened are charging requests to the CSMS via the web or mobile app, or directly to the CS via technologies such as BLE, NFC and RFID [4, 5]. A MitM in these communications could leak sensitive user information (e.g., IDs) to later impersonate him/her [49].

3.2.5 Denial of service

This threat disables the availability of system services and may cause significant disruption and damage. This also means that if an attacker performs a DoS, for example, on the communication with the authentication server, end users will not be able to request CTs, interrupting the real energy charge in their EVs (TC-2, TC-3 and TC-6). On the other hand, if the aim of the attack is to interfere with OCPP transactions (e.g., through an on-path attacks such as black holes, selective forwarding or gray holes, or replays [8, 16]) or deny access to the database of the CSMS or EMS, this can have even a greater impact by causing loss of control of the DERs and CSs (TC-1, TC-2, TC-3 and TC-6).

As mentioned above, the OCPP protocol may be manipulated in order to deny service to CSs or the CSMS. For example, a malicious CSMS or an attacker with a Master Pass may stop other users' transactions or even disable the availability of CSs (F03, C16 and G04 UCs). In addition, if the attacker changes the datetime parameter ("*DateTime*" CV) of a CS with respect to the CSMS, it would lead to a desynchronisation, and, therefore, reserve transactions would not start and stop at the corresponding time. Thus, the duration of any OCPP transaction related to the starting of a charging would not either correspond to the date-time parameter of the CSMS. Attackers may carry out a similar attack with users' IDs to exploit H01 UC and make massive reservations of EVSEs with a high expiration date. This disables other legitimate users from having the ability to reserve and use these reserved connectors by the adversaries. Moreover, if an attacker carry out a DoS in the communication channel between the CSMS and the CS to force the CSs enter into offline mode, the attacker may take advantage of the offline authorization modes (C13 and C15 UCs) to gain access the CS, as also noted in [8]. Attackers may achieve this purpose through jamming, flooding, replay or massive sending of OCPP heartbeats in short periods of time.

As for energy assets, attackers may be able to alter the EMS, the storage systems or the communication between them so that the storage system is deliberately perturbed. The storage system may, e.g., be blocked to users while the market price is high, i.e., when it is usually recommended to extract energy from the storage system. Moreover, DERs are connected to the MG bus through power converters, whose operation is generally regulated through digital controllers. If attackers gain malicious access to the control and alter the activation signals of the converters or incorporate delays in them, it may cause both the power converters and the energy source itself to operate with electrical magnitudes (voltage, current and/or power) that exceed the maximum allowed. This could result in damage to electrical components or even breakage (TC-2). This vulnerability is also present in electrical storage systems. Controllable loads (EVs or others) carry out their load according to an established criterion, and a control is performed to evaluate the suitability of the load. Access to the data on which these criteria are based may result in a failure to connect loads to the grid. In the case of EVs, their charging/discharging process would not be carried out. For example, adversaries may alter economic data and cause this impact (in an electricity market-oriented scenario), or may also intentionally change data related to grid support services. On the other hand, if an attacker modifies the operating set-points of the generators and loads – decided by the EMS to ensure that the grid operates correctly in terms of voltage and frequency – the MG could become unstable and, as a result, totally or partially inoperative (TC-8, TC-10).

As highlighted in [8], DoS against power flows may also arise. In V2G networks, where the CI is equipped to enable bidirectional power transfer, attackers may execute sophisticated attacks. They could prepare several synchronized attack vectors on different CSs connected to the same power transformer at peak demand hours (interval of highest demand in grid connection and use of CSs). The aim is to extract power from the EV batteries, revert power on a massive scale and cause significant local blackouts or damage to electrical equipment (TC-9) in the MG or the external power system. For instance, energy storage systems, loads connected to the MG (e.g., other EVs) or the converter to connect to the power grid may seriously be affected.

3.2.6 Elevation of privilege

There are two ways to connect to OCPP-based CIs: (i) as a user through a website, mobile application or directly with the CS, where the only functionalities are to reserve the connector of a nearby CS in order to charge his/her EV battery; and (ii) as a CSO via the CCS, with control and configuration functionalities over the CSMS and EMS. To gain unauthorized access by one of these two means, attackers start by finding weak points through which they may first penetrate the network. They then attempt to escalate privileges to gain further permissions or access other sensitive systems.

