SANDIA REPORT
SAND2022-9315
Printed July 2022

Sandia National Laboratories

Cybersecurity for Electric Vehicle Charging Infrastructure

Jay Johnson, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, Kandy Phan, Michael Kunz
Sandia National Laboratories

Rick Pratt, Tom Carroll, Lori Ross O'Neil, Brian Dindlebeck, Patrick Maloney, James O'Brien, David Gotthold
Pacific Northwest National Laboratory

Roland Varriale, Ted Bohn, and Keith Hardy
Argonne National Laboratory

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

As the U.S. electrifies the transportation sector, cyberattacks targeting vehicle charging could impact several critical infrastructure sectors including power systems, manufacturing, medical services, and agriculture. This is a growing area of concern as charging stations increase power delivery capabilities and must communicate to authorize charging, sequence the charging process, and manage load (grid operators, vehicles, OEM vendors, charging network operators, etc.). The research challenges are numerous and complicated because there are many end users, stakeholders, and software and equipment vendors interests involved. Poorly implemented electric vehicle supply equipment (EVSE), electric vehicle (EV), or grid operator communication systems could be a significant risk to EV adoption because the political, social, and financial impact of cyberattacks—or public perception of such—would ripple across the industry and produce lasting effects. Unfortunately, there is currently no comprehensive EVSE cybersecurity approach and limited best practices have been adopted by the EV/EVSE industry. There is an incomplete industry understanding of the attack surface, interconnected assets, and unsecured interfaces. Comprehensive cybersecurity recommendations founded on sound research are necessary to secure EV charging infrastructure. This project provided the power, security, and automotive industry with a strong technical basis for securing this infrastructure by developing threat models, determining technology gaps, and identifying or developing effective countermeasures. Specifically, the team created a cybersecurity threat model and performed a technical risk assessment of EVSE assets across multiple manufacturers and vendors, so that automotive, charging, and utility stakeholders could better protect customers, vehicles, and power systems in the face of new cyber threats.

ACKNOWLEDGEMENTS

This work was funded by the U.S. Department of Energy Vehicle Technologies Office under Grant DE-EE0034819.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
CAN	Controller Area Network
CCS	Combined Charging System
CSO	Charging Service Operator
DCFC	DC Fast Charger
DER	Distributed Energy Resources
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
MQTT	MQTT (No expansion)
OCHP	Open Clearing House Protocol
OCPP	Open Charge Point Protocol
TCU	Telematic Control Unit
V2V	Vehicle-to-vehicle Communication
WAP	Wireless Access Point
xFC	Extreme Fast Charger

1. BACKGROUND

Electric vehicle (EV) charging is widely expected to open new pathways to increasingly impactful cybersecurity risk for critical energy and transportation infrastructures, but significant knowledge gaps remain concerning cybersecurity risks and solutions. There has been substantial research into how the computerization and connectedness of modern vehicles represents cybersecurity risks to electric, autonomous, and connected vehicles. A wide variety of systems are affected including keyless entry, telematics and tracking, customer and dealer data onboard or in mobile devices or even cloud servers as well as safety critical functions including driver steering and braking control themselves[1,2]. However, far less research has focused on the security of electric vehicle supply equipment (EVSE). For this project, the team investigated cybersecurity of EVSE devices, communications to the vehicle, and upstream connections. For the latter, EVSE-to-headend system cybersecurity is typically encrypted cellular traffic to a cloud-based environment; these networks interact with fleets or aggregations of charging systems so it has been hypothesized that successful compromise may grant adversaries access to resources that could affect the electric grid, medical services, agriculture, manufacturing, defense, and transportation operations.

Potential cybersecurity impacts will worsen with greater prevalence of electric vehicles in passenger and freight applications and higher power chargers—e.g., DC fast chargers (DCFCs), extreme fast chargers (XFCs), and Megawatt Charging Systems (MCSs). Researchers from the trucking industry and government have drawn attention to the possible impacts of cyberattacks electric vehicle charging, citing vulnerabilities in vehicle systems followed by the publication of best practices guides recommending controls and mitigations[3,4]. Most recommendations follow established best practices for protecting vehicles, vehicle telemetry systems, and industrial control systems, with calls to implement NIST and other best practices[5,6,7,8].

Recognizing the need to understand EVSE cybersecurity vulnerabilities, attack vectors, risks, consequences, and security solutions, the DOE Vehicle Technologies Office (VTO) has recently funded several research projects. This research community, along with other government agencies, came together multiple times to exchange ideas and information[9]. In comparison to the other EVSE cybersecurity projects, this work focused on understanding vulnerabilities in high-power EVSE equipment and the potential risk to the power system if these devices were controlled maliciously.

---

[1] K. Koscher et al., "Experimental security analysis of a modern automobile," IEEE Symposium on Security and Privacy, IEEE Computer Society, 2010.
[2] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Computers & Security, Volume 103, 2021, https://doi.org/10.1016/j.cose.2020.102150.
[3] DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report, DOT-VNTSC-DOE-18-01, March 2018.
[4] NMFTA, GRIMM, & USDOT/Volpe Center. Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cyber Security, Version 1.2.1, May 30, 2018.
[5] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses," Energies, vol. 15, no. 11, p. 3931, May 2022, doi: 10.3390/en15113931. URL: http://dx.doi.org/10.3390/en15113931
[6] ElaadNL, EV Charging Systems Security Requirements. European Network for Cyber Security. Commissioned by ElaadNL. Version1.01. August 2017. URL: http://encs.eu/wp-content/uploads/2017/10/EV-Charging-Systems-Security-Requirements.pdf
[7] ElaadNL, EV Charging Systems Security Architecture. European Network for Cyber Security, Final Version, April 2016.
[8] ElaadNL, EV Charging Systems Security Threats. European Network for Cyber Security, Final Version, April 2016.
[9] NISTIR 8294, Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE), April 2020.

2. PROJECT STRUCTURE

The goal of this project was to protect U.S. critical infrastructure and improve energy security through technical analysis of the risk landscape presented by the anticipated massive deployment of interoperable EV chargers. To improve the vehicle industry's cybersecurity posture, this project:

- conducted adversary-based assessments of charging equipment,
- created a threat model of EV charging, and
- analyzed power system impact for different attack scenarios.

The outcomes of this project included:

- A threat model for EVSE and associated infrastructure and services (See Section 3, Threat Model)
- Recommendations for the automotive industry based on EVSE penetration testing (See Section 5, EVSE , and Section 8, Mitigations and Recommendations)
- Cyberattack power system impact analyses with remediation recommendations (See Section 6, Power System Consequences, and Section 7, Power System Risk)
- Clear documentation of gaps in EVSE cybersecurity and the path forward to address those weaknesses (See Section 8, Mitigations and Recommendations)

The task structure of this project is shown in Figure 2-1, wherein the left side (blue) estimates the probability of different attack scenarios and the right side (green) estimates the consequence of attack scenarios. The cybersecurity risk of a given attack is the combination of the likelihood and impact of the attack. Using the structure and studying a range of attack scenarios, optimal mitigations could be determined to prevent attacks at specific points in the attack kill chain (i.e., the steps to accomplish adversary goals).

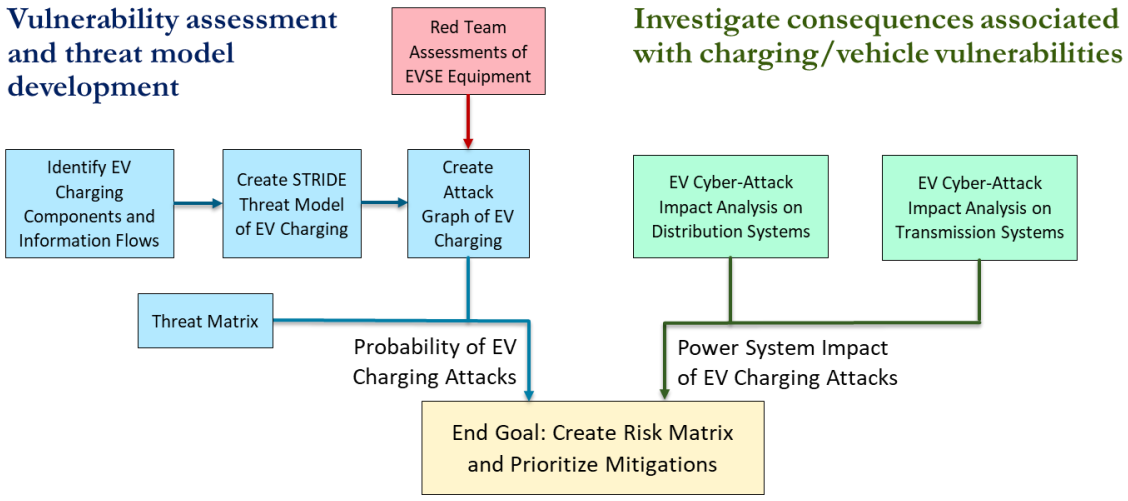

Figure 2-1. Project tasking.

Walking through Figure 2-1, the following activities were conducted in this project:

- **Identify EV Charging Components and Information Flows**. While implementations, topologies, and data exchanges vary between vendor and jurisdiction, there are some common features. Many of these are depicted in Figure 2-2. In the middle of the figure is the Extreme Fast Charger (xFC), DC Fast Charger (DCFC), or other charging point with an external plug or plugs, authentication terminal (e.g., the front console), and a hidden maintenance terminal. There may be multiple chargers at a single physical location, potentially with co-located distributed energy resources (DER). The EV-to-EVSE communications use a range of protocols including CCS (PLC-based with IP stack) and CHAdeMO, Tesla, or BG/T 20234 (all CAN bus-based). Within the vehicle there are a range of communication-based services connected to different cloud services to support music, browsing, navigation, infotainment, etc. The EVSE often has a cellular connection the EVSE operator or service provider can use to capture charging sessions and prognostics data using Open Charge Point Protocol (OCPP), IEEE 2030.5, or proprietary protocols. The service provider may connect to other service provider backend networks to verify charging transactions on chargers they don't own using Open Clearing House Protocol (OCHP) or to grid operators using Open Smart Charging Protocol (OSCP), OpenADR, or some other protocol.

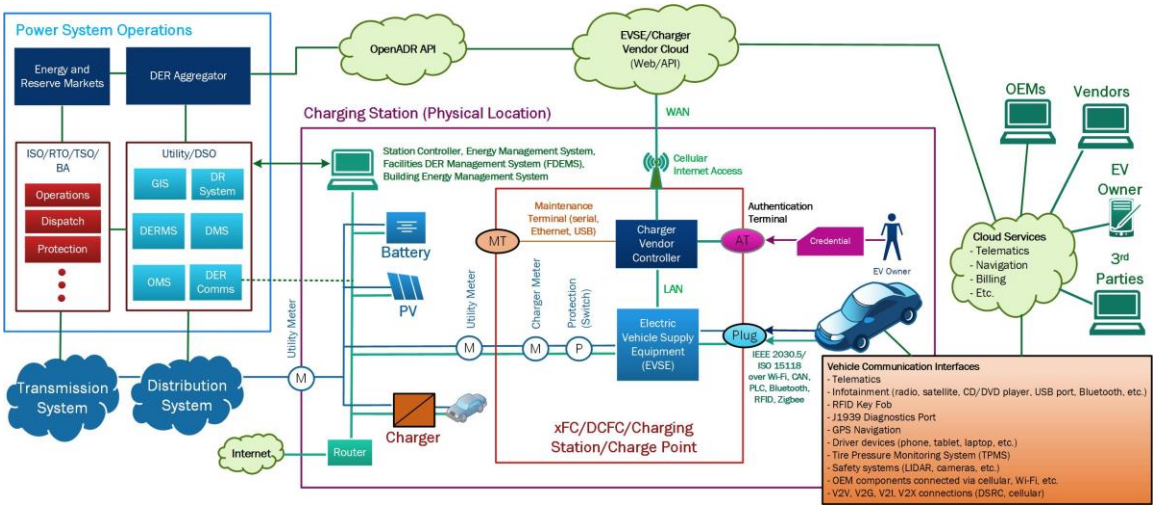

Figure 2-2. Electric vehicle communication systems to different components and entities.

- **Create STRIDE Threat Model of EV Charging**. Threat modelling is a useful technique to understand potential cyber hazards. To create the EV charging threat model, the EVSE communication ecosystem was created with the trust boundaries and all the processes were enumerated. Then different types of threats (spoofing, tampering, denial of service, etc.) were evaluated within the model to identify appropriate controls and mitigations.

- **Create Attack Graph of EV Charging**. Attack graphs were created to plot potential adversary actions to move from system or network access points to achieve consequences of concern. The exercise illustrated the importance of preventing attackers from pivoting between corporate, EV, and EVSE networks to achieve the goals.

- **EV Cyber-Attack Impact Analysis on Transmission Systems**. Part of the project was to determine the impact of potential vulnerabilities on the power system and different levels. For the transmission analyses, bulk electrical power system simulations were performed to understand the risk to the grid when EVSE were controlled in aggregate in a region and across large geographical areas.

- **EV Cyber-Attack Impact Analysis on Distribution Systems**. Localized power system simulations were conducted for a multiple of vehicle-to-grid (V2G) control scenarios to determine the risk to feeder-level power system operations.
- **Penetration Testing of EVSE Equipment**. The team assessed the cybersecurity posture of state-of-the-art EVSE equipment using authorized, adversary-based assessment techniques, often in close collaboration with the vendors. This approach was used to estimate the skill and time it would take adversaries to execute different attacks.
- **Risk Analysis**. Combining the likelihood of EVSE cyberattacks with the power system consequence was used to generate a notional risk matrix, as standardized in IEC 62443-3-2[10]. These scales are useful in estimating the level of difficulty in conducting these attacks and were used to estimate the likelihood of a successful EVSE cyberattacks. Threat profiles are simplified representations of the spectrum of adversaries from single actors with limited skills, time, and funding to nation states with hundreds of people, years of time, and millions of dollars in resources.[11,12]
- **Prioritize Mitigations**. Based on the penetration testing and the risk matrix, the team prioritized mitigations that would reduce the number of high-consequence/low-threat level attacks. The recommendations were designed to reduce the attack surface or eliminate credible attack vectors based on the cybersecurity assessments and threat model.

[10] IEC 62443-3-2, "Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design," 2020.
[11] D. P. Duggan, S. R. Thomas, C. K. K. Veitch, and L. Woodard, "Categorizing Threat: Building and Using a Generic Threat Matrix," SAND2007-5791, Sept. 2007.
[12] D. P. Duggan and J. T. Michalski, "Threat Analysis Framework," