White Paper of Charging Interface Initiative e.V (CharIN)

Electric Vehicle Supply Equipment (EVSE) Threat Model

2024-06-25

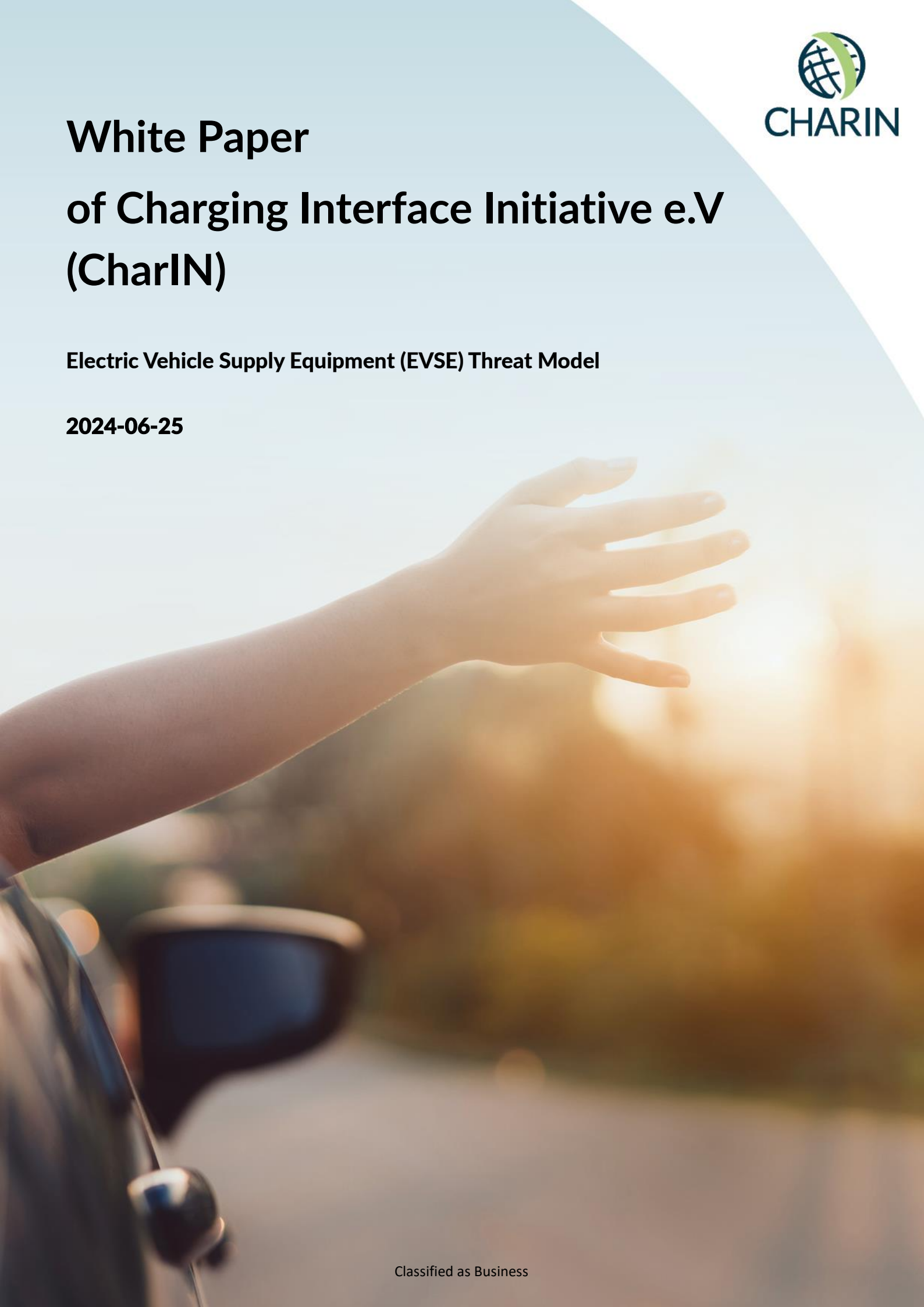

Table of Contents

1. Contributors

We would like to express our sincere gratitude and appreciation to all the contributors to this white paper, who have generously shared their insights, expertise, and feedback on the topic of cybersecurity and vulnerabilities in the electric mobility. Their valuable contributions have enriched the quality and depth of this white paper and have helped us to present a comprehensive and balanced perspective on the opportunities and challenges of electric vehicles (EVs) and their impact on human and environmental sustainability. We have together also explored the potential cybersecurity threats that exist in EV charging stations (EVSEs), communications to EVs, and upstream services, such as EVSE vendor cloud services, third party systems, and grid operators.

We hope that this white paper will inspire further dialogue and collaboration among the diverse stakeholders of the EV ecosystem and will foster a responsible and ethical development of this transformative technology.

Task Force lead:

Mayank Sharma	Schneider Electric

Subgroup lead:

Kevin Harnett	IOActive

Subgroup Members:

Theis Solberg Hjorth	Danfoss
Brian Dindlebeck	Pacific Northwest National Laboratory
Roland Varriale	Argonne National Laboratory
Maggie Shipman	Southwest Research Institute
Thomas Ruof	Mercedes Benz
Gabriella Fiore	ABB E-mobility
Heinfried Cznottka	Achelos GmbH
Zoran Radonjic	Irdeto

2. Executive Summary

The (Battery) Electric Vehicle (BEV/EV) and charging infrastructure landscape is rapidly evolving in a market where cost and time-to-market are valued higher than security. Technologies used to build the BEV ecosystem suffer from well-known cybersecurity issues, which expose vulnerabilities and risk. Current perception is that charging stations are build-and-forget devices, and not that they are highly exposed, network connected, physically vulnerable endpoints which pose a great challenge to threat mitigation.

Charging infrastructure provides necessary functionality and support for the transportation sector, which increases the need for security. The first EV charging systems were built solely with regard to mandated security requirements inherited from their components, such as payment systems. However, modern energy systems, such as Electric Vehicle Supply Equipment (EVSEs), use, or will shortly use, technologies such as smart grids and BEVs to balance renewable energy source consumption. Securing such an advanced, fully connected, and heterogeneous supply grid will take a similar effort to the ICT (Information and Communication Technology) sector that secures webservers and cloud infrastructure.

This work developed a charging infrastructure model, based on assumptions of common deployments, and identifies the common risks, threats, vulnerabilities, and design flaws that can plague these technologies when they are built without regard to security. We describe the consequences of disregarding these threats, but also highlight known risk mitigations to reduce the risk of compromise, to aid designers, builders, and auditors of these systems.

The analysis work is done on an abstract model that organizations can tailor to fit their specific implementations or systems. This work aims to inform Electric Vehicle Charging Infrastructure (EVCI) stakeholders of security issues and provide best practices on how to mitigate them.

The paper uses the High Consequence Events (HCE) methodology developed by Idaho National Lab (INL) which calculates risk exposure. This quantitative methodology augments traditional risk calculation which depends on threat, vulnerability, and consequence by adding additional impact criteria: Magnitude, Duration, Recovery Effort, Safety Costs, Effect Propagation Beyond EV or EVSE and EV Industry Confidence/Reputation Damage.

Finally, the threat scenarios were ranked by HCE score and categorized into four impact areas: (1) Generic, (2) Grid and EV, (3) Implementors and Operators, and (4) Payment and Billing. Notable, high-ranking threats in these categories include compromise of cloud hosting provider infrastructure (Generic), compromising endpoints or management servers to cause grid impact (Grid and EV), denial of EV charging (Grid and EV), physical or software tampering with EVSE to cause local (EVSE) or grid level malfunctions (Grid and EV), privileged access to administrator networks (Implementers and Operators), denial of payment processing (Payment and Billing).

3. Glossary

APT	Advanced, Persistent Threat
CharIN	Charging Interface Initiative e.V.
CPO	Charge Point Operator
CSMS	Charging System Management System
CVE	Common Vulnerabilities and Exposures
DoS	Denial of Service
DC	Direct Current
DSO	Distribution System Operator
EMI	Electro Magnetic Interference
EMS	Energy Management System
EN	Europäische Norm/European Norm (i.e., European Standards)
EVCI	Electric Vehicle Charging Infrastructure
EVSE	Electric Vehicle Supply Equipment, charging station, charge point
HCE	High Consequence Event, vulnerability ranking system
ICE	Internal Combustion Engine
ICEV	Internal Combustion Engine Vehicle
ICT/IT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
ISO	International Organization for Standardization
OEM	Original Equipment Manufacturer
PLC	Powerline communication
SAE	Society of Automotive Engineers
SDO	Standards Developing Organization
SIL	Safety Integrity Level
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. A method for threat modelling

4. Introduction

CharIN is dedicated to developing and establishing the Combined Charging System (CCS) as the standard for charging light-duty vehicles and supports the development of the Megawatt Charging System (MCS) as the standard for charging commercial vehicles.

This document was created by the Task Force Cybersecurity Work Package 2 (WP2: Threat Modeling) working group of the CharIN association. The purpose of the working group is to specify common vulnerabilities and their consequences in charging infrastructure, with focus on the EVSE (charging station).

WP2 used two types of EVSEs, as their baseline for the EVSE threat modeling:

- **Level 2 EVSEs** that offers higher-rate AC charging through 240V (in residential applications) or 208V (in commercial applications) electrical service, and is common for home, workplace, and public charging. Level 2 chargers provide 7kW-19kW of power.
- **Direct Current Fast Charging (DCFC)** equipment that offers rapid charging along heavy-traffic corridors at installed stations. DCFCs provide 50kW-350kW of power.

This work is intended to support the security analysis and risk assessment effort required by regulations such as the European Union Cyber Resilience Act[1] and the Cybersecurity Act[2].

4.1. Intended Audience

This document is intended for implementers, developers, testers, architects, designers, security officers, auditors, standards writers, and all people who need to be aware of the known attacks against the types of devices and communication technologies present in the charging infrastructure. The information is based on experience from known attacks against similar types of devices, communication technologies, APIs, and other technologies used in contexts within industry and IT.

4.2. Caveats

This document should be considered with the following caveats:

- The document's findings are limited to the assumptions it is built upon, such as the interactions between EV, EVSE, CPO, etc.
- The scoring and threats are limited by the sum of the contributors' knowledge and experience.
- The threats are defined at a high-level and not associated with specific CVEs, vendors, or hardware.
- Stakeholders and decision-makers should consider applicability of threats to their specific business use cases.

[1] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[2] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

4.3. Scoping Discussion

This document specifies common threats mapped to a high-level architectural dataflow diagram of a charging infrastructure, with a focus on the EVSE. External services and their connection to the EVSE are also included, such as payment systems, operators, vendors, users, grid, etc.

While we ranked threats and proposed mitigations, these were completed at a very high model level based on a simplified architecture model to provide widespread applicability (See Appendix A). Threats will likely need additional analysis and adaptation to fit a specific business implementation.

Topics out of scope include backend systems, databases, cloud technology, and most of the architecture that is not directly connected and communicating with the EVSE. Implementations are also out of scope in order to provide a high-level threat model that is suitable for different and evolving setups.

4.4. Methods of Analysis

The threat modeling method used within this white paper to identify threats and mitigations is STRIDE (Kohnfelder & Garg, 1999), (Shostack, 2014), based on examining each element in the system model and enumerating common attack techniques against the system. As threats generally tend to follow the transfer and storage of data, STRIDE is applied to dataflow models.

The model of the attacker is classified as a Dolev-Yao intruder, i.e. the attacker has full knowledge of the system and can intercept and alter any flow of data between interfaces.

Threat scenarios have been identified, based on known attack patterns. They are a simplified version of a kill chain or attack tree, since specifying the consequences of an attack is difficult without a specific implementation to examine. However, threat scenarios illustrate the impact in a way that can be mapped to an existing system.

Threats to the charging infrastructure have been ranked using the High Consequence Event (HCE) method, which is further defined in *Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure* (Carlson, et al., 2023). The threat model provided in this paper should be a guideline to assist in ranking efforts of other systems.

We have noticed that some rankings differ based on cultural and legislative differences across geographical territories, so readers are encouraged to use the rankings here only as a baseline for ranking an actual system. The HCE ranking system also lacks a clear mechanism for ranking Advanced Persistent Threats (APTs), i.e. threats that exploit a vulnerability and then lie dormant and undetected for long periods of time.

4.5. Threat Modeling with STRIDE

This section has a brief introduction to STRIDE, followed by a short discussion of how STRIDE does not include consequences of exploited threats, and how threat scenarios add this context.

STRIDE is an acronym representing a security threat modelling method where each letter represents a different kind of threat: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege, as defined in Figure 1.

The original article introducing **STRIDE** (Kohnfelder & Garg, 1999), defines threat, vulnerability, and attack as follows (emphasis added in italics):

Threat: Any potential *occurrence*, malicious or otherwise, *that can have an undesirable effect on the system resources* (files, registry keys, data-on-wire, etc.). Undesirable effects can be a system crash, the ability to read a sensitive file or modify a registry key, and so forth.

Vulnerability: Some *characteristic that makes it possible for a threat to occur*. Examples include weak security on a file, buffer overflows, and (in a server product running on Windows NT) missing client impersonation calls when servicing client requests.

Attack: An *action taken* by a malicious intruder *to exploit certain vulnerabilities to enact the threat*. Examples of attacks include steps taken by a non-administrator to acquire administrator privileges and a technique that allows private data to be leaked.

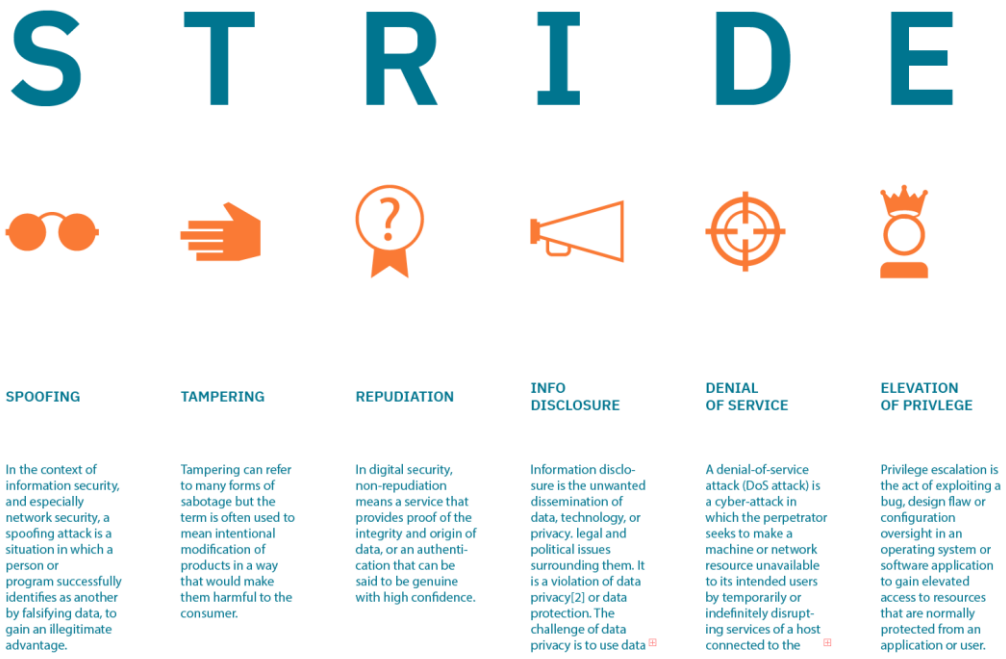

Figure 1 STRIDE overview[3]

[3] https://developer.ibm.com/articles/threat-modeling-microservices-openshift-4/

STRIDE is a popular tool for improving security of software during development. The authors also include examples of a threat or vulnerability for each element of STRIDE, such as this example for repudiability:

"Undetected attempts to break into a user account by the attacker.
Lack of failed logon audits is the vulnerability"

Threat models, such as STRIDE, do not take into account the real-world consequences of the attacker's action. This paper attempts to address the missing consequence of an action with threat scenarios. A threat scenario is a short narrative that describes an actor's actions, the exploited vulnerability, and the resulting consequence. Using the previous example, the threat scenario might be, "Undetected attempts to break into a user account by an attacker *allows an attacker eventual access to the user account*, *which allows an attacker to perform additional malicious activity under the guise of an authorized user*" (Kohnfelder & Garg, 1999), where the italics embody the effect or *impact to an organization's objectives* which must be considered for a cyber-physical system such as the EV ecosystem. The italicized text is absent from the STRIDE example because STRIDE does not consider consequences as a result of exploited vulnerabilities.

5. EVSE Threat Modeling

5.1. Threat Model Findings

This section introduces the methods used for threat modelling, and at the end is an abbreviated table of the highest ranked threats. The full table is in Appendix A.

5.1.1. How To Read Threat Model Findings

The threat model findings are read by inspecting a threat scenario for the impact of a focus of concern and cross-examining the score for a given category.

As an example, consider the abbreviated threat scenario “An attacker physically tampers with EVSE power electronics to damage EVs or the grid (compromised electricity load balancing)”. The overall HCE Severity Score is 3.5 out of 5, representing moderate severity. “Magnitude”, “Duration”, and “Effect Propagation Beyond EV or EVSE” are all 5, so those contribute most to the score. Depending on role, a reader may have more interest in a score of 5 for “Duration” than “Effect Propagation Beyond EV or EVSE”.

A cybersecurity implementer may focus on mitigating grid impact by addressing the “Level of Impact” score. In conclusion, the objective in reading the threat model findings is to identify the impacted focus of business concern and identify criteria for mitigation.

5.1.2. Threat Model Assumptions

When creating and refining these threat models, the authors intended to be comprehensive in including necessary functioning parts of the EVSE, while also excluding certain systems and components that may not provide value to the general EVSE stakeholder. Due to the interdependence of an EVSE, many disparate and specialized systems may need to be accounted for. Several threat models may expound upon our core threat model and offer hypotheticals based on subject matter expertise or personal experience with these systems. The models and scenarios presented within this white paper were refined through several rounds of internal review to ensure that a unified vision of core EVSE capabilities were covered.

The rapid evolution and advancement of EVSE componentry and implementation may give rise to deviations from the supplied threat model. This requires both an adaptation of the results presented in this white paper, and also that the work is revised and updated periodically.

5.1.3. Legislation and Regional Differences

There are differences and similarities between the use cases and regulations for EVs in the European Union and the USA. As an example of regulatory similarities, relevant authorities in both locales have determined to procure only EVs for certain sectors or for the whole population, with similar timelines through approximately 2035. Figures 2 and 3 show approximate timelines for some selected EV OEMs.

Contrastingly, the EU and USA EV infrastructures have a similar appearance, but the connections between entities may not be the same. For example, in the USA, it is possible that a charging station operator is also the local electric utility. Another important distinction is the perceived inevitability of electric vehicle adoption in Europe where it is already law. This difference was made apparent during discussions amongst the authors. The use cases, regulatory differences, and cultural perspectives have been incorporated in the threat model.

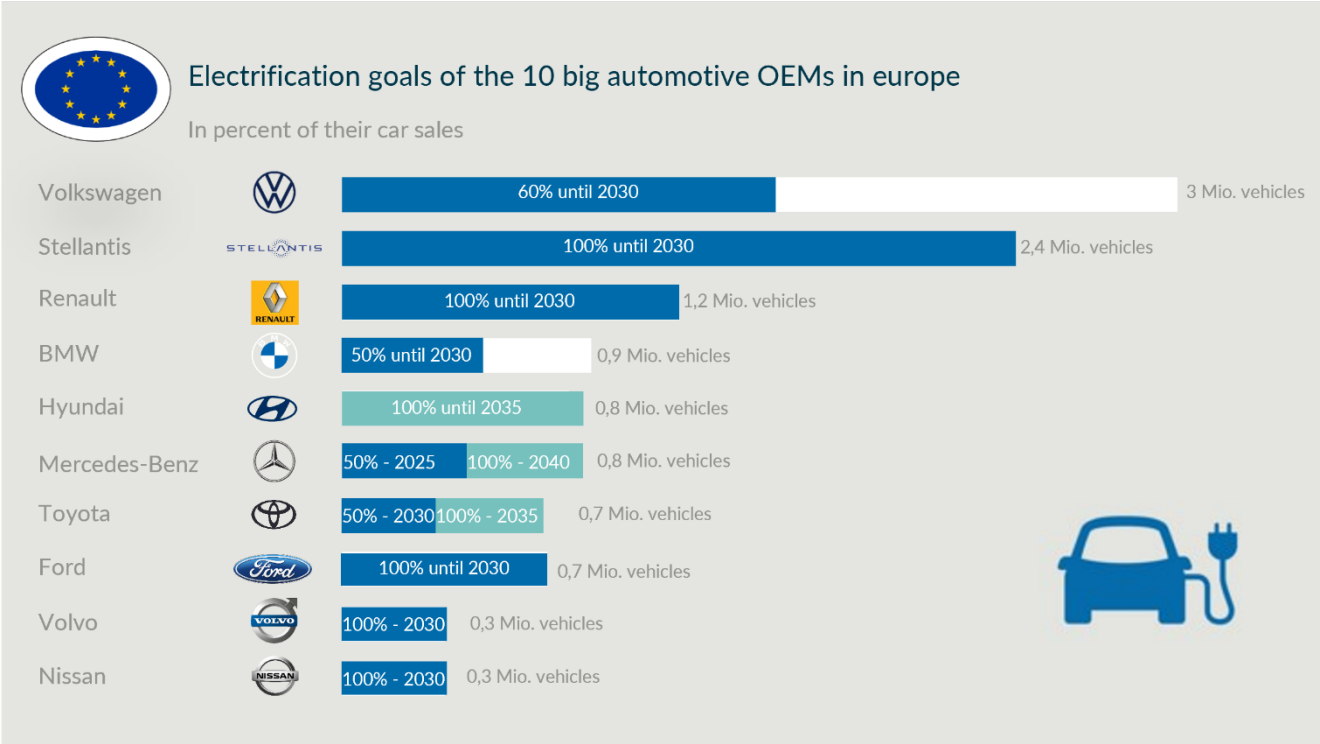

Figure 2 Electrification goals for the Europe Union (Tausendteufel, 2022)

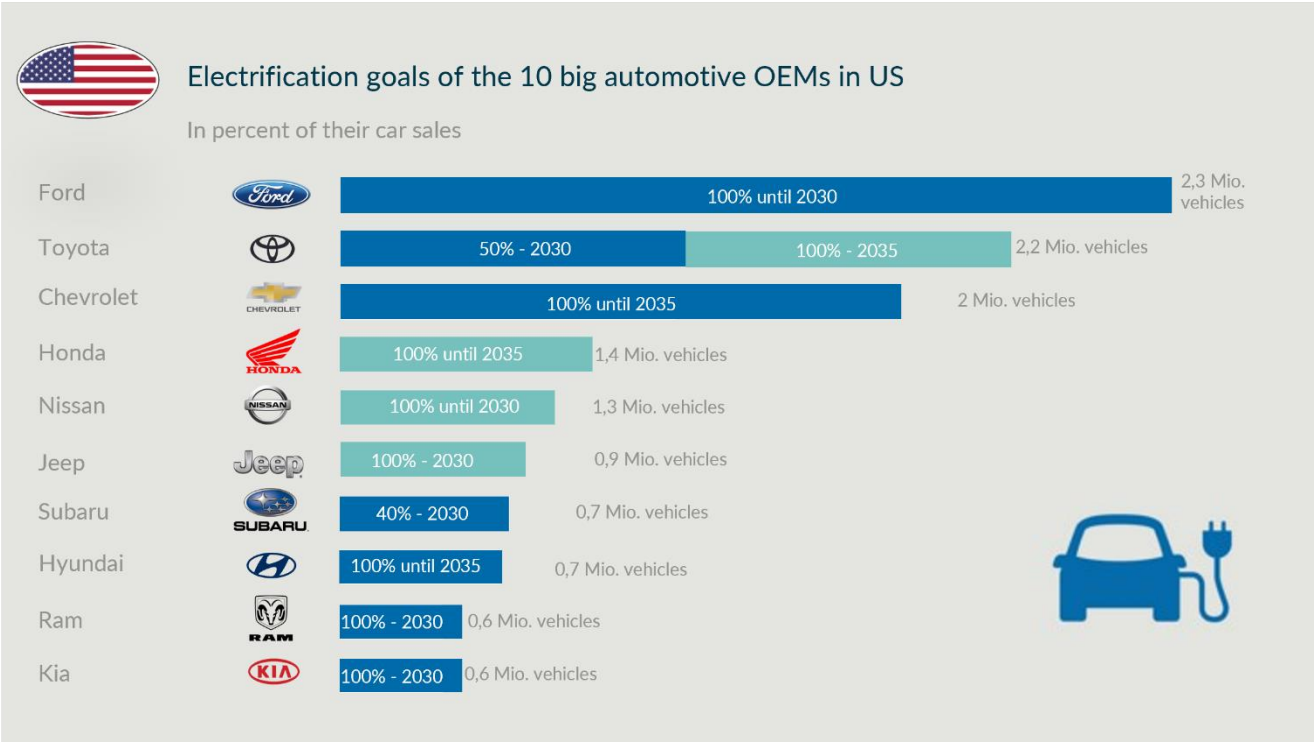

Figure 3 Electrification goals for the USA (evadoption, 2018)

The following releases exemplify the worldwide trends for the adoption of EVs over the coming years:

- In the USA, Executive Order 14057[4] restricts all government agencies' new acquisitions of light-duty vehicles to only EVs by 2027 and mid- and heavy-duty vehicle acquisitions to only EVs by 2035.
- In California, Executive Order N-79-20[5], ends sales of ICE passenger vehicles and trucks by 2035[6].
- The EU and UK have banned sales[7] of new combustion engine cars from 2035.

Also, in the current political climate, the recycling of battery components is a matter of national sovereignty, since critical raw materials are imported from places that do not always agree with democratic ideals:

- The EU has enacted a law on the acquisition of critical raw materials[8], some of which are used for battery components.

In addition, the EU will mandate recycling of battery materials[9]

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/08/executive-order-on-catalyzing-clean-energy-industries-and-jobs-through-federal-sustainability/
[5] https://ww2.arb.ca.gov/resources/fact-sheets/governor-newsoms-zero-emission-2035-executive-order-n-79-20
[6] https://www.gov.ca.gov/wp-content/uploads/2020/09/9.23.20-EO-N-79-20-Climate.pdf
[7] https://www.europarl.europa.eu/topics/en/article/20221019STO44572/eu-ban-on-sale-of-new-petrol-and-diesel-cars-from-2035-explained https://www.gov.uk/government/publications/transitioning-to-zero-emission-cars-and-vans-2035-delivery-plan
[8] https://www.europarl.europa.eu/news/en/agenda/briefing/2023-12-11/1/critical-raw-materials-securing-the-eu-s-supply-and-sovereignty
[9] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/european-critical-raw-materials-act_en

5.2. Threat Model Diagrams

The presented threat model is based on the architecture model specified in Appendix A. This architecture is a simplified model, and any practical deployment will differ. This means the threat model is not exhaustive and may be inaccurate in some places; therefore, some conventional wisdom needs to be applied to map the model to a real EVSE system.

The threat scenarios point out common problem areas that may or may not exist in a given system, and do not provide a complete checklist of all the threats that must be considered. Its purpose is to guide the reader to think about parts of the system that may be overlooked, or those for which someone else may be assumed to be responsible for securing when in fact no one has thought of it. This should also assist with threat modeling for these missing parts by providing a partial picture of the types of threat scenarios for a given component.

The identified threats scenarios were ranked using the HCE method, which the authors define as a quantitative methodology that augments traditional risk calculation, which depend on threat, vulnerability, and consequence by adding an additional impact feature. The method uses eight categories of impact, and a rank from zero to five in each category, where zero is no impact and five is the highest severity of impact. Figure 1 includes the definitions of each of the criteria from *Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure* (Carlson, et al., 2023). The HCE Severity Score is the average score of the individual criteria score.

There are four kinds of stakeholders that could be impacted by the conclusion of a threat scenario. For the purposes of the threat model and scoring, each threat scenario only impacts one stakeholder. In the real world, most threat scenarios will impact more than one stakeholder. The four categories of Generic, Grid & EV, Implementers & Operators, and Payment & Billing are an attempt to balance the utility of this document for stakeholders and estimate the most likely impacted stakeholder.

The Impact On column represents the stakeholder that could be impacted by a given threat scenario, and is meant to aid reading comprehension of the table:

- Generic: These do not fit in one of the other categories or were highly likely to impact more than one category.
- Grid & EV: These are threat scenarios to the power grid and EV.
- Implementers & Operators: These are threat scenarios to implementers and operators, which includes CPOs and EVSEs.
- Payment & Billing: These are threat scenarios to the payment and billing stakeholders.

Criteria	Not Applicable (N/A) (0)	Low (1)	Medium (3)	High (5)
Level of Impact	N/A	Single unit affected (EV, XFC, or WPT)	Multiple units at a single site affected (EV, XFC and/or WPT)	Multiple units at multiple sites affected (EV, XFC and/or WPT)
Magnitude (proprietary / standardized)	N/A	Manufacturer-specific protocol implementation (EV or EVSE)	>1 manufacturer protocol implementation (supply chain) (EV or EVSE)	Across all standardized systems (both EVSE and EVs)
Duration	N/A	<8 hours	>8 hours to <5 days	>5 days
Recovery Effort	Automated recovery without external intervention	Equipment can be returned to operating condition via reset or reboot (performed remotely or by onsite personnel)	Equipment can be returned to normal operating condition via reboot or servicing by offsite personnel (replace consumable part; travel to site)	Equipment can be returned to normal operating condition only via hardware replacement (replace components, requires special equipment, replace entire units)
Safety	No risk of injury or death	Risk of minor injury (no hospitalization), but NO risk of death	Risk of serious injury (hospitalization), but low risk of death	Significant risk of death
Costs	No costs incurred	Cost of event is significant, but well within the organization's ability to absorb	Cost of event will require multiple years for financial (balance sheet) recovery	Cost of event triggers a liquidity crisis that could result in bankruptcy of the organization
Effect Propagation Beyond EV or EVSE	N/A	Localized to site	Within metro area	Regional
EV Industry Confidence, Reputation Damage	No impact to EV adoption	Minimal impact to EV adoption	Stagnant EV adoption	Negative EV adoption

Table 1. HCE Ranking description (Carlson, et al., 2023)

5.3. Summary Findings

Table 2 is a summary table of findings, sorted by impact area and then the HCE score. For the complete list of threat scenarios, including vulnerability descriptions and mitigations, see Appendix A: Threat Model Details. The purpose of this table is to provide an overview of what are probably the most severe threats in each category, as a guideline for prioritizing further analysis.

The summary table defines the threat scenarios, which involve the consequences of an attack and how the attack was conducted. The reader should remember the context of a given threat scenario while reading.

The terminology is explained in section 5.1.1.

Threat Scenario	Impact on	HCE Severity Score	Level of Impact	Magnitude	Duration	Recovery Effort	Safety	Costs	Effect Propagation Beyond EV or EVSE	EV Industry Confidence, Reputation Damage
An attacker compromises privacy/sensitive data by compromising the cloud hosting provider of the vendor or operator	**Generic (non-specific)**	3.375	5	3	5	3	0	3	5	3
An attacker gains access to a device via downgrade attack	**Generic (non-specific)**	2.125	5	1	5	2	0	2	1	1
An attacker obtains genuine access credentials to devices because the credentials are not properly protected	**Generic (non-specific)**	1.875	5	1	5	1	0	1	1	1
An attacker compromises exposed management console to change active frontend rectifier setpoints	Grid & EV	4	5	5	5	4	2	3	5	3
Attacker injects false data into energy markets to imbalance grid or manipulate energy costs	**Grid & EV**	3.625	5	3	3	4	2	3	4	5
CSMS transmits false data to DSO to cause unnecessary islanding event	Grid & EV	3.5	4	5	5	4	0	4	5	1
Compromised updates falsify EV reported remaining distance	Grid & EV	3.5	5	3	5	3	1	4	5	2

An attacker physically tampers with EVSE power electronics to damage EVs or the grid (compromised electricity load balancing)	Grid & EV	3.5	1	5	5	4	2	3	5	3
An attacker uses CSMS to broadcast RemoteTransactionStop, causing voltage transients on the grid	Grid & EV	3.5	5	3	5	3	2	3	5	2
An attacker denies charging via wireless interference on the charging cable	Grid & EV	3.375	2	5	5	3	2	3	5	2
An attacker leverages a large number of EVs to abort charging, causing undesirable grid impacts	Grid & EV	3.25	5	1	5	3	2	3	5	2
Compromised DSO limits CSMS load, impeding charging and CSMS revenue	Grid & EV	3.125	5	1	5	3	0	5	5	1
An attacker abuses a compromised EVSE to spread malicious code onto vehicles while they charge	Grid & EV	2.75	5	2	5	3	0	3	3	1
EVSE transactions lose non-repudiation via CSMS compromise, enabling an actor to provide free electricity at one or many EVSEs	Grid & EV	2.625	5	1	5	3	0	1	5	1

Attacker alters EVSE power electronics firing angle, reducing power factor correction	**Grid & EV**	1.875	3	1	3	2	2	2	1	1
Attacker modified cord set injects 15118 responses, causing a race condition, so the EV connects without TLS	**Grid & EV**	1.875	2	1	5	3	0	1	0	3
Physical tampering to force EVSE into faulted state to prevent charging	Grid & EV	1.625	1	1	5	3	0	1	1	1
An attacker gains access to the EVSE and extracts confidential data	Grid & EV	1.5	3	1	2	3	0	1	1	1
An attacker alters unencrypted data in transit	Implementers & Operators	3.375	5	3	5	3	0	3	5	3
Attacker gains admin access by impersonating remote admin tools	Implementers & Operators	3.375	5	3	5	3	0	3	5	3
An attacker impersonates the client (EV, EVSE, App, etc.) with copied credentials	Implementers & Operators	2.25	4	2	5	3	0	1	2	1
An attacker gains control of the DNS server the device uses to redirect configuration updates, firmware updates, trusted entity	Implementers & Operators	2.125	5	1	5	2	0	2	1	1

updates, certificate renewal, etc. to a malicious server										
EVSE requires physical servicing following attack that causes a faulted state	Implementers & Operators	1.625	1	1	5	2	0	2	1	1
An attacker uses a privileged physical connection to upload malware or alter device configuration data	Implementers & Operators	1.5	1	1	5	2	0	0	0	3
An insider at a third-party vendor executes unauthorized software on a network host or device	Implementers & Operators	1.375	5	1	1	1	0	1	1	1
An attacker prevents communication from EVSE to payment system	Payment & Billing	3.125	3	3	5	3	0	3	5	3
Vehicle ECU swap to bill power transfer to someone else	Payment & Billing	2.5	1	2	3	5	3	2	3	1
EVSE cannot access necessary cloud services to process payment	Payment & Billing	2.375	1	1	5	3	2	3	1	3
Payment interface requires maintenance EVSE user account creation with weak password/credentials	Payment & Billing	2.25	1	3	5	3	2	1	1	2
Payment system uses vulnerable third-party libraries	Payment & Billing	2.25	1	3	5	3	2	1	1	2

Attacker leverages EVSE to modify payment processing execution flow or data path	Payment & Billing	1.875	5	1	5	1	0	1	1	1
Spoofed or cloned RFID allows attacker to bill power transfer to another party	Payment & Billing	1.75	1	0	3	5	2	2	1	0

Table 2 – EVSE Threat Scenarios HCE Rankings

6. Conclusions and Next Steps

In 2023, events in Europe have shown that nation states are willing and capable of using cyberwarfare as a means of disrupting infrastructure, such as telecommunications, food production, and energy production. EV charging infrastructure is critical for the transport sector of a nation; therefore, it is a target for both state-sponsored and organized crime; the differences between the two have become blurrier in past years. The digital, connected nature of EV charging infrastructure makes it vulnerable to malware, ransomware, Denial of Service (DoS) attacks, and other remote attacks that are defined in this white paper.

The scope of this white paper is limited to the EVSE charging station, which is central to the EV infrastructure, but the grid, EVSE vendor, payment, and operations are also targets for attackers, and the threat modelling of these entities is left as future work.

Identifying common threats relevant to the charging infrastructure model revealed some notable classes of threats and vulnerabilities, and other insight that bear highlighting, along with possible mitigations.

6.1. Key Future Considerations

The EV charging infrastructure requires a higher level of connectivity between the vehicle/driver and provider (EVSE) than any previously deployed transportation system. Users (drivers) interact with potentially dangerous power electronics of a voltage class previously only found in industrial applications, and normally only handled by qualified people.

The following are key future considerations:

Charging stations are a new type of public IIoT device

The term Industrial Internet of Things (IIoT) refers to interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management. While the compromise of a single charging station is not critical, the compromise of thousands of EVSEs simultaneously would be critical to national security. This means the infrastructure as a whole is vulnerable to systemic or architectural attacks.

IIoT and other critical devices used in commercial, retail, industrial, or similar contexts are traditionally implemented as closed ecosystems and not accessible by untrained personnel. Existing and similar public infrastructure devices (such as fuel pumps, ATMs, etc.) are normally operated on smaller scales and not widely connected. The highly connected and shared digital infrastructure required for future EVSEs is more similar to ICT infrastructure than traditional industrial device deployments.

Telemetry and EVSE charging planning data

If battery technology does not drastically improve, the user experience and charging time management must improve, in combination with data-driven deployment of charging stations. Planning infrastructure deployment requires telemetry of user behavior and volume along certain routes to measure and keep up with demand, including accounting for seasonal changes and events (e.g., concerts, sports, festivals, holidays, tourism, etc.). Gathering telemetry on how often chargers are used is necessary to plan infrastructure expansions.

On a separate scale, vehicles would also need to be able to plan routes and book timeslots for charging along the road for a trip, in order to accurately predict arrival times, including rebooking or rescheduling when delays occur. This is especially important for goods transport and food safety.

This telemetry and measurement data would be vulnerable to interception and manipulation, as well as privacy violations.

Recovery from cybersecurity attacks

Many malware threats are exacerbated if the EVSE is not capable of recovering from a compromise/attack via a secure remote firmware update mechanism. Without such a mechanism, recovery from compromise requires physical access, which is expensive and does not scale well. Mitigation requires hardware-based security, and a software secure enclave or secure state that the EVSE can go back to (i.e., erase compromised code and install trusted firmware). In addition, we have seen examples of state-sponsored malware groups pre-positioning by infiltrating critical infrastructure and lying dormant for months or years without detection, which means that the lack of malfunction does not mean a lack of infiltration.

Ongoing maintenance of trusted devices

The traditional mindset of "build-deploy-forget" used for embedded devices in the public space is not compatible with a world in which zero-day attacks are actively exploited 15 minutes after publication. Similar to the way in which websites establish secure connections to browsers, the use of a Public Key Infrastructure (PKI) is necessary to establish trust between charging stations, operators, vehicles, and vendors. PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[10] and manage public-key encryption[11] to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

As with webhosts on the Internet, such a system requires maintenance, monitoring, and regular renewal of certificates.

End-of-life software support for power electronics

The maintenance and software hygiene required to keep a system secure also means that when a vendor decides to stop offering security patches for an EVSE product, due to the interconnectedness of the charging infrastructure, the infrastructure itself can become vulnerable to attack, not just the devices that are no longer supported. A single insecure networked device becomes a threat to the network, and its impact can extend beyond the vulnerable device itself, because it is part of a larger interconnected system. It is unclear how to handle such situations if charging stations are expected to last for decades.

If a device is no longer supported, who is responsible for maintaining it? For example, if a charging station no longer receives vendor security updates after five years, will the station be scrapped because it is a threat to the charging infrastructure? Discarding EVSE charging station hardware because the software is no longer updated seems contrary to some countries' pledges of reducing e-waste.

[10] https://en.wikipedia.org/wiki/Public_key_certificate
[11] https://en.wikipedia.org/wiki/Public-key_cryptography

Continued operation of charging stations when the vendor ceases to exist

When goods, public, and private transport are all electrified and charging stations are critical to transport infrastructure (for example, ensuring perishable food is not damaged and causes safety concerns), there are questions around whether software will be required to be public or in escrow along with the private keys for the devices‘ Public Key Infrastructure (PKI). This would enable another vendor to take over maintenance and updates. In Europe, other types of critical infrastructure are regulated to ensure continuity and shared access.

There is also a challenge in notification when EVSE charging stations are no longer maintained. Unless reporting is mandatory, vulnerable charging stations could continue to operate without anyone being aware of it. Operators will need to be audited to ensure the charging stations they are responsible for are updated, and that they are still supported by the vendor.

Insider attacks

Even if there is an architectural assumption that only legitimate CPOs, vendors, payment services, and other trusted parties have access to the infrastructure, it is still vulnerable to insider attacks.

As with any large public architecture, bad actors are a threat: These are actors that can get into the system via legitimate means and become an inside attacker. It is entirely possible to spoof any of the companies in the EVSE ecosystem and gain access to critical data/systems as a trusted entity.

6.2. Mitigations

This section contains suggestions of known mitigations for the threats presented in this white paper.

6.2.1. Meta-mitigations for Systemic and Architectural Threats

As mentioned in a previous section, there are classes of threats to the charging system itself which will require mitigations:

- High connectivity of an Industrial Internet of Things (IIoT) device
    - Mandatory security features in EVSE devices, on par with mandatory EMI, fire safety, etc. Conformance testing will be needed. Focus on resilience, monitoring, and recoverability.
    - The adoption of a security framework, e.g., IEC 62443 (Security for Industrial Automation and Control Systems, and mandatory full (or partial) compliance with it. This is already the strategy for other industrial sectors, e.g., marine societies.
- Gatekeeping, monopolies/cartels, vendor lock-in, proprietary extensions:
    - An existential threat to any widely deployed, shared public architecture, is the motivation of companies to monopolize, gatekeep, use vendor lock-in, use patents, use proprietary protocols/formats, and otherwise interfere with an ecosystem to dominate parts of it at the expense of users. Traditionally, such threats to the architecture can be mitigated with open standards and regulatory enforcement to use them.
    - Mandatory compliance with harmonized standards. The EU is already moving towards this standards-based approach (e.g., CCS2 plug standard).
    - Be aware that cryptography makes it very easy to create artificial incompatibility — its very purpose is to block actions. Require the use of open standards for communication and security protocols without proprietary extensions that seek to undermine compatibility.

    - Mandatory compatibility for payments: currently in the EU there is a patchwork of different loyalty card schemes for accessing charging stations. Similarly in the United States payment system implementations differ across vendors, contain a mix of payment as a service or APIs, and do not currently offer unified models or architectures.
    - There are already consultancy companies selling ways to integrate EV charging into rewards, discounts, offers, points-based programs, and other loyalty schemes, all of which potentially influence the mass transit networks of cities.
    - The car transit network and its business model are very different from traditional, regulated fuel prices and oil companies. There needs to be price regulation on publicly accessible charging stations.
- Security infrastructure and PKI
    - Require use of standardized PKI methods and providers. Mandatory processes for handover of secrets for sunsetting companies, to ensure business continuity.
    - Annual compliance cybersecurity testing of PKI and security infrastructure for vendors.
    - Mandatory secure recovery functionality for EV charging stations. Considering the capabilities of state-level malware, the assumption must be that it is possible to compromise the connected network of EV charging stations and inject malware. There must be an agreed recovery method from such an attack that vendors have implemented in devices, or at least they must be liable for fixing their devices when they are attacked. Any recovery method, like any backup method, must be regularly exercised to prove it is still working.
    - Develop vetting procedures for companies that deploy EVSE infrastructure networks and APIs. Establish proper trust boundaries that still assume hostile actors can become part of the infrastructure and payment networks.

6.2.2. Mitigations for EVSE Devices and Organizations

The threat model in Appendix A: Threat Model Details lists mitigations for each threat in more details, but there are a few general principles that should also be followed.

To achieve security, defense-in-depth must be used; in general, this means that mitigations must overlap, and multiple mitigations are necessary for each threat, because one will inevitably fail, and it will be unknown which one will fail.

The design principles in *The protection of information in computer systems* (Saltzer & Schroeder, 1975) are still sound. EV charging stations should be secure-by-design due to what they actually are: highly critical, highly exposed, highly connected, highly attractive targets for cybercriminals to conduct malicious harm to national security and obtain financial gains. EVSEs are not traditional industrial systems that live in a closed ecosystem, they are exposed to the worst of the Internet, and cannot be fully physically secured.

It is important to both be specific about implementations of mitigations and to evaluate them regularly. For instance, a mitigation might add the TLS protocol to a communication channel, but there are many ways to implement TLS without actually making it secure, such as:

- Not making it mandatory to use TLS, or by allowing insecure ciphers
- Allowing downgrade attacks, by only mandating authentication of the server and not the client
- Not securing the Public Key Infrastructure that manages device identities and trust
- Not updating the software libraries when vulnerabilities are found

Traditional industrial development and deployment methods have been focused on time-to-market and request queues of new features for customers. Unfortunately, this comes at the expense of software quality and security especially. This is apparent from research into the state of security in Industrial Internet of Things devices (Al-Zahrani, 2023), (Marianna Lezzi, 2018), (Serror, 2021),Operational Technology (Sisinni, Saifullah, Han, Jennehag, & Gidlund, 2018), vulnerability reports[12] and advisories for Industrial Control Systems (ICS)[13],[14], etc.

Security management is about focusing on code robustness, continuous implementation of a Secure Development Life Cycle (SDLC) process, and security patch distribution. Compliance with a framework such as IEC 62443 (security in industrial automation and control systems), the ISO 27000 series (security and risk assessments of ICT systems), and the NIST 800 series (security and risk assessment of ICT systems) shows that a vendor has not only understood this, but also implemented it in their development processes.

[12] https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/
[13] https://cve.ics-csirt.io/cve
[14] https://www.cisa.gov/news-events/cybersecurity-advisories

7. Frameworks and Harmonized Standards

Several references and standards exist to create a comprehensive look at how to operate, secure, and protect EVSEs. Furthermore, these can be combined with industry standard documents such as MITRE's ATT&CK framework and the OWASP Top Ten, which are applicable but do not specifically address EVSE, to create more detailed and tailored recommendations to organizations. This section will highlight each of these standards and references at a high level to provide background into existing EVSE cybersecurity work.

IEC 62443[15] Cybersecurity for Industrial Control and Automation Systems

This standard outlines a security profile for SCADA/ICS, OT and IoT devices which aligns well with components and technology used within EVSEs and interface systems. These commonalities allow for portability of this standard to this specific application which offer a good starting point for assessing EVSE development, production, and operation.

OWASP Top Ten[16]

This list is a periodic survey, aggregation, and analysis of top web application vulnerabilities based on a survey of security professionals.

MITRE ATT&CK Framework[17]

A knowledgebase of tactics, techniques, and procedures for adversary behavior. There are databases for enterprise systems, mobile devices, and Industrial Control Systems. The information is based on threat intelligence and incident reports. Furthermore, ATT&CK contains threat profiles and known tools, tactics, and procedures for threat groups and APTs.

ISO 27000 Series[18]

The ISO 27000 series is a collection of standards for IT security that cover the complete lifecycles of patch management, risk assessment, security for network, applications, storage, systems, privacy, and other systems.

[15] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[16] https://owasp.org/www-project-top-ten/
[17] https://attack.mitre.org/matrices/ics/
[18] https://www.iso.org/standard/iso-iec-27000-family

NIST SP 800 Publications[19]

The NIST SP 800 publications cover security and risk management, in a similar way to the ISO 27000 series. SP 800-53[20] in particular is about security and privacy controls for IT. Other SP 800 standards cover frameworks for risk assessments, software development lifecycles, etc.

ISO 15118-2[21] and 15118-20[22]

These two standards outline implementations and specifications for EV to EVSE communications during a charging session, mainly within the networking layer.

Open Charge Point Protocol (OCPP)[23]

OCPP represents the main protocol stack that EVSEs use to communicate power demands. Currently, two main versions of the protocol are in use: OCPP 1.6 and 2.0, which both utilize WebSockets for communication, but have slightly different architectures, guarantees, and implementations.

Idaho National Laboratory (INL) High Consequence Events (HCE) [24]

This methodology takes INL's previous approach towards calculating risk exposure with consideration to resilience with the premise that certain events may not occur frequently, but their existence poses an asymmetric risk to operational capabilities. This quantitative methodology augments traditional risk calculation which depends on threat, vulnerability, and consequence by adding an additional impact feature.

ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering[25]

ISO/SAE 21434 is an international standard that defines the requirements and processes for cyber security engineering in road vehicles.

[19] https://csrc.nist.gov/publications/sp800
[20] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
[21] https://www.iso.org/standard/55366.html
[22] https://www.iso.org/standard/77845.html
[23] https://www.openchargealliance.org
[24] https://www.sae.org/publications/technical-papers/content/2023-01-0047/
[25] https://www.sae.org/standards/content/iso/sae21434/

8. References

Al-Zahrani, F. S. (2023). Industrial Internet of Things: A Cyber Security Perspective Investigation. *2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC).* doi:10.1109/ICAISC56366.2023.10085080

Carlson, B., Rohde, K., Crepeau, M., Salinas, S., Medam, A., & Cook, S. (2023). *SAE*. Retrieved from https://www.sae.org/publications/technical-papers/content/2023-01-0047/

evadoption. (2018). Retrieved from https://evadoption.com/ev-sales/evs-percent-of-vehicle-sales-by-brand/

Kohnfelder, L., & Garg, P. (1999, April 1). The threats to our product. Retrieved from https://web.archive.org/web/20230701095532/https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

Marianna Lezzi, M. L. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. In *Computers in Industry* (Vol. 103, pp. 97-110). doi:https://doi.org/10.1016/j.compind.2018.09.004.

Saltzer, J., & Schroeder, M. (1975, September). The protection of information in computer systems. *Proceedings of the IEEE*. Retrieved from https://ieeexplore.ieee.org/document/1451869/authors#authors

Serror, M. a. (2021). Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *17*(5), 2985-2996. doi:10.1109/TII.2020.3023507

Shostack, A. (2014). *Threat Modeling: Designing for Security.* Wiley.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, 4724 - 4734.

Tausendteufel, F. (2022, May). *Agora Verkehrswende*. Retrieved from https://www.agora-verkehrswende.de/veroeffentlichungen/automobilhersteller-und-ihre-elektrifizierungsziele/

Appendix A: Threat Model Details

An initial version of the threat model is captured in Appendix; however, as previously stated, this is a mutable document that the authors intend to be revised and updated over time as EVSEs evolve. As such, these findings are presented as a starting point for discussion and inclusion within organization-specific threat models and risk assessments. These findings may have limited applicability within specific organizations and more applications within others, which this working group aims to satisfy by creating a core model which can be extended as needed (see Threat Model Assumptions in section 5.1.2 of this document).

A.1. Threat Model Dataflow Diagrams

Each diagram represents the dataflow of a part of the EVSE and an external system. The labels correspond to the labels in the threat scenarios in section A.3 showing the approximate logical location of a threat in these high-level dataflow models.

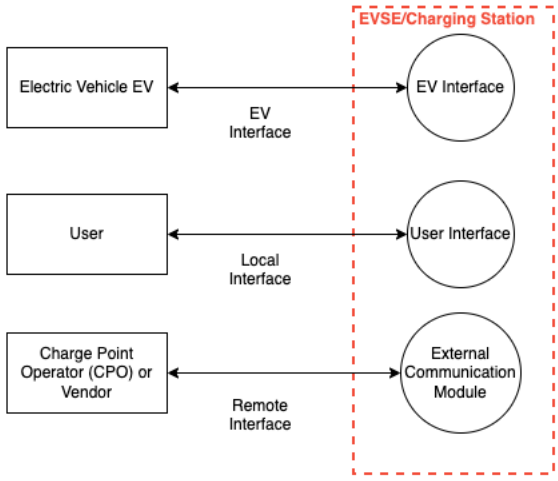

Figure 4. T0 diagram, High-Level Architecture

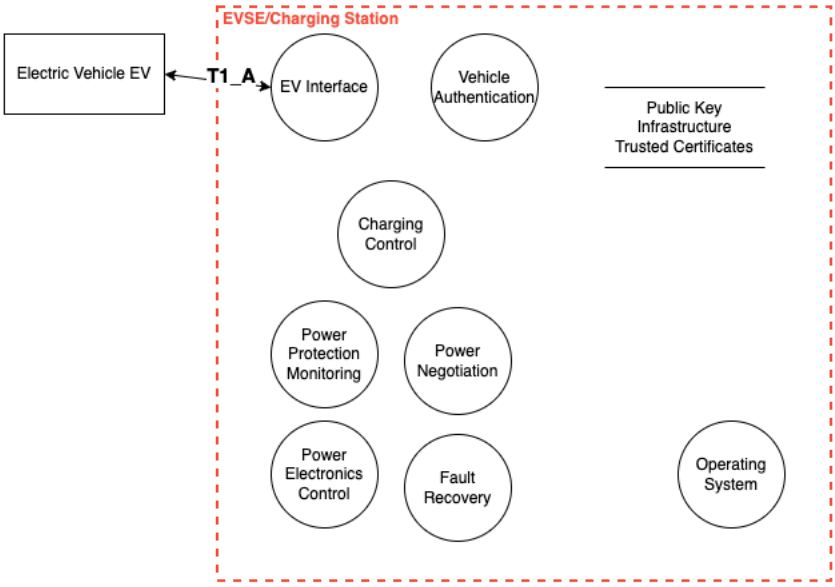

Figure 5. T1 diagram, EV to EVSE

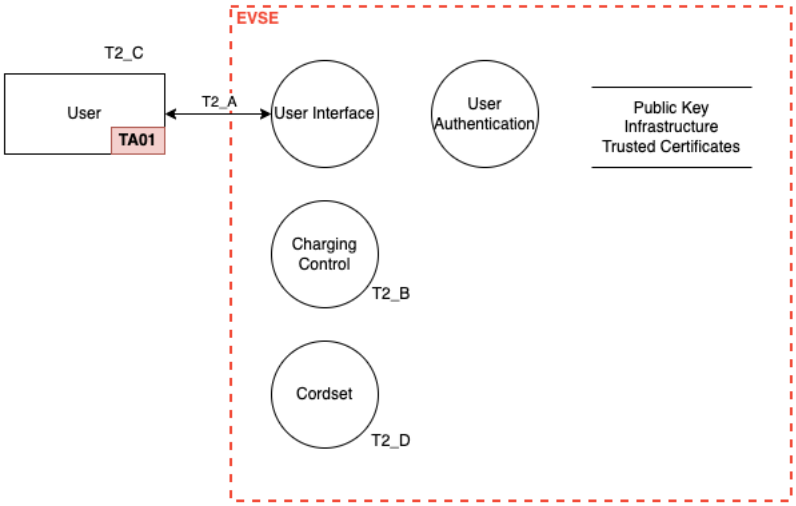

Figure 6. T2 diagram, EVSE to User

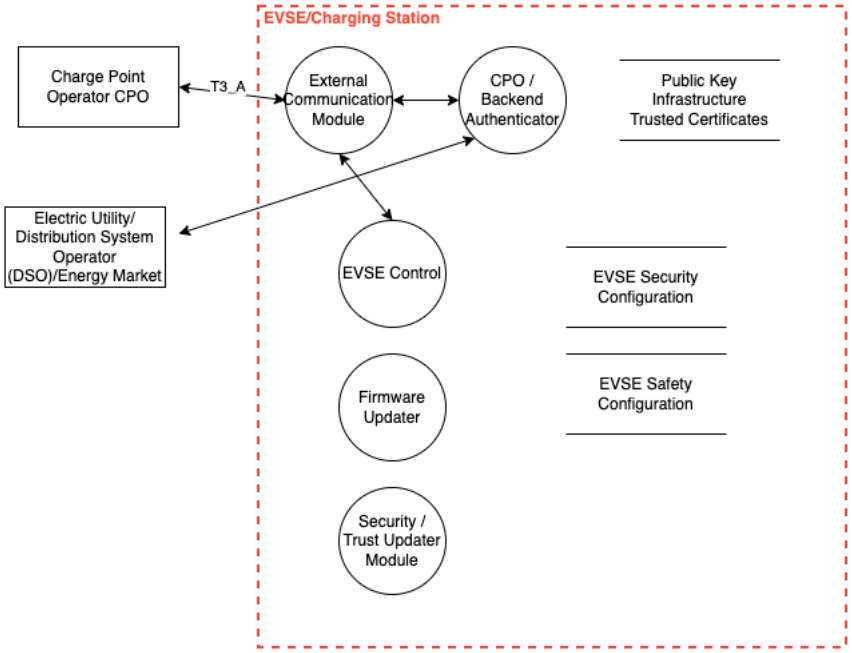

Figure 7. T3 diagram, EVSE to CPO

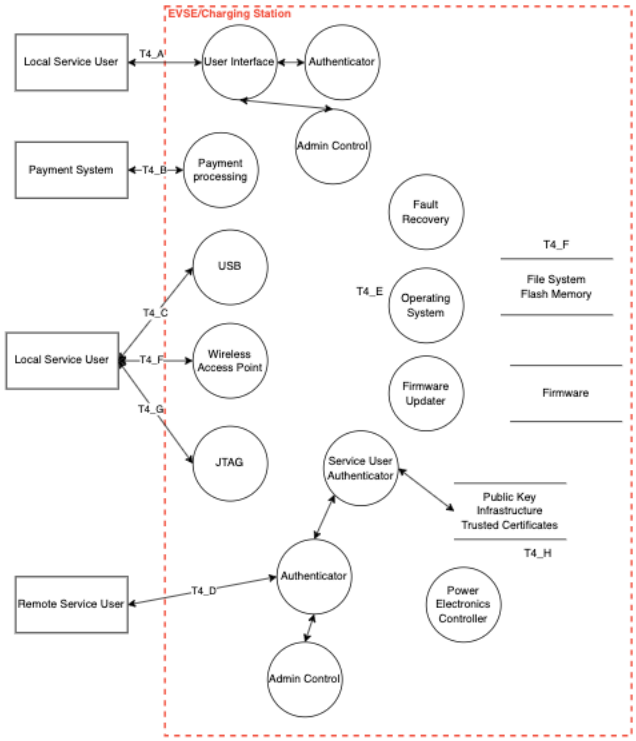

Figure 8. T4 diagram, standalone EVSE

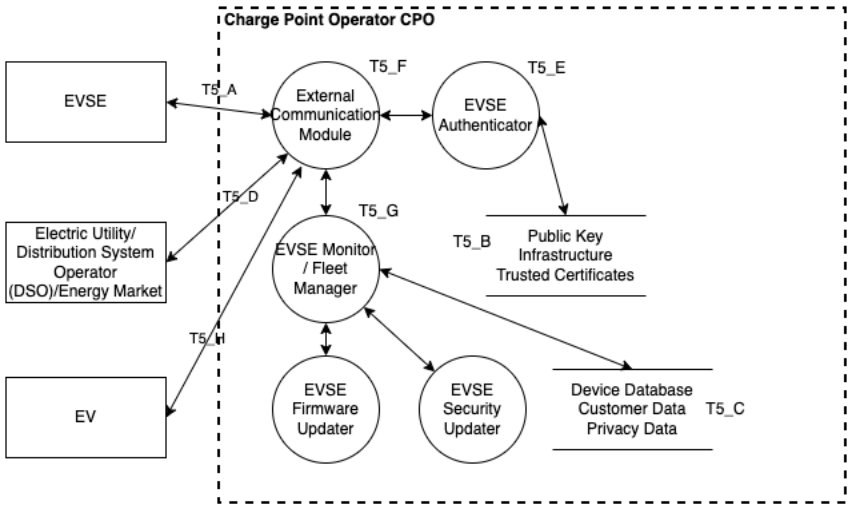

Figure 9. T5 diagram, CPO to EVSE

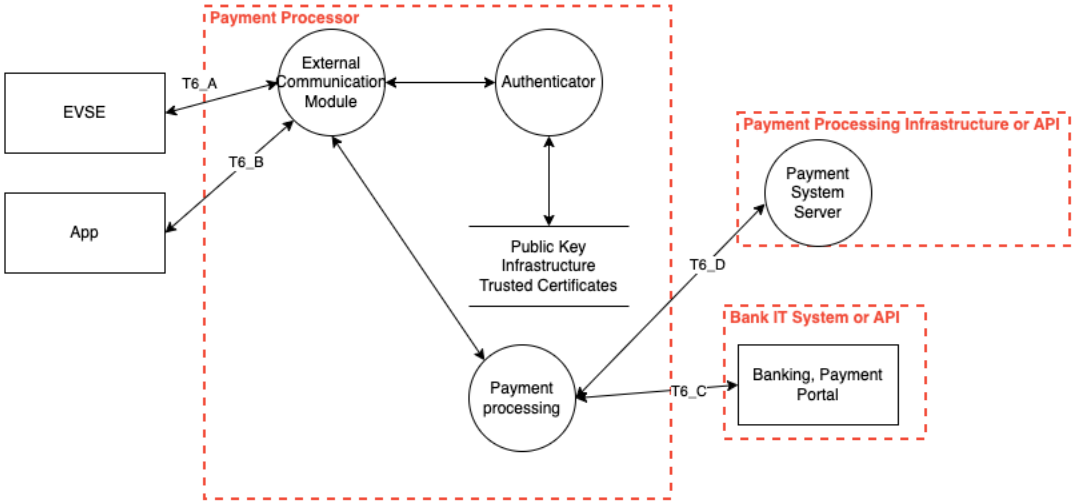

Figure 10. T6 diagram, EVSE to payment system

A.2. Charging Infrastructure Architecture Model

This high-level architecture model shows the entities involved in EV charging transactions. The threat modelling in this white paper was focused on the EVSE since it is the most vulnerable element in the infrastructure.

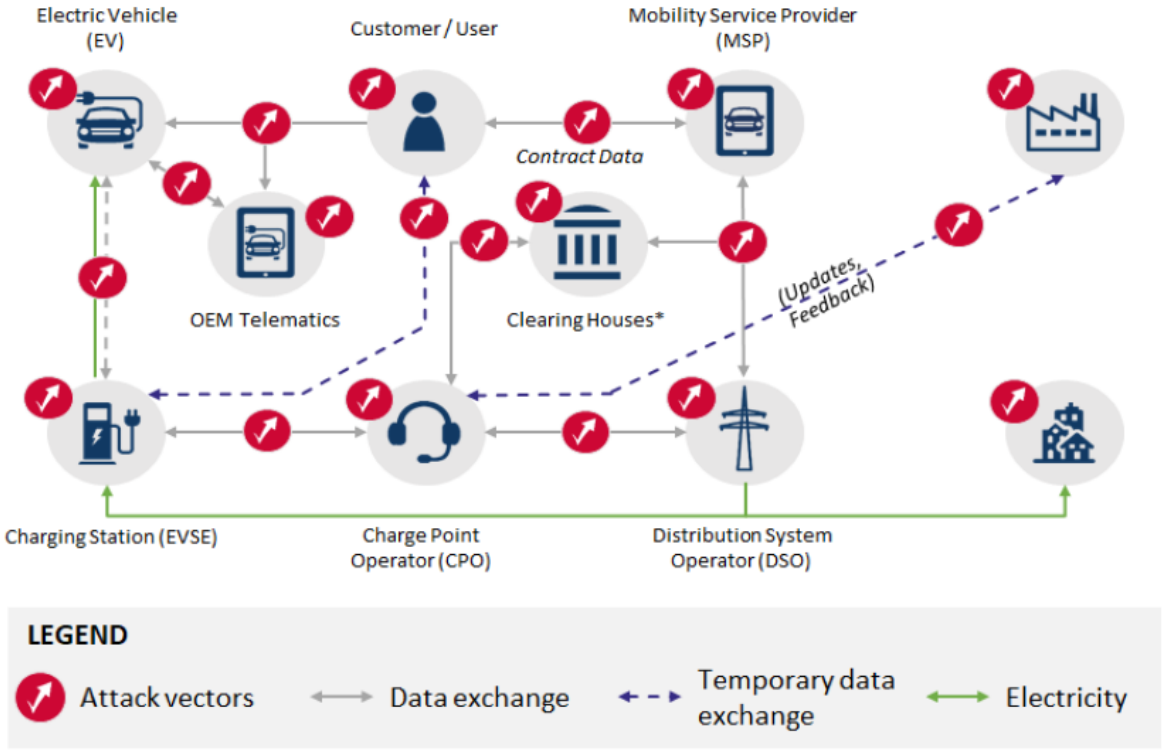

Figure 11. Charging Infrastructure with attack vectors

A.3. Complete Table of Threat Scenarios

Each scenario in this table includes the following information:

ID: Unique ID of the entry in the table.

Ref: A label that references the diagrams in Appendix A.1 showing approximately where the threat is located in the architecture.

Threat Scenario: This is a description of the beginning and conclusion of a threat. At minimum, these are a sentence that have an entity and a vulnerable element, component, or subsystem.

Threat: This column connects the threat scenario to STRIDE.

Attack Vector: The definition of each of these terms is from the CVSS v3.1 specification document[26]. Their definitions were applied to our model, so they served the authors for inspiration more than being applied literally. As this document uses the following terms:

- “Network” is a remote attack vector, typically across the internet or a geographically distant location, such as an operator cloud.
- "Adjacent” means the attack vector is bound to a network stack but the attack is limited to a logically adjacent network.
- “Local” attack vectors are local to the network. This is distinct from network and adjacent because those threat vectors have a router or gateway in-between attacker and vulnerable component.
- “Physical” attack vectors are defined as those requiring the malicious agent to physically touch the specific component.

Impact On: The stakeholder that could be impacted by a given threat scenario (see Section 4.2 for details):

- Generic: These did not fit in one of the other categories or were highly likely to impact more than one category.
- Grid & EV: These are threat scenarios to the grid and EV.
- Implementers & Operators: These are threat scenarios to implementers & operators, which includes CPOs and EVSEs.
- Payment & Billing: These are threat scenarios to the payment & billing stakeholders.

Vulnerability: Some characteristic that makes it possible for a threat to occur.

Mitigation: Security control, risk reduction.

HCE Severity score: See Table 1 in Section 5.2.

[26] https://www.first.org/cvss/v3.1/specification-document

ID	Ref	Threat Scenario	Threat	Attack vector	Impact on	Vulnerability	Mitigations	Comments	HCE Severity Score	Level of Impact	Magnitude	Duration	Recovery Effort	Safety	Costs	Effect Propagation Beyond EV or EVSE	EV Industry Confidence, Reputation Damage
A65	T4_D, T4_A	An attacker manipulates the wall clock (absolute time) of a device to allow expired credentials or signatures to become valid. The attack can be local by changing the configuration of a device, or intercepting the time update queries of a device, or global by controlling the time server	Tampering	Network	Implementers & Operators	Embedded devices usually do not have secure time circuits. RTC can be manipulated or disabled, or may not exist because the vendor saved the cost. Credentials expire so they do not need to be revoked, so expired credentials would not be discoverable in another way (e.g. OCSP/CRL). Certificates and signatures are all reliant on the device knowing the correct time and date. Expired credentials are not protected, and it is not considered a security breach if, e.g. laptops or devices with expired credentials are stolen or compromised.	Secure time circuits on the device. Device implements the secure version (only) of NTP. Use standard trusted NTP pools, not vendor-specific servers or untrusted servers. Fallback mechanism when time is not known, or has not been updated, rather than assume the default bootup start time is secure or safe to use. Expired credentials are more easily obtained by attackers, because they are usually not protected as well as active credentials. This means expired credentials can be stolen or bought more easily.		4.25	1	5	3	5	5	5	5	5
A102	T4	EVExchange: Given chargers C1 and C2, vehicles (A)ttacker and (V)ictim, the cordsets are tampered such that power flows from C1 to A, C2 to V, but communication from C1 is tied to V, C2 is tied to A. The victim then pays for the Attacker's power transfer.	Tampering	Physical	Payment & Billing	Assumption that power and communications terminate at the same charger	Regularly inspect charging facilities looking for signs of tampering. Incorporate tamper resistantance into facilities and equipment. Monitor customer accounts for atypical usage.	M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "EVExchange: A relay attack on electric vehicle charging system," in Computer Security–ESORICS 2022, ser. Lecture Notes inComputer Science, vol. 13554, 2022, pp. 488–508.	4.00	5	5	5	4	2	3	5	3
A34	T4_E	Payment system may include vulnerable third party libraries which may lead to inadvertant path to EVSE access	Repudiation	Network	Payment & Billing	Insufficient updating on processor system	Establish and maintain a regular patch window for processor software and dependencies		3.88	1	4	4	5	3	4	5	5
A9	T1_A	A large body of vehicles simulatenously abort charging, decreasing demand, causing voltage and frequency transients, thereby causing generator trip offs	Denial of Service	Network	Grid & EV	e.g., the attacker compromises OEM cloud	Perform Security assessments on all supply chain providers and components to promote end-to-end security and reliability and reduce supply chain risk	S. Acharya, Y. Dvorkin and R. Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?," in IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5099-5113, Nov. 2020, doi: 10.1109/TSG.2020.2994177. Carlson, B., Rohde, K., Crepeau, M., Salinas, S. et al., "Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure," SAE Technical Paper 2023-01-0047, 2023, https://doi.org/10.4271/2023-01-0047.	3.75	5	5	3	4	0	4	4	5
A101	T1_A, T2_D	An attacker modifies the cordset, allowing her to inject SDP responses with the security set to 0x10, "No transport layer security." A race condition occurs, the EV prefers the earlier over the later response from the charger. The EV then connects without employing TLS	Tampering	Adjacent	Grid & EV	TLS downgrade attack. In ISO 15118-2 a vehicle has option to connect to insecure charger.	At the charger, monitor for SDP responses that differ from the ones sourced by the charger. Once TLS becomes widely available, don't offer insecure connection.	M. Zhdanova, J. Urbansky, A. Hagemeier, D. Zelle, I. Herrmann, and D. H offner, "Local power grids at risk–an experi- mental and simulation-based analysis of attacks on vehicle-to-grid communication," in Proc. of the 38th Annual Computer Security Applications Conf, (ASAC), 2022, pp. 42–55. Requires physical access, not scalable, does not prevent charging services	3.63	2	5	5	4	2	3	5	3
A81	T4_F	An attacker gains access to a device and alters the log files to add events that never occurred, or modify existing events	Repudiation	Local	Implementers & Operators	Unprotected log files can be altered to hide malicious activity	Protect log files. Protect security events or security logs with stronger protections. Securely transfer logs to remote servers and ensure log services on the device are securely separated from user privileges or user space, so a compromised device cannot be made to stop logging or sending logs externally with evidence of compromises.		3.63	5	5	5	4	0	4	5	1
A79	T4_D, T4_A	An attacker gains access to a device by negotiating the connection to a less secure one, which has known vulnerabilities	Elevation of Privileges	Network	Generic (non-specific)	Downgrade attacks are a known problem, in which the attacker negotiates a cipher suite that has known vulnerabilities, or simply contains NULL ciphers.	Use the latest patched versions of crypto libraries. Ensure crypto libraries and TLS or other connectivity session contexts are configured to only allow known secure cipher suites, i.e. not null ciphers, or ciphers that have known vulnerabilities (MD5, SHA1, RC4, DES, anything with short keylengths, NULL, etc. etc. The graveyard of insecure ciphers keeps growing.) NIST and ENISA issue guidance on which ciphers and keylengths to use, depending on the expected lifetime of devices/secrets. These recommendations change over time, so vendors must be able to update cipher lists in deployed devices		3.63	5	5	3	3	0	5	3	5
A73	T4_E	A third-party vendor (inside attacker) decides to run unauthorised software on the devices	Tampering	Network	Implementers & Operators	Third-party libraries/apps/code may change unexpectedly. There are cases of third-parties deciding to 'update' their code to run bitmining or other CPU-heavy activities on devices, or implement 'telemetry' that sends device data back to their servers, often without proper privacy or encryption protection measures.	Examine changes to third-party libraries before updating them on devices. Be able to patch devices in a reasonable timeframe if a third-party library/app needs to be replaced, or is found to violate your security policies.		3.50	5	4	4	4	2	4	0	5
A12	T4_C01, T5_C	Attacker intercepts and manipulates OCPP traffic sent to and from the EVSE to gather customer or EVSE information. (most likely MITM scenario is from the local charging infra and within the backend infra. With prooper secure channels a MITM scenario shoult not exist.)	Information Disclosure	Network	Implementers & Operators	Authentication - OCPP 1.6J allows the use of TLS 1.0 and 1.1, which are officially deprecated	Use TLS v1.2 or OCPP 2.0.1 which requires TLS v1.2		3.50	3	5	5	3	2	3	5	2
A67	T4_A, T4_D, T4_C, T4_F	An attacker gains remote access to device due to credential stuffing, or weak credentials	Spoofing	Network	Implementers & Operators	Use of weak/guessable credentials, passwords, single factor authentication, reused credentials, etc. makes devices vulnerable to attacks	Use a proper PKI, certificates, asymmetric keys, signed messages, multi-factor authentication, etc. for device authentication access. Do not use passwords/shared secrets/symmetric keys/PSK/single-factor authentication/etc. for Machine to Machine communication. Do not reuse credentials, do not generate credentials based on serial number, MAC address, or other guessable sources. Separate remote access methods from local/service access methods, if local usability is a concern (i.e. don't implement password and PIN for remote access just because you need it for local access).		3.50	5	1	5	5	2	3	5	2
A63	T4_D	An attacker gains access to servers or channels that were thought to be secure, because the EVSE vendor ceases to exist.	Spoofing	Network	Generic (non-specific)	When a vendor ceases to operate, their domain name and other hardcoded endpoints can be resold to malicious actors. In principle, if someone buys their assets they will also take over the crypto keys and can issue signed updates	Malicious actors can purchase assets, including cryptographic keys from a bankrupt vendor. The architecture shall not assume that all participating companies in backend communication are benign or cannot be compromised. Trust shall be revokable when a company ceases to operate, or begins acting maliciously for any reason.		3.38	5	2	3	3	3	3	4	4
A60	T4_A	An attacker exploits remote side-channel attacks against an EVSE/EV/App to gain privileged access or copy credentials (timing attacks, oracle attacks, etc.)	Information Disclosure	Network	Implementers & Operators	Cryptographic algorithms in common use are vulnerable to timing attacks unless whitening functions are applied	Use secure and tested crypto libraries with whitening functions		3.38	5	3	3	3	3	3	4	3
A40	T5_F	MSP adds insecure extensions to OCPP 2.0.1 allowing root access	Elevation of Privileges	Network	Implementers & Operators	Insecure coding practices	Better developer training or testing		3.38	5	3	5	3	0	3	5	3
A21	T4_A	An attacker reverse engineers Hardcoded Payment identifiers for free charging	Spoofing	Adjacent	Payment & Billing	Hardcoded credentials	Make the payment identifiers more fluid, change them for every transaction or after a set amount of time.	Duplicate of A14? Not a duplicate. A14 is a single person abusing hardcoded credentials, A21 represents someone who reverse engineered the credentials. The word "leaks" was removed.	3.38	5	3	5	3	0	3	5	3
A82	T4_F	An attacker gains access to a device and alters the log files because they are not protected, or do not require elevated privileges to access	Tampering	Local	Implementers & Operators	Unprotected log files can be altered to hide malicious activity	Protect log files. Protect security events or security logs with stronger protections. Securely transfer logs to remote servers and ensure log services on the device are securely separated from user privileges or user space, so a compromised device cannot be made to stop logging or sending logs externally with evidence of compromises.		3.38	5	3	5	3	0	3	5	3
A95	T5_D	Attacker tampers with the Aggregator-Utility capacity forecasts	Tampering	Network	Grid & EV	Aggregator misrepresents capacity or vehicles available for bidirectional power transfer	Human monitoring and machine monitoring and checking historical data. e.g. a human asks "does this capacity forecast look correct? Or a machine asks the same question "Is this capacity forecast within 5 percent of what I expect? If not, then flag for human review")		3.38	4	3	5	3	2	3	5	2
A47	T1_A	An attacker circumvents AuthN/AuthZ mechanisms by performing debug attacks during power cycle	Elevation of Privileges	Physical	Implementers & Operators	Active unprotected debug routine that can by triggered on powercyce	Disable debug routine for devices in the field		3.38	3	5	5	4	0	4	5	1
A38	T4_C, T4_G, T4_F, T4_D, T4_A	An attacker gains access to a charger and installs malware on it that will install malware on EVs that charge using that charger	Tampering	Network	Grid & EV	Malware is introduced to the EVSE via some attack. The malware can spread to the EV via the communication channel when the EV connects to charge.	Monitor EVSEs for malware. Monitor EVs for malware. Penetration testing on the communication stacks in both EVSE and EV; malware is likely to spread via a buffer overflow or vulnerability in the stack implementations, more than via a legitimate data transfer. Keep communication stacks up to date, ensure vulnerabilities are found, patched, and distributed to all EVSEs and EVs.		3.25	3	1	5	5	2	3	5	2
A44	T4_D	An attacker gains access to the unsecured EVSE network infrastructure via the Internet	Tampering	Network	Implementers & Operators	Missing Network Segmentation, exposure of critical components on the internet	Network segmentation, VPN, Zero Trust Design approach		3.25	5	5	5	3	0	2	5	1
A32	T4_B	Attacker leverages EVSE to modify payment processing execution flow or data path	Tampering	Adjacent	Payment & Billing	If payment processor resides on EVSE hardware/software attacker leverages EVSE control to affect processor functionality	Test manipulation of interactions between these entities for trust based attacks	How is this different from A18? (more detail needed)	3.13	5	3	3	3	0	4	3	4
A23	T5_D	An actor compromises DSO via phishing -> escalation of privilege to admin to limit CSMS load, impeding charging	Spoofing	Network	Grid & EV	People or unnecessarily exposed email address	Better training/non-guessable email addresses		3.13	5	1	5	3	2	3	5	1
A75	Ecosystem	A vendor (inside attacker) creates patents or other vendor-locked implementations of parts of the system architecture to remove free competition	Tampering	Network	Generic (non-specific)	Maximising the cost of switching to competitors is an objective for vendors. These implementations live in the margins of standards, or where standards are ambiguous, or the parts they do not attempt to specify	Ensure that open standards are made available which are comprehensive enough to prevent anti-competitive behaviour. Ensure that there is a compliance/test program that vendors must adhere to.		3.13	5	1	5	3	2	3	5	1
A55	T5_A, T6_A	An attacker connects to the network using copied client credentials and impersonates the client (EV, EVSE, App, etc.)	Spoofing	Network	Implementers & Operators	Usage of user credentials that are easily duplicated, e.g. passwords or symmetric keys, give attackers privileged access that is effectively genuine and very difficult to block or detect without additional context	Use credential types that are difficult to duplicate, e.g. asymmtric keys, zero knowledge and challenge protocols, and use multi-factor authentication that are not all stored/originating from the same device		3.13	4	3	5	3	2	2	5	1
A25	T5_D	CSMS transmits false data to DSO to cause unnecessary islanding event	Spoofing	Network	Grid & EV	Insufficient authentication of data source	The utility can possibly check other loads or use out of band measurements.	CSMS is the same as CPO	3.13	4	4	2	1	3	4	5	2
A49	T4_C, T4_G	An attacker use diagnostic port access to alter power electronics firing angle, thereby reducing power factor correction	Tampering	Physical	Grid & EV	Exposed diagnostic port allows access to low-level power electronics configurations	Do not expose diagnostic port. Do not have hardcoded maintenance passwords/backdoors. Two-factor authentication on diagnostics access	Assumption: physical access Method: exposed or easily revealed diagnostic port (USB, RS-232, SSH, etc)	3.13	1	5	3	5	0	4	3	4
A33	T4_A	Payment interface requires maintenance EVSE user account creation with weak password/credentials	Elevation of Privileges	Network	Payment & Billing	Poor business/IT practices	Do not rely on custodial accounts with easy to guess or hard coded passwords		3.13	1	3	3	4	2	3	4	5
A41	T5_B	An attacker persistently DDoSes OCSP responders, keeping CSMSs from obtaining up-to-date Certificate Status responses	Denial of Service	Network	Implementers & Operators	OCSP responders are a bottleneck, often a DDoS	CAs need to scale out the OCSP responders; Operators need to build out infrastructure to improving response caching	OCSP responders are operated by CAs as part of their responsibilities. In Webpki, inability to contact OCSP responders is treated as fail open, that is, assume that verification success.	3.00	3	3	3	3	3	3	4	2

A91	T5_E	Attacker uses EVSE to bridge into station operator network	Tampering	Local	Implementers & Operators	Operators trusting the network	Apply zero trust network architectures. Continuous authentication and authorization to tailor access to EVSE behaviors		3.00	2	3	5	3	0	3	5	3
A68	T4_D, T5_A, T6_A, T6_B	An attacker alters data in transit through a proxy (MitM attack) because the data is not encrypted end to end	Tampering	Network	Implementers & Operators	"Secure link-based systems", i.e. systems that are based on authentication (and optional encryption) between each link in the network are inherently insecure if a single link can be compromised, and there is no way to detect this at the endpoints. Such systems are common in the world of embedded devices, with concepts such as brokers/aggregators/proxies, and symmetric link-encryption. Ideally, the sender of a message knows the cryptographic identity of the receiver, and can dedicate the message to the receiver (mutual authentication), or at least the sender can sign the message to prove its origins, and the receiver is expecting the message, and can check for freshness.	Use PKI and identities to authenticate messages. Use challenge-response protocols to ensure freshness of messages, and prevent replay attacks. Do not use systems where proxies are able to recover a message payload and repackage it, effectively removing the proof of origin. The endpoint that consumes the payload must be the same endpoint that the message is dedicated to.		3.00	5	3	3	3	2	2	3	3
A72	T5_C	An attacker compromises privacy or sensitive data by compromising the cloud hosting provider of the vendor or operator	Information Disclosure	Network	Generic (non-specific)	Vendors may choose to outsource their cloud infrastructure, meaning they do not own the endpoints that their devices communicate with. Cloud providers can be coerced, or simply not compliant with security policies. Secure breaches in cloud hosting solutions are also frequently due to misconfigurations, or bad default permissions on access. Private data require special attention and is under regulation.	Self-hosting of critical infrastructure for privacy and sensitive data. Proper security policies for data processing and storage. Only outsource of less critical data collection functions. Only use cloud providers that are security and privacy compliant and regulated. Do not host services in countries that may have an interest in disabling the charging infrastructure in the countries you operate in.		3.00	5	1	5	3	2	2	5	1
A24	T5_C	EVSE transactions lose non-repudiation via CSMS compromise, enabling an actor to provide free electricity at one or many EVSEs	Repudiation	Network	Grid & EV	CSMS	CSMS protections (MFA, monitoring, RBAC)		3.00	5	1	5	3	2	2	5	1
A52	T2_C	An attacker forges payment proof to EVSE from EV/App connection	Spoofing	Local	Payment & Billing	When the EVSE is not part of the payment transaction, but receives a proof of payment from the user, that proof can be forged or replayed	Payment proofs must contain fresh data to prevent replay attacks, e.g. timestamps or a backend server response to a challenge issued by the EVSE as part of the transaction.		3.00	4	3	3	3	0	3	4	4
A83	T4_A, T4_B, T4_C, T4_D	An attacker gains access to a device because third-party code has known vulnerabilities, but no patch is available	Tampering	Network	Implementers & Operators	Third-party code either has a zero-day vulnerability, or a vulnerability has been disclosed, which has not been patched.	The third-party code can be disabled or replaced with a similar functionality.		2.88	5	1	5	3	2	3	1	3
A56	T4_C	An attacker gains privileged access to EVSE via physical connection (JTAG, HMI, USB, local wireless, serial, etc.) to disable it	Denial of Service	Physical	Implementers & Operators	Local interfaces are not secured and provide elevated privileges (either by default, or trivially achievable)	Disable debug interfaces during manufacturing (JTAG, etc.). Secure all open interfaces and require authenticated multi-factor access. Protect critical functions such as configurations and power states.		2.88	1	1	5	5	2	3	5	1
A18	T4_E	An attacker compromises EVSE vendor to disable EVSE operator's charging network (based on Moscow)	Denial of Service	Network	Implementers & Operators	EVSE Vendor had backdoor access to EVSEs they sold	Operator should check for and remove backdoor access.	https://www.mdpi.com/1996-1073/15/11/3931	2.88	4	1	5	3	2	2	5	1
A89	T4_D, T4_E	An attacker manipulates the wall clock, causing EVSE to misapply charging profile, incurring demand costs	Elevation of Privileges	Network	Implementers & Operators	EVSEs local time is synchronized from network sources. If network sources are susceptible to interference, time-based functions may be triggered to run	Use standard trusted NTP pools, not vendor-specific servers or untrusted servers. Use fallback mechanism when time is not known, or has not been updated, rather than assume. Consider multiple sources, including local GPS clock and cellular time		2.88	2	3	5	3	2	2	5	1
A20	T5_F	An attacker launches a DoS attack on a utility to prevent EVSE communication to CNO	Denial of Service	Network	Grid & EV	Publicly accessible web server/Shared resources between EVSE comms and IT infrastructure	DoS protection service/Separate network resources	Utility is EVSE operator or OCPP server	2.88	3	3	5	4	0	3	1	4
A94	T3_A	Electric utility leaks EV location and other metadata because of overly aggressive data logging	Information Disclosure	Network	Grid & EV	Aggregator or CPO logs transaction information about location and payment that can violate users' privacy. The logs are kept for longer than required since no data retention policy is defined.	Aggregrator should be selective in what data they store, for what purpose, and for how long.		2.75	3	3	3	4	1	2	4	2
A26	T4_B	1	Elevation of Privileges	Physical	Payment & Billing	Payment interface contains software or hardware vulnerabilities that allow for unintended control flow	Harden processor against known vulnerabilities and establish regular maintenance/update cadence		2.75	5	3	5	3	2	1	1	2
A100	T5_D	An attacker injects false data into energy markets to grid imbalance, increased energy cost or significantly reduced energy costs	Spoofing	Network	Grid & EV	If the attacker can spoof or tamper with forecasts, utilities will erroneously commit and dispatch the generators and schedule the demand	Monitoring, anomaly detection, comparison of predicted costs.	https://www.sciencedirect.com/science/article/pii/S2666792422000166#bib0021	2.75	5	3	5	3	2	1	1	2
A70	T4_D	An attacker disables a device by making failed login attempts	Denial of Service	Network	Implementers & Operators	Devices that disable accounts after 3 retries, or that use an exponential login rate-limiter that has no upper bound, can be used to deny services to legitimate users, without the attacker presenting a trusted credentials.	Repeated failed logins shall not disable accounts. Rate-limiting login shall have an upper bound (and not just exponentially add longer and longer times between logins). Repeated failed logins should be monitored and logged. Failed logins may also trigger an additional mandatory multi-factor or additional security measures, since the device/account is clearly under active exploitation.		2.75	3	3	3	3	3	2	3	2
A84	T4_A, T4_B, T4_C, T4_D	An attacker gains access to a device due to poor code quality that allow basic methods of compromise	Tampering	Local	Implementers & Operators	Use of home-grown code for critical security functions. Lack of rigorous security testing. Lack of regular testing. Lack of static/dynamic code analysis.	Use static code analysis. Use standard test methods for common known vulnerabilities, e.g. OWASP, MITRE, CVE. Use standard libraries for critical and security functions, keep them patched and up to date. Test every code release. Use an approved and comprehensive test plan that is updated as the threat landscape changes.		2.75	5	2	5	3	0	3	3	1
A30	T4_B, T4_A	Attacker glitches payment interface	Elevation of Privileges	Physical	Payment & Billing	Hardware device used to bypass payment processor functionality	Incorporate glitching attacks in hardware testing		2.75	1	1	5	3	2	3	5	2
A85	T6_A, T6_B, T6_C	Attacker gains access to the payment processing cloud platform	Repudiation	Network	Payment & Billing	Inherent trust in payment processing network	This risk may need to be accepted		2.75	5	2	5	3	0	1	5	1
A11	T4_C01	Attacker intercepts and manipulates OCPP traffic sent to and from the EVSE to impersonate OCPP server. (most likely MITM scenario is from the local charging infra and within the backend infra. With prooper secure channels a MITM scenario shoult not exist.)	Spoofing	Network	Implementers & Operators	Authentication - OCPP 1.6J allows the use of TLS 1.0 and 1.1, which are officially deprecated	Use TLS v1.2 or OCPP 2.0.1 which requires TLS v1.2		2.75	3	1	5	3	2	2	5	1
A76	T4_D, T4_A	An attacker gains privileged access to a device by using a copy of a software administration tool. Either via a local or remote connection	Elevation of Privileges	Network	Implementers & Operators	If devices are not able to verify the identity and authorisation of a connection or a tool, anyone with a copy of the tool is able to connect to the device	Administration/service software tools that connect to the device must use a secure session, and must present verifiable credentials to the device before elevation of privilege.		2.75	3	1	5	3	2	2	5	1
A28	T4_A	Attacker leverages EVSE to interface with payment processing network	Tampering	Adjacent	Payment & Billing	Trust boundary may allow for implicitly trusted interactions between EVSE and payment processor	Test manipulation of interactions between these entities for trust based attacks		2.63	5	2	3	3	2	2	3	1
A46	T4_D	An attacker gains privileged access via unsecure exposed API endpoints	Elevation of Privileges	Network	Implementers & Operators	Missing proper authorization mechanisms and checks	Implement automatic authorization testing in developer pipeline		2.63	5	1	5	3	0	1	5	1
A66	T4_E	An attacker alters a device configuration or installs malware, and this action is not detected	Tampering	Local	Implementers & Operators	Devices are not regularly scanned for malware or misconfigurations, so even trivial attacks are never detected (every attack becomes 'stealthy' if no one ever checks if a device has been compromised)	Regular scan/update of devices, online check of configurations. Routine hardware factory reset and re-update to flush out persistent stealthy malware, and ensure no malware is present in memory, and the device is executing unaltered software (could be part of physical maintenance cycle). Routine hardware reboot/reset of the device (coordinated to minimise loss of service at a location). Malware detection or scanning capabilities on the device, maybe a thin hypervisor that sends back regular reports, and a larger data aggregation/monitoring would be able to detect anomalies.		2.63	2	1	5	3	2	2	5	1
A43	T4_B, T4_A	An attacker applies glitching attacks to circumvent authentication of the EVSE (dismantling needed)	Tampering	Physical	Implementers & Operators	Missing checks on microcontroller to detect and prevent glitchting	Enable microcontroller glitching prevention		2.63	2	1	5	3	2	2	5	1
A57	T4_E	An EVSE is unable to recover from an attempted attack or failure/error, and must be serviced physically to recover	Denial of Service	Local	Implementers & Operators	Devices do not protect their configurations and cannot recover from misconfigurations and failures (intended or not). Device cannot recover gracefully from attempted attacks, e.g. packet flooding, after the attack stops.	Watchdog timers, reflash of Golden Image (rollback image), detection of error modes and recovery. Devices shall recover from network attack attempts when they stop. Devices shall detect failures/errors and enter failure states, e.g. a threshold counter for failed transactions. If users have attempted to use the device and the operation has failed several times, the device shall assume it is at fault, and enter a recovery sequence. Devices shall detect and automatically engage restarts/reboots to recover from trivial errors. A service technician shall only be required to physically recover the device from unforeseen and disastrous failures, not from trivial errors.		2.63	1	1	5	5	0	3	5	1
A27	T4_B	Payment information is intercepted and modified	Tampering	Local	Payment & Billing	Payment information is transferred in a format that can be intercepted by an attacker and resent	Ensure data is encrypted in transit		2.38	5	2	5	3	0	1	2	1
A90	Ecosystem	The hardware root of trust expires	Denial of Service	Local	Generic (non-specific)	Manufacturer's root certificate expires, either because of lapse or forced by advancing time. Firmware updates can then not be applied	Implement secure mechanism for root replacement. Use standard trusted NTP pools, not vendor-specific servers or untrusted servers. Use fallback mechanism when time is not known, or has not been updated, rather than assume. Consider multiple sources, including local GPS clock and cellular time.		2.38	5	3	2	2	2	2	2	1
A59	T5_G	An attacker sets up a fake EVSE/CPO/EVSE Provider company or just a fake server to participate in a legitimate network. The attacker can receive connections from legitimate devices/vehicles/systems, which they can compromise or manipulate (MitM) or send back malicious data.	Spoofing	Network	Generic (non-specific)	Backend infrastructure is vulnerable to insider attacks if authentication is equated with authorisation. Attackers setting up a seemingly legitimate company and connecting to the a backend network can gain access to sensitive data, or send malicious data to other participants.	Backend infrastructure shall be clear on the data being exchanged, ensuring private information, payment data, and other sensitive data is not leaked to other participants. Backend infrastructure shall sanitise and verify data coming from other nodes. Especially scripts or executable code being transferred via APIs can be malicious. The architecture shall not assume that backend communication and all participating companies are benign		2.38	5	1	5	3	2	1	1	1
A71	T4_D	An attacker compromises a device by compromising the cloud hosting provider of the vendor or operator	Spoofing	Network	Implementers & Operators	Vendors may choose to outsource their cloud infrastructure, meaning they do not own the endpoints that their devices communicate with. Cloud providers can be coerced, or simply not compliant with security policies. Secure breaches in cloud hosting solutions are also frequently due to misconfigurations, or bad default permissions on access.	Self-hosting of critical endpoints for devices, e.g. firmware or configuration updates, and only outsourcing of less critical data collection functions. Only use cloud providers that are security compliant and regulated. Do not host services in countries that may have an interest in disabling the charging infrastructure in the countries you operate in.		2.38	5	1	3	3	0	1	5	1
A92	T4_A, T4_E	Attacker uses management terminal to configure different HMI landing site	Tampering	Physical	Implementers & Operators	Lack of integrity checks against known good configurations	Employ verification or domain restrictions within explicit allow lists		2.38	1	1	5	3	0	3	5	1
A8	T1_A, T5_D	An attacker gains access to CSMS and broadcasts a RemoteTransactionStop, causing over voltage transients on distribution network	Tampering	Network	Grid & EV	Trust is implied between charger and the CSMS, but CSMS autheticates users. Charging Station Operator and Network Charger Provider may not be the same organizzation.	Stochastically delay grid impacting delays. See UK "Regulations: electric vehicle smart charge points"	We assume the hardware protections fail (that is, the RemoteTransactionStop has emergency priority)	2.38	5	1	5	3	2	1	1	1
A80	T4_F, T4_E	An attacker gains access to a device and alters the log files to hide that the device was compromised	Tampering	Local	Implementers & Operators	Unprotected log files can be altered to hide malicious activity. Forensic investigations are difficult to do on compromised devices that do not show an accurate sequence of events	Protect log files. Protect security events or security logs with stronger protections. Securely transfer logs to remote servers and ensure log services on the device are securely separated from user privileges or user space, so a compromised device cannot be made to stop logging or sending logs externally with evidence of compromises.		2.38	5	1	5	3	2	1	1	1
A1	T4_D	An attacker uses default credentials on a management console exposed on the internet to gain admin access	Elevation of Privileges	Network	Generic (non-specific)	Remote Management Interaface exposed to the internet; Default usernames + password	Opt 1. Change to device individual credentials upon deployment or Opt 2. connect the system to a central authentication system, and disable default accounts	Discussed on session April 18th	2.38	2	3	3	3	0	5	0	3
A2	T4_E	An attacker abuses a compromised EVSE to spread malicous code onto the vehicle while charging for later malicious actions	Tampering	Adjacent	Grid & EV	Improper parsing on vehicle's charging controller	Hardening parsing implementation (Fuzzing, Code Reviews, Pentest)	possible motivation: to permanently disrupt charging capabilities (of a certain fleet)	2.25	5	2	3	3	0	1	2	2
A69	T4_D, T4_H	An attacker gains control of an online Certificate Authority and is able to sign software that a device trusts	Tampering	Network	Generic (non-specific)	Browsers contain hundreds of trusted CAs of varying degrees of credibility. CAs can be compromised and their keys used to sign malware. If the device does not have a limited list of trusted CAs, and a separation of trusted identity and authority, then any public CA can sign software and the device will assume it is good.	Browsers revoke CAs by issuing a software update (OCSP/CRL are useless because they cannot revoke a root certificate, a revocation list is signed by the root). Devices shall only contain a list of trusted CAs that are relevant to its PKI, and not the entire Internet PKI that browsers contain. Devices shall also separate the concept of trusted identity and authority. When a software package (or configuration update, or any type of data) is received, the device must both check that the identity of the sender is trusted AND that the sender is allowed to sign this type of data.		2.25	5	2	3	2	0	3	1	2

A99	T1_A	An attacker tampers with PCC meter reading communications, reducing perceived power consumption, causing the EVCF to exceed transfomer capacity, hit with demand charges, etc.	Tampering	Adjacent	Implementers & Operators	Metering data alterations are undetectable	Digitally sign and verify meter data; implement secure communications		2.25	4	0	0	4	0	3	5	2
A31	T4_E, T4_B	Payment interface leaks metadata	Information Disclosure	Adjacent	Payment & Billing	Insecure transfer of information from payment processor including not encrypting useful metadata	Ensure pertinent details are encrypted in transit		2.25	5	2	2	2	1	2	3	1
A14	T4_A	An attacker employs hardcoded Payment identifiers (i.e., for debugging or testing) to enable free charging	Spoofing		Payment & Billing	Failure of authentication/Easily guessable RFID	Monitor access patterns for hardcode IDs;		2.13	5	1	5	2	0	2	1	1
A58	T4_D	An attacker discovers EVSEs connected to the Internet (via Shodan, Censys, etc.) and stages remote attacks	Information Disclosure	Network	Implementers & Operators	Devices are either misconfigured, or default configuration is not intended for connection to the Internet. Device runs open ports and services that are not secure on the Internet	Devices are on a secure VPN and are not exposed to the Internet. Devices are not discoverable on the Internet		2.13	5	2	2	3	0	2	2	1
A10	T4_E, T4_C, T4_F, T4_G	Botnet/stealth takeover via physical access, or remote. Dormant malware waits for trigger event to disrupt EVSE.	Tampering	Physical	Implementers & Operators	Malware is introduced to the EVSE, either via remote attack or physical where attacker drives along the main motorways and stops at every service station to infect the charging stations there. The malware is stealthy and lies dormant until a trigger event (command signal, date and time, etc.). The EVSEs are disrupted, e.g. by denying service or damaging internal components that require physical servicing/replacement. Such an attack can render vital transport roads useless for days.	Malware/intrusion detection on EVSE. Monitoring of physical access ports and central alerting/logging. Regular reboot of EVSE devices to remove memory resident malware. Regular wipe and reinstall of OS and applications on EVSE devices, to remove storage persistent malware.		2.13	5	1	5	2	0	2	1	1
A19	T3_A	INL HCE - An unattenative operator performs RemoteStopTransaction on number of chargers, causing overvolt or undervolt event	Denial of Service	Network	Grid & EV	A command safe for individual chargers become problematic when synchronized to a set of chargers	EVSEs implement stochastic delays for performing commands that may impact grid health. CSMS should have safeguards to limit the dispatch of said commands	https://www.gov.uk/guidance/regulations-electric-vehicle-smart-charge-points	2.13	4	1	5	3	0	2	1	1
A74	Ecosystem	A vendor (inside attacker) creates proprietary data formats, closed protocols, or other undocumented features/extensions to the standards to monopolise parts of the system architecture	Tampering	Network	Generic (non-specific)	Proprietary data formats, closed protocols, vendor-specific extensions, and other attempts to undermine standards are created by vendors to achieve vendor lock-in on a platform, or parts of a system. This creates artificial costs of change, which maintains their position and kills innovation and progress. Anticompetitive behaviour is usually only dealt with when regulators step in, at which point much of the damage has already been done.	Enforce the use of open standards, open protocols, open formats. This provides a level playing field for all participants, and ensures that change and competition are favoured.		2.13	5	1	5	3	0	1	1	1
A87	T4_B	EVSE uses online repository/service matching spoofable identifiers to payment methods	Spoofing	Local	Payment & Billing	Unique identifiers used for payment are easily identifiable and spoofable	Ensure identification method meets NIST identity assurance standards		2.13	2	1	5	3	0	1	5	0
A50	T4	An attacker physically damages the EVSE. Theft of cables/copper, vandalism, damage to grid connection/transformer (disables the cluster of nearby charging stations)	Denial of Service	Local	Implementers & Operators	Physical attacks against the hardware and power electronics on site. Theft is a motivation when there are high-power cables with copper. Vandalism can be done against physical parts.	Implement theft deterrents: cables are marked so it is difficult to sell them. Physical protection: cables and valuable parts are not easy to dismantle. Power electronics are protected from physical attack, locked boxes. Physical area security: well-lit, open spaces, easy to see at a distance. Fenced or underground transformers and grid connectivity.		2.13	2	1	5	3	2	2	1	1
A77	T4_D, T4_A	An attacker gains privileged access to a device by impersonating a software administration tool. Either via a local or remote connection	Spoofing	Network	Implementers & Operators	If devices are not able to verify the identity and authorisation of a connection or a tool, anyone impersonating the tool can gain access, e.g. by reverse-engineering the protocol, or sending magic numbers	Administration/service software tools that connect to the device must use a secure session, and must present verifiable credentials to the device before elevation of privilege. The use of a certain protocol, or making a connection with a certain software tool is not a proper authorisation method.		2.00	5	1	5	2	0	0	0	3
A13	T4_B6	An attacker swaps vehicle ECUs so that the power transfer is billed to someone else	Spoofing	Physical	Payment & Billing	Tokens are insecurely stored or storage is readily defeated	Associate ECU token with other vehicle unique properties		2.00	1	1	5	3	0	1	3	2
A4	T4_C, T4_F, T4_G	An attackers gains access to the EVSE and extracts confidential data	Information Disclosure	Adjacent	Grid & EV	Insecure Diagnostic Port, Default Diagnostic Password	Unique Diagnostic Password	e.g. Payment information is stolen by an actor connecting to a physical diagnostic interface, and using an exploit(default credentials) to become root	2.00	3	0	3	5	2	2	1	0
A6	T1_A	An attacker physically accesses the EVSE to tamper with the EVSE power electronics protocol (PEP) (e.g.,CANT module or ARP spooing) to cause (e.g.) overvoltage to vehicle (damaging to EV), heated cable (harm to user), power module load balancing (harm to distribution network)	Tampering	Physical	Generic (non-specific)	A typical charging station decouples the system board from the power electronics. A simple protocol is then employed for the system board to command the power electronics module	(1) Monitoring of internal networks, (2) authenticate internal communications	Labeled generic since damage can occur in multiple places (EV, driver, grid)	2.00	1	2	2	2	4	2	2	1
A61	T4_E	An attacker exploits a known vulnerability in the EVSE/EV/App that has been fixed, but the patch has not been applied to the device	Tampering	Network	Implementers & Operators	Lack of patch management or remote patch capability, lack of patch tracking of which devices are running which versions of firmware, lack of tracking to discover that a patch has been released for a critical issue	Use proper patch management (ISO 27000 series), devices that are accessible remotely must also be patchable remotely. Software BOM and live version tracking on all devices. Tracking of version updates on everything on the Software BOM		1.88	5	1	5	1	0	1	1	1
A53	T4_C, T4_F, T4_G	An attacker gains privileged access to EVSE via physical connection (JTAG, HMI, USB, local wireless, serial, etc.) to upload malware or alter configuration of trusted servers, DNS, CAs, firmware, bootloader, files, memory, etc.	Tampering	Physical	Implementers & Operators	Local interfaces are not secured and provide elevated privileges (either by default, or trivially achievable)	Disable debug interfaces during manufacturing (JTAG, etc.). Secure all open interfaces and require authenticated multi-factor access. Protect critical configuration files on the device, do not allow direct access to file systems. Require signed updates to all files (firmware, bootloader, configurations).		1.88	1	1	5	3	2	1	1	1
A15	T4_A03	An attacker enters the EVSEs cabinet, MITM/port steal/... communication between system controller and meter (websockets or MQTT), and increases/decreases meter readings	Tampering	Local		Inadaquate EVSE-meter communication integrity	Employ a cryptographic communications protocol or enable cryptographically signed metering receipts		1.88	4	1	5	3	0	1	1	0
A29	T4_B	Attacker spoofs payment card processor	Spoofing	Adjacent	Payment & Billing	Attacker creates a malicious entity to hijack and respond to payment requests	Ensure proper authentication/authorization of payment system through PKI or similar functionality		1.88	3	1	3	2	2	2	1	1
A13	T4_A, T4_B	An attacker clones RFID token so that power transfer is billed to someone else	Spoofing	Adjacent	Payment & Billing	Failure of authentication/Easily guessable RFID	Monitor access patterns; Implement secure payment scheme, such as EMV, NFC, etc.	Discussed on May 2, 2023	1.88	1	3	3	3	0	3	0	2
A93	T5_F	Attacker takes over a charging network due to DNS expiration	Tampering	Network	Implementers & Operators	Operators neglects renewing domain name	Operator should ensure domain name record contact information is current and pay ahead of time. Business continuity plan must specify what to do when operator ceases to exist		1.75	5	1	1	2	2	1	1	1
A54	T4_C, T4_F, T4_G	An attacker gains privileged access to EVSE via physical connection (JTAG, HMI, USB, local wireless, serial, etc.) to copy client credentials so they can impersonate it	Information Disclosure	Physical	Implementers & Operators	Local interfaces are not secured and provide elevated privileges (either by default, or trivially achievable)	Disable debug interfaces during manufacturing (JTAG, etc.). Secure all open interfaces and require authenticated multi-factor access. Protect client/device identity so it is not easily duplicated with physical access, e.g. by placing cryptographic asymmetric keys in cryptochips or secure elements.		1.75	1	1	5	3	0	1	0	3
A5	T2_D	An attacker executes a denial of charging attack by causing physical interferences on the charging cable	Denial of Service	Physical	Grid & EV	Charging cable acts as an unintentional antenna	N/A	Brokenwire	1.75	3	1	2	3	0	3	1	1
A97	T5_F	An attacker denies charger from communicating with the CSMS using {disconnecting Ethernet cable, arp spoof, cutting switch or local CSMS power}. CSO-configured policy establishes free charging if communication cannot be established	Denial of Service	Adjacent	Implementers & Operators	CSO configures free charging during communications outages	Review if free charging fallback is best aligned with busy objectives; harden network and communication mechanisms (physical protections) to mitigate malicious interference;	Loss-of-communication fallback behavior is typically charger configurable	1.63	2	1	5	3	0	1	1	0
A86	T4_A	Free Charging codes are hard coded into EVSE logic and users can input them	Spoofing	Local	Payment & Billing	Some EVSE logic may contain hard coded values for charge testing which can be leveraged for free charging in production	Ensure that testing values and hard coded values are inspected and evaluated prior to deployment in production.		1.63	5	1	1	2	0	2	1	1
A62	T4_D	An attacker gains control of the DNS server the device uses to redirect configuration updates, firmware updates, trusted entity updates, certificate renewal, etc. to a malicious server	Tampering	Network	Implementers & Operators	Use of non-standard, vendor-specific DNS servers that can depricate, disappear, be compromised. Use of normal DNS instead of DNSSEC	Use DNSSEC and use global DNS services that are unlikely to be compromised or disappear (Cloudflare, OpenDNS, Google, etc.) Make DNS part of a configuration that can be updated remotely, if needed later		1.63	5	1	1	1	0	3	0	2
A48	T4_A	An attacker tampers with the HMI interface by using unsecured interfaces (e.g. Bluetooth)	Tampering	Local	Implementers & Operators	Interfaces to HMI not disabled (Bluetooth, Remote Maintenence channels, etc)	Hardening of HMI components, operating system, and interfaces		1.50	1	2	5	2	0	1	0	1
A64	T4_D, T4_A	An attacker gains access to EVSE/EV/App using known vulnerabilities because the EVSE vendor no longer exists or provides security updates	Tampering	Network	Generic (non-specific)	When a vendor ceases to operate, the devices they have sold and deployed will not be updated and vulnerabilities discovered in their code will not be patched. When a new vulnerability is disclosed, this means all their deployed devices are vulnerable to attacks and present a danger to users and the rest of the architecture	The architecture shall have a security policy for what to do when vendors no longer provide security updates to deployed critical infrastructure. This may happen due to the vendor ceasing to exist, or simply not keeping up with security patches in a reasonable time, or refusing to patch vulnerabilities for whatever reason. There shall also be punitive mechanisms that force vendors to provide security updates and maintain the security of their deployed hardware.		1.50	5	1	3	1	0	1	0	1
A51	T4_B	An attacker prevents communication from EVSE to payment system	Denial of Service	Network	Payment & Billing	Data communication to payment system is blocked or denied, to prevent verification of payment or details. This can also happen when the network is down, servers are down, the nearby telecom tower is unreachable, network equipment fails, etc.	Consider what the failover state is, e.g. charging is denied and the station is useless, or charging can still be done, but under decreased payment security conditions. Payment transactions can be stored and processed later, when connectivity is restored. Backup modem or alternative communication path for emergency usage when normal usage is degraded; could be common for clusters of chargers.		1.50	1	1	2	3	0	3	1	1
A98	T4_D	An attacker denies charger from communicating with the cloud-based CSMS by {DDoSing the cloud service; DDoSing the charger/VPN gateway interface, severing charger uplink}. CSO-configured policy establishes a default charging policy of TxDefault(0), meaning the CSMS must communicate the power level	Denial of Service	Network	Implementers & Operators	When TxDefault(0) is used for load management of a feeder, the CSMS sets the charging profile based on existing EV charging facility power profile	No charge is the fail secure outcome. CSMS elastic scaling may address and DDoS prevention service may address the DDoS. Financial controls need to be established		1.38	2	1	2	3	0	1	1	1
A42	T4_G	An attacker extract crypto material via JTAG physical access	Tampering	Physical	Implementers & Operators	JTAG interface not disabled and/or pins still present	Remove JTAG pins, disable diagnotic services		1.38	3	1	2	1	0	1	2	1
A45	T3_A	An attackers gains access to the manufacturer network and uses maintenance channels to control the EVSEs	Elevation of Privileges	Network	Implementers & Operators	Missing privileged access management for 3rd parties	Protect access from 3rd parties with additional AuthN/AuthZ means		1.38	5	1	1	1	1	2	0	0
A3	T4_C, T4_G	An attacker forces the EVSE station into safety mode by physically tampering with the Control PCB	Denial of Service	Physical	Grid & EV	Housing of EVSE not tamper-proof	Tamper-proof EVSE Housing	Difficult to scale	1.38	1	1	3	2	0	2	0	2
A88	T4_B	EVSE cannot access necessary cloud services to process payment	Denial of Service	Network	Payment & Billing	EVSE may not be able to process payment due to access issues	Ensure payment processing connectivity exists and enable remote logging and notifications for connectivity problems		1.25	1	1	1	3	0	2	0	2
A78	T5_B	An attacker obtains genuine access credentials to devices because the credentials are not properly protected	Information Disclosure	Network	Generic (non-specific)	Certificate credentials depend on a private key, shared secret credentials depend on a shared key. Both of these can be copied from someone with the proper authority. Private keys can be more difficult to obtain because they can be better protected by the OS or hardware, but that requires using these protection methods, which are platform-dependent.	Use asymmetric/certificate credentials wherever possible, both for human users and Machine-to-Machine connections. Ensure credentials are protected by hardware (e.g. TPM) and the OS, and are not trivial to copy from a file or from memory. Use multi-factor authentication on credentials where possible, especially less secure credentials or those for human users.		1.25	5	0	1	1	0	1	1	1
A7	T5_E	An attacker bypasses the credentials on a management console exposed to the internet to change active frontend rectifier setpoints	Elevation of Privileges	Network	Grid & EV	buffer overflow, SQL injection, XSS, CSRF	Two-factor authentication on Internet APIs. Use secure libraries and configurations that are not vulnerable to injection and buffer overflows.	This is a cloud interface	1.13	1	1	2	1	0	1	2	1
A17	T6_C	An attacker steals the JSON Web Token and associates account with a developer account for free charging	Spoofing	Network	Payment & Billing	JSON Web Token reuse	Change development JSON Web Token regularly		1.13	3	1	1	1	0	1	1	1