In addition, there are two types of privilege escalation: horizontal and vertical. In the horizontal mode, an attacker expands his/her privileges by accessing the data of other accounts at the same level. For example, an attacker could leak a legitimate user's security credential and get unauthorized access to the victim's account to make charging requests with the victim user's account. In contrast, in vertical mode, an attacker can obtain such an access through an existing but compromised user account. The attacker starts from a less privileged account until he/she gains the permissions of an IT/OT administrator. This situation would correspond to one where the adversary, without permissions, is able to manipulate and add his/her ID to the local authentication list (C13 UC) in order to later elevate his/her privileges as a legitimate user. Alternatively, an attacker with user permissions could tamper with "*MasterPassGroupId*" CV and add his/her ID (like a "legitimate" stakeholder) to get the Master Pass permissions. In either case, and as an "authorized" user within the system, he/she could exploit further UCs; e.g., to reserve power in an unauthorized manner (TC-5), or take advantage of the Master Pass to stop any ongoing transaction (TC-1-3, TC-8).

The three methods to authorize a user when the CS is in offline mode in OCPP (corresponding to C functional block of Table 9) are (some already analyzed previously in [8]): (i) *authorization cache*, (ii) *local authorization list*, and (iii) *unknown offline authorization.* The former maintains a record of IDs that the CSMS has successfully authorized previously. An adversary could manipulate this cache to add a record with a malicious ID and force the offline mode (with a subsequent DoS to the CSMS) to achieve unauthorized use of the CS. The local authorization list has a list of IDs, which is periodically synchronized with the list of the CSMS (D01 UC). A malicious CSMS or MitM could send a tampered list with invalid IDs, and then force the offline mode to use these invalid IDs, gaining unauthorized access to the CS. Finally, if the unknown offline authorization option is enabled, a CS allows automatic authorization of any unknown ID that is not necessarily in the local authorization list or authorization cache. In this case, an attacker must first enable the "*OfflineTxForUnknownIdEnabled*" CV to *TRUE*; and under this situation the attacker may take advantage of this modality to cause fraud. He/she may request unauthorized CTs using an invalid ID when the CS is offline (C15 UC).

On the other hand, if an advanced adversary manages to elevate its privileges and gain access to the EMS or CSMS in a stealthy manner, it could lead to greater consequences. Some of them have been mentioned above: (i) inability to configure the MG (TC-1); (ii) disclosure of configuration data and system status (TC-4); (iii) altering consumption data with the aim of economic fraud (TC-7); or (iv) even desynchronizing system parameters (TC-8), putting physical equipment and human lives at risk. CPSs, such as CS infrastructures, increase the number of vulnerabilities due to: (i) the growing complexity of Industry 4.0 communication technologies, combining wired and wireless networks; (ii) their high exposure to external networks, where the CCS commonly contacts external links over the Internet; (iii) increasingly extensive inter-network communications, increasing the number of DERs and smart meters to take advantage of local renewable energy generation and demand management; and (iv) the inheritance of vulnerabilities in established or growing tools, such as the TLS and OCPP communication protocols [28].

Table 11 summarizes all the threat consequences found in each STRIDE threat in a CSs-based MG. In addition, we can observe that T and D threats have a direct impact on the generation and distribution of energy by the MG, and therefore pose a higher risk to the system. In the following section, we will evaluate each of the STRIDE threats on (c) and (e) using the DREAD model, and then propose a list of countermeasures.

Table 11: List of threat consequences for each identified STRIDE threat

STRIDE	Threat	Threat consequences	Energy
S	User spoofing	TC-5, TC-7	
	CSMS spoofing	TC-[2-9]	
	EMS spoofing	TC-1, TC-3, TC[7-8], TC-10	
	CS spoofing	TC-4, TC-5, TC-8, TC-9	
T*	OCPP messages	TC-7, TC-8	
	OCPP CVs	TC-[2-3], TC-[5-6], TC-[7-8]	
	DERs	TC-1, TC-8	✓
	Storage systems	TC-10	✓
R	Meter values	TC-7	
	Errors responsible	-	
I	OCPP messages	TC-4	
	User-CSMS	TC-4	
	User-CS	TC-4	
	Databases	TC-4	
D*	User authentication	TC-2, TC-3, TC-6	
	CSMS	TC-1, TC-2, TC-6	
	EMS	TC-1	
	CS	TC-1, TC-3, TC-6	
	MG	TC-2, TC-8, TC-10	✓
	Revert energy	TC-9	✓
E	User authorization	TC-5, TC-7	
	Admin in CSMS	TC-4, TC-7, TC-8	

*T and D threats directly affect MG power generation, distribution and storage

Table 12: DREAD criteria (based on [24])

	High || [8.0, 10.0]	**Medium || [5.0, 8.0)**	**Low || [1.0, 5.0)**
Damage	Attacker is able to cause severe damage to the system; modify CVs; send operations to the CSs	Disclosure of sensitive data (user IDs/CVs/user consumptions); cause minor damages such as energy theft and economic fraud	Disclosure of non-sensitive data; (telemetry values, public data) the attack cannot be extended to other devices
Reproducibility	The attack can be carried out at any time and in any situation	The attack can be carried out at certain conditions (e.g., in during peak demand hours)	Even if the vulnerability exists, the attacker is unable to carry out the attack (e.g., private CSs in a secure location)
Exploitability	The attack does not require security knowledge. It can be performed by a novice, skilled and expert adversaries in a short time	The attack requires a low level of security knowledge. It can be performed by a skilled and expert adversaries	The attack requires a extremely level of security knowledge and in-depth knowledge of the system. It can be only performed by an expert adversary
Affected users	The whole system is affected (CSs, CCS, MG, EVs, users...)	Partial users/systems are affected	The attack only affects the target entity
Discoverability	System and net. vulnerabilities are known and the attacker has access to relevant infor. to exploit them	System and network vulnerabilities exist, but are not known to the attacker	The attack has been identified and its vulnerabilities have been patched

3.3 DREAD model for threat assessment

DREAD provides a mnemonic for the classification of security risks using five categories: Damage, Reproducibility, Exploitability, Affected users and Discoverability. Table 2 (in Section 3) details the evaluation procedure and description of each of the DREAD categories. There are different quantitative evaluation methods for this model. In this case, we have followed a variant of the procedure proposed by Microsoft [3]. We evaluate each STRIDE threat in each component with respect to each DREAD category with a value from 1 to 10, where 1 is a low impact and 10 a high-risk threat. After this, we make a weighted average for each STRIDE threat, thus obtaining a numerical value that indicates the level of risk in the system as a whole. In addition, in order to provide a qualitative risk analysis, we establish a list of criteria that relate the evaluations to the rating values. The qualitative risk analysis is based on experience. In this case, we have classified the risk levels as high, medium and low following the criteria proposed by Kavallieratos and Katsikas in [24]. These criteria are also defined in Table 12.

In order to assess the risk, we consider the threats classified in Table 11 (cf. Section 3.2). For each of these threats, each of the criteria established by DREAD are scored manually with a score from 1 to 10. In this case, the risks are analyzed in terms of the impact and consequences on CSs, leaving aside other related infrastructures, such as the MG, to reduce the scope. Moreover, Table 13 reflects the results of this assessment analysis, where T and D (which directly affect energy) correspond to the highest risk threats in CIs. This table also shows how a tampering or DoS leads to major impacts on the system (high risk in Damage and Affected users criteria) and could also be executed by adversaries without detailed security or network knowledge (high risk in Reproducibility, Exploitability and Discoverability criteria). This analysis coincides with the preservation of integrity and availability requirements that are essential in any ICS, and which correspond to T and D in the STRIDE model (cf. Table 1).

On the other hand, S and E threats present a medium level of risk, except for two that are high risk ("CS spoofing" and "OCPP CVs"). As the previous cases, a spoofing or elevation of privileges could have major consequences for the organization, such as fraud, unauthorized access, inefficient operations or energy destabilization. However, for these threats, adversaries require greater cybersecurity expertise (low risk in Exploitability criterion) and, in addition, the threats could be partially/fully covered by appropriate defense measures (low risk in Discoverability criterion), such as security policies, identity management, principle of least privilege, etc. In contrast, R and I threats present the lowest risk. R is easily addressed through the use of digital signature and I is also controlled with the correct use of TLS or VPNs. Note that these measures are already addressed in the OCPP-v2.0.1 protocol with security profiles 2 and 3, strongly affecting the Discoverability criterion of the DREAD model. Other significant DREAD criteria, which influence the low risk assessment of these threats, are Damage and Affected users.

Overall, threats directly related to CSs present a high level of risk, mainly due

Table 13: Cyber and energy risks in each identified threat using DREAD

STRIDE	Threat	D	R	E	A	D	Risk
S	User spoofing	6	9	8	5	8	Medium (7.2)
	CSMS spoofing	8	6	5	8	4	Medium (6.2)
	EMS spoofing	8	6	5	8	4	Medium (6.2)
	CS spoofing	9	9	8	7	7	High (8)
T	OCPP messages	9	9	6	9	4	Medium (7.4)
	OCPP CVs	9	9	9	7	9	High (8.6)
	DERs	9	8	4	8	5	Medium (6.8)
	Storage systems	7	9	8	9	5	Medium (7.6)
	Revert energy	7	5	4	10	6	Medium(6.4)
R	Meter values	3	6	5	3	1	Low (3.6)
	Errors responsible	1	5	4	2	1	Low (2.6)
I	OCPP messages	5	7	4	5	6	Medium (5.4)
	User-CSMS	5	6	4	2	4	Low (4.2)
	User-CS	5	7	7	2	8	Medium (5.8)
	Databases	5	7	2	8	3	Medium (5)
D	User authentication	6	10	9	5	10	High (8)
	CSMS	9	8	8	10	7	High (8.4)
	EMS	9	8	8	9	8	High (8.4)
	CS	10	10	10	7	9	High (9.2)
	MG	10	8	8	10	6	High (8.4)
E	User authorization	5	9	8	3	9	Medium (6.8)
	Admin in CSMS	9	7	3	9	5	Medium (6.6)

to their high exposure to the public. The fact that CSs are generally deployed in open environments makes them more prone to physical attacks, whether natural or intentional. Reproducibility, Exploitability and Discoverability criteria of the DREAD evaluation model are highly affected in these threats. Table 13 clarifies that "CS spoofing", "OCPP CVs" (the variables are stored in the CS) and "DoS to the CS" are the threats with the highest risk in each of the corresponding STRIDE categories.

4 Recommendations for mitigation

This section explores a set of recommendations to address the threats discussed in the previous section, and especially those related to D and T together with those presenting high and medium risk (≥ 5.0) in Table 13.

4.1 Priority recommendations for risks [8.0, 10.0]

As stated in the previous section, the most potential threats are those related to "DoS to CS", manipulation of "OCPP CVs" and "CS spoofing". These three threats require OCPP transaction-level protection and especially for A01 UC. For this protection, it is advisable to force the use of mutual authentication via TLS using certificates in the CS and CSMS (security profile 3 in OCPP-v2.0.1). Although this action avoids any disclosure or manipulation of identification variables (such as Identity and BasicAuthPassword), the TLS version also influences the protection process, where it is also recommended to apply TLSv1.3 or related protocols such as IPSec. On the other hand, as CSs are generally deployed in open and public environments, TLS certificates (included private keys stored in plain text) may also be easily manipulated through a physical access. In these circumstances, it is necessary to foresee a surveillance plan (e.g., installation of cameras), as well as the deployment of CSs enabled with shock-resistant casings and SW-based anti-tampering solutions to prevent not only access to keys and certificates, but also illicit modifications [16].

Any DoS also has a significant social and economic impact, so it is essential to activate redundant mechanisms that facilitate not only the permanent connection to the CSMS, but also the authentication and authorization of legitimate users. To do this, it is essential to (i) address mainly redundant architectures in terms of communication and services, such as the use of proxies around the CSs (or in the local controllers), and to (ii) periodically update the list of users (with unique IDs) who have permissions to charge their EVs. In this way, it is possible to facilitate the authorization of legitimate operations with the CSMS when stations lose connection with the central system. Likewise, the official authorities, owners of the Master Pass, must follow training programs to avoid denials of service, caused by themselves or by others who may have stolen the Master Pass. One way to detect these unfortunate situations, caused mainly by lack of knowledge or training, would be through reputation mechanisms capable of identifying irregular behavior at the user level (lack of interest or knowledge),

Table 14: Priority recommendations for potential threats in OCPP-v2.0.1

Threat	Priority	Related UC IDs	Mitigation action		Benefiting	Reducing
DoS to CS	High (9.2-8)	F03 C16 G04 I02 H01 C13 C15	TLSv1.3 under OPCC security profile 3 or IPSec to avoid MitM actions	R	C, I, A, AU	TC-1, TC-2, TC-3, TC-6; I-1, I-2, I-3
			Hash functions to verify the integrity of SW components in CSs	R	I	
			Digital signature for each OCPP transaction, or the use of MAC functions	R	NR, AU, I	
			Periodic update of the list of users authorized to charge energy in CSs.		AU, AUT	
			Redundant mechanisms (e.g., proxies, communication links) to prevent on-path attacks or authentication in offline mode		A, AU	
			Continuous maintenance and certification of HW/SW components	R	A, I	
			Reputation mechanisms to estimate anomalous user and device behaviors		A, I, AK	
			Data traceability to detect occasional or frequent deviations in one or more transactions	R	I, A, AU, AT	
			Surveillance and tamper-resistant constructions	R	Safety, I	
			Diagnostics, detection and dynamic event management systems	R	C, I, A, AU	
Manipulation of OCPP CVs	High (8.6)	B05 JO2 K01 I02	TLSv1.3 under OPCC security profile 3 or IPSec to avoid MitM actions	R	C, I, A, AU	TC-2, TC-3, TC-5, TC-6, TC-7, TC-8; I-1, I-2 I-3,
			Encryption of sensitive data (e.g., OCPP CVs, IDs)		C	
			Hash functions to verify the integrity of SW components and data in CSs	R	I	
			Digital signature for each OCPP transaction, or the use of MAC functions	R	NR, AU, I	
			Data traceability to detect occasional or frequent deviations in one or more transactions	R	I, A, AU, AT	
			Surveillance and tamper-resistant constructions	R	Safety, I	
			Diagnostics, detection and dynamic event management systems	R	C, I, A, AU	
CS spoofing	High (8)	A01	TLSv1.3 under OPCC security profile 3 to avoid using identification CVs (Identity and BasicAuthPassword) and MitM actions, or IPSec	R	C, I, A, AU	TC-4, TC-5, TC-8, TC-9; I-1, I-2, I-3, I-4
			Management of unique IDs for each user, device and transaction	R	AU, AUT	
			Digital signature for each OCPP transaction, or the use of MAC functions	R	NR, AU, I	
			Surveillance and tamper-resistant constructions	R	Safety, I	
			Diagnostics, detection and dynamic event management systems	R	C, I, A, AU	
Manipulations of DERs and storage systems	Medium (7.4-6.4)	N03-N06 K01 K10	Periodically validate power components to verify compliance with regulatory frameworks and international constraints on voltage levels and operational frequency		Safety, I	TC-1, TC-8, TC-10; I-1, I-2, I-3
			Continuous maintenance and certification of energy components		Safety, A, I	
			Data traceability to detect occasional or frequent deviations in energy components and transactions	R	I, A, AU, AT	
			Surveillance and tamper-resistant constructions	R	Safety, I	
			Diagnostics, detection and dynamic event management systems	R	C, I, A, AU	
User, CSMS and EMS spoofing	Medium (6.2-7.2)	C01-06 B01 B10	TLSv1.3 under OPCC security profile 3 to authenticate each part (CSMS, EMS, CS) or IPSec	R	C, I, A, AU	TC-[1-10]; I-1, I-2, I-3, I-4
			Management of unique IDs for each user, device and transaction	R	AU, AUT	
			Awareness to end users about the importance of protecting their credentials and security IDs		AK, AU, AUT	
			Awareness to human operators about the importance of protecting the ecosystem		AK, AU, AUT	
			Access control to the CS under the principles of least privilege, and avoid escalation of privilege		AU, AUT	
			Digital signature for each OCPP transaction, or the use of MAC functions	R	NR, AU, I	
			Diagnostics, detection and dynamic event management systems	R	C, I, A, AU	
User authorization and admin in CSMS	Medium (6.8-6.6)	C13 C15 D01	TLSv1.3 under OPCC security profile 3 to authenticate each part (CSMS, CS) or IPSec	R	C, I, A, AU	TC-4, TC-5, TC-7, TC-8; I-1, I-2, I-3, I-4
			Valid local authorization lists composed of unique IDs associated with legitimate entities and received from a valid CSMS		AU, AUT	
			Avoid as much as possible the authentication in offline mode, and deploy proxies that manage access control via the CSMS		AU, AUT	
			Least privilege principles and segmentation of functions to avoid escalation of privilege	R	AU, AUT	
			Digital signature for each OCPP transaction, or the use of MAC functions	R	NR, AU, I	
			Diagnostics, detection and dynamic event management systems	R	C, I, A, AU	
Information disclosure	Medium (5.8-5.0)	B06 B08	TLSv1.3 under OPCC security profile 3 to authenticate each part (CSMS, CS) or IPSec	R	C, I, A, AU	TC-4; I-3, I-4
			Encryption of sensitive data (e.g., OCPP CVs, IDs)	R	C	
			Least privilege principles and segmentation of functions to avoid escalation of privilege	R	AU, AUT	
			Privacy-enhancing technologies and approaches for the CSMS and EMS	R	C, privacy	

C: confidentiality, I: integrity, A: availability, AU: authentication, AUT: authorization, NR: non-repudiation, AK: awareness and knowledge, R: countermeasure repeated by some other action but also through mechanisms that enhance data traceability to identify at any time the use and misuse of the Master Pass. In this case, we highlight the capacities of some disruptive technologies like blockchain since it guarantees data immutability, traceability, auditability, and accountability [33, 50].

Malware (in a CS, the CSMS or the EMS) is another threat that can cause DoS. It can be detected by checking the integrity of each SW component. This type of verification is also critical to deal with manipulations to OCPP CVs (B05 UC). Not only encryption schemes are useful to prevent direct access to their content, but also the traditional use of Message Authentication Message (MAC) functions and hash functions (e.g., SHA-256 / SHA-512) can be useful. The latter can even help the CS to (i) not only verify the integrity of each variable, but also to (ii) manage digital signatures for each OCPP transaction, ensuring authentication, non-repudiation and accountability. In other words, any action performed in the CS, including those performed after authentication in offline mode (C13 and C15 UCs), could be logged and linked. This also means that each entity (including the device/process or a transaction) within the organization has to have a unique ID to link operations and actions.

Specific mechanisms for HW and SW diagnostics and advanced detection, supported by dynamic event management systems like the Security Information and Event Management (SIEM) systems in the CSMS, could also facilitate local and global monitoring of all these potential threats and enable the system to make timely decisions [14]. These mechanisms usually rely on Machine Learning (ML) algorithms to predict any deviation in the normal status of control components and their behavior [12]. Depending on the capabilities of the devices that integrate them, the selection of the model can vary. The authors of the work [6] determine that decision trees, fuzzy logic, rules, statistics and clustering may be good candidates for detecting anomalies in very limited devices. Moreover, SW agents and additional (current, voltage, phasor and power) sensors acting as inspectors can be integrated as part of a distributed or collaborative detection system [12, 16] to extend the input data for these techniques, and ensure greater accuracy in detection processes. The goal could be, for example, to identify if there is an illogical physical correspondence that may affect the actual availability of the CS, and may be strong evidence of a possible attack or accidental threat. In this sense, reputation measures at device level can also be a good approach to estimate when maintenance actions should be launched and plans should be reviewed accordingly.

4.2 Priority recommendations for risks [5.0, 8.0]

As can be seen in Table 14, most of the countermeasures are transversal to all UCs − those marked in the table with the symbol R −, including those countermeasures considered of medium risk. From the table, we also note that access control should follow solutions that prevent offline authentication modes. This requires maintaining the connection to the CSMS using, for example, redundant mechanisms as mentioned above, and validating any connection with external entities, via TLS with certificates and digital signature in each transaction.

On the other hand, continuous maintenance and certification of energy components (DERs and storage systems) is also relevant to guarantee the availability of minimum services to the end user. In this sense, anomaly-based detection mechanisms and diagnostics with support in blockchain networks for traceability of anomalies can also be incorporated to predict variations in the behavior of critical components (e.g., caused by failures or by malicious CSOs - related to the N03-N06 UCs). This information can even feed to other analytics of the EMS to, for example, (i) favor the smart charging procedures and their profiles (related to K UCs), or (ii) optimize existing resources in the EMS. The latter is relevant for managing MG controller set-points; increasing run-time may mean that this power system is not scalable. Instead of this centralized approach, an alternative could be the implementation of distributed control algorithms. Coordinated and distributed control algorithms make use of the information sent by the immediate neighbors in the MG topology and incorporate them into the optimization sub-problem to reach the optimum solution with an iterative process [19]. For instance, several CSs may exchange data related to their current operation, which may help the local controllers to decide their best set-point. In this way, the data integrity weaknesses that the control algorithm must withstand are limited to a smaller area.

Last but not least, it is necessary to protect any OCPP data, either during its transfer (related to the B06a dn B08 UCs) or its storage in the CS, CSMS or the EMS. As indicated above, not only TLS or IPSec should be part of the future EVCI designs, but also cryptography primitives should be part of the encryption processes of any sensitive data in the CS, the CSMS and the EMS. Depending of the data volume and the analytic models applied, privacy-enhancing technologies should be contemplated to protect user privacy [8]. In general, CCS systems, and especially CSMS and EMS, manage multiple types of data (e.g., consumption per zone) whose access can help attackers infer private information, even if it is encrypted [21]. In addition, attackers can also deduce users' routine patterns by observing how frequently the CSs are used. Thus, more research remains to be done on techniques that (i) intensify the randomness of resource usage and device location within the infrastructure, and (ii) obfuscate the OCPP transactions to protect real consumption.

4.3 Other essential recommendations

To complement the detection processes identified in the previous section, both CSs and CSMSs must be able to automatically estimate and manage potential risks [14]. This means that the consequences of malicious interactions of (trusted) third parties, lack of physical and logical protection, and lack of testing on critical resources can be prevented by dynamically calculating potential risks. For proper governance, it is also mandatory to comply with regulatory frameworks, establish security controls and follow current strategic and organizational procedures according to current standards. Through these standards, it is possible to harmonize and incorporate new approaches (whether on the CS side, the CSMS or the EMS) complying with international and national regulatory schemes, and especially those related to the energy sector.

As mentioned above, any record can be considered a good practice that benefits the operation of other systems (e.g., SIEMs) and the governance of an organization. Through these records, it is possible to derivate security breaches by verifying the compliance with regulatory frameworks and plans. For example, updating of CS firmware is often a priority requirement within maintenance plans, and should be carried out with care, first verifying the CSMS certificate (source of the download) and firmware signature (as recommended in L01 UC instead of L02). As is evident, these solutions, and others mentioned throughout this paper, can demand high computational and storage resources to enrich analysis processes and improve decision making, impacting (in some way) the operational processes of each CS. Charging stations are often equipped with limited cyber-physical elements [6] which forces the scientific community to continue researching on solutions that are based on effective and lightweight approaches in order not to clash with operational requirements.

5 Conclusions and future work

This work comprises a risk assessment analysis with application to charging infrastructures connected to MGs under the control of the OCPP-v2.0.1 protocol. The analysis, based on the combination of the traditional methodologies STRIDE+DREAD and denoted in this work as $\mathrm{SD}^{\mathrm{c+e}}$ $-$ c, control and e, energy $-$, has proven to be a feasible tool for classifying and prioritizing threats. The results indicate that tampering and denial of service pose the greatest risks, which in turn confirms that integrity and availability requirements in critical systems are essential to ensure control of operations and availability of minimal services, such as energy. We also believe that $\mathrm{SD}^{\mathrm{c+e}}$ can be applied to other critical systems where energy and computing elements are jointly managed, giving a broad and useful perspective of vulnerabilities and threats to be faced. As a complement to this study, the paper also adds a set of recommendations for mitigation, established according to the risk analysis of $\mathrm{SD}^{\mathrm{c+e}}$ and priorities.

As future work, we intend to extend the study to contemplate new charging scenarios, such as bidirectional charging networks (V2G) and wireless charging. These types of scenarios present new threats, electronics, control and power flows, which have not yet been analyzed in the literature.

6 Acknowledgements

This work has been supported by the “Smart and Secure EV Urban Lab II” through the Second Own Plan of Smart-Campus of the Universidad de Malaga, and partially funded by the Spanish Ministerio de Ciencia e Innovacion (MICINN) by project PID2019-110531-RA-I00 from the “Proyectos de I+D+i - RTI Tipo A” programme, and by the SecureEdge project also funded by the Spanish Ministerio de Ciencia e Innovacion (AEI/10.13039/501100011033/) under Grant

PID2019-110565RB-I00.

References

[1] ISO 15118-2:2014 Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements, 2014.

[2] ISO 15118-1:2019 Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition, 2019.

[3] Threat modeling for drivers - Windows drivers | Microsoft Docs, 2021.

[4] S. Akter, T. Chakraborty, T. A. Khan, S. Chellappan, and A. A. Al Islam. Can You Get into the Middle of Near Field Communication? *Proceedings - Conference on Local Computer Networks, LCN*, pages 365–373, 2017.

[5] M. Albahar, K. Haataja, P. Toivanen, and M. A. Albahar. Bluetooth MITM Vulnerabilities: A Literature Review, Novel Attack Scenarios, Novel Countermeasures, and Lessons Learned. *International Journal on Information Technologies & Security*, 4(May 2018), 2016.

[6] C. Alcaraz, L. Cazorla, and G. Fernandez. Context-awareness using anomaly-based detectors for smart grid domains. *9th International Conference on Risks and Security of Internet and Systems*, 8924:17–34, 04/2015 2015.

[7] C. Alcaraz, J. Lopez, and S. Wolthusen. Policy enforcement system for secure interoperable control in distributed smart grid systems. *Journal of Network and Computer Applications*, 59:301–314, 2016.

[8] C. Alcaraz, J. Lopez, and S. Wolthusen. OCPP Protocol: Security Threats and Challenges. *IEEE Transactions on Smart Grid*, 8(5):2452–2459, 2017.

[9] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi. A Detailed Security Assessment of the EV Charging Ecosystem. *IEEE Network*, 34(3):200–207, 2020.

[10] F. Atlantic and B. Ra. The PEV Security Challenges to the Smart Grid : Analysis of Threats and a Mitigation Strategies. *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 300–305, 2013.

[11] C. Chen, L. Xiao, S. D. Duan, and J. Chen. Cooperative optimization of electric vehicles in microgrids considering across-time-and-space energy transmission. *IEEE Transactions on Industrial Electronics*, 66(2):1532–1542, 2 2019.

[12] J. Cumplido, C. Alcaraz, and J. Lopez. Collaborative anomaly detection system for charging stations. *Computer Security – ESORICS 2022*, pages 716–736, 2022.

[13] M. Faheem, S. Shah, R. Butt, B. Raza, M. Anwar, M. Ashraf, M. Ngadi, and V. Gungor. Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges. *Computer Science Review*, 30:1–30, 2018.

[14] S. Fischer-Hübner, C. Alcaraz, A. Ferreira, C. Fernandez-Gago, J. Lopez, E. Markatos, L. Islami, and M. Akil. Stakeholder perspectives and requirements on cybersecurity in europe. *Journal of Information Security and Applications*, 61(102916), 09/2021 2021.

[15] G. Shao. MITRE ATT&CK. ATT&CK v12, 015-2022.

[16] 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 Communications Surveys Tutorials*, 24(3):1504–1533, 2022.

[17] L. Gebauer, H. Trsek, and G. Lukas. Evil steve: An approach to simplify penetration testing of ocpp charge points. In *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4, 2022.

[18] 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 Transactions on Smart Grid*, PP(c):1, 2021.

[19] Y. Guo, H. Gao, and Q. Wu. Distributed cooperative voltage control of wind farms based on consensus protocol. *International Journal of Electrical Power & Energy Systems*, 104:593–602, 1 2019.

[20] S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal. Threat Modeling Methodologies: A survey. *Sci.Int.(Lahore)*, 26(4):1607–1609, 2014.

[21] M. Jegorova, C. Kaul, C. Mayor, A. Q. O'Neil, A. Weir, R. Murray-Smith, and S. A. Tsaftaris. Survey: Leakage and privacy at inference time. *arXiv preprint arXiv:2107.01614*, 2021.

[22] J. Johnson, T. Berg, B. Anderson, and B. Wright. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. *Energies*, 15(11), 2022.

[23] C. Jouvray, G. Pellischek, and M. Tiguercha. Impact of a smart grid to the electric vehicle ecosystem from a privacy and security perspective. *World Electric Vehicle Journal*, 6(4):1115–1124, 2013.

[24] G. Kavallieratos and S. Katsikas. Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering*, 8(10):1–19, 2020.

[25] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer. Stride-based threat modeling for cyber-physical systems. *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pages 1–6, 2017.

[26] J. H. Lee, D. Chakraborty, S. J. Hardman, and G. Tal. Exploring electric vehicle charging patterns: Mixed usage of charging infrastructure. *Transportation Research Part D: Transport and Environment*, 79:102249, 2020.

[27] G. Li, D. Wu, J. Hu, Y. Li, M. S. Hossain, and A. Ghoneim. HELOS: Heterogeneous load scheduling for electric vehicle-integrated microgrids. *IEEE Transactions on Vehicular Technology*, 66(7):5785–5796, 7 2017.

[28] Z. Li, M. Shahidehpour, and F. Aminifar. Cybersecurity in Distributed Power Systems. *Proceedings of the IEEE*, 105(7):1367–1388, 7 2017.

[29] S. Lightman and T. Brewer. Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE), 2020.

[30] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, and H. Xin. Robust and Resilient Distributed Optimal Frequency Control for Microgrids Against Cyber Attacks. *IEEE Transactions on Industrial Informatics*, 2021.

[31] Microsoft. Uncover Security Design Flaws Using The STRIDE Approach, 2019.

[32] Microsoft. STRIDE chart Microsoft Security, 2021.

[33] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, 8(1):18–43, 2021.

[34] F. Nejabatkhah and Y. W. Li. Cyber-Security of Smart Microgrids: A Survey. *Energies*, 14:27, 2020.

[35] Open Charge Alliance. Open Charge Point Protocol 1.6, 2015.

[36] Open Charge Alliance. Open Charge Point Protocol 2.0.1, 2020.

[37] C. Orellana, M. M. Villegas, and H. Astudillo. Mitigating security threats through the use of security tactics to design secure cyber-physical systems (CPS). *ACM International Conference Proceeding Series*, 2:109–115, 2019.

[38] Z. Pourmirza and S. Walker. Electric Vehicle Charging Station: Cyber Security Challenges and Perspective. *2021 9th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2021*, pages 111–116, 2021.

[39] N. Priyadharshini, S. Gomathy, and M. Sabarimuthu. WITHDRAWN: A review on microgrid architecture, cyber security threats and standards. *Materials Today: Proceedings*, 2020.

[40] J. E. Rubio, C. Alcaraz, and J. Lopez. Addressing Security in OCPP: Protection Against Man-in-The-Middle Attacks. *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, 2018-January:1–5, 2018.

[41] O. Sadeghian, A. Oshnoei, B. Mohammadi-ivatloo, V. Vahidinasab, and A. Anvari-Moghaddam. A comprehensive review on electric vehicles smart charging: Solutions, strategies, technologies, and challenges. *Journal of Energy Storage*, 54:105241, 2022.

[42] S. Sahoo, T. Dragicevic, and F. Blaabjerg. Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pages 1–1, 11 2019.

[43] A. Satapathy and J. Livingston. A Comprehensive Survey on SSL/ TLS and their Vulnerabilities. *International Journal of Computer Applications*, 153(5):31–38, 2016.

[44] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi. Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power Energy Systems*, 137:107784, 2022.

[45] S. Sen and V. Kumar. Microgrid control: A comprehensive survey. *Annual Reviews in Control*, 45:118–151, 2018.

[46] T. W. Tseng, C. T. Wu, and F. Lai. Threat Analysis for Wearable Health Devices and Environment Monitoring Internet of Things Integration System. *IEEE Access*, 7:144983–144994, 2019.

[47] C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu. Impacts of Cyber System on Microgrid Operational Reliability. *IEEE Transactions on Smart Grid*, 10(1):105–115, 1 2019.

[48] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. *Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012*, pages 55–62, 2012.

[49] Y. Zhang, J. Weng, R. Dey, and X. Fu. Bluetooth low energy (ble) security and privacy. *Encyclopedia of Wireless Networks*, 2(Bluetooth):123–134, 2020.

[50] P. Zhuang, T. Zamir, and H. Liang. Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Transactions on Industrial Informatics*, 17(1):3–19, 2021.

[51] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access*, 9:29775–29818, 2021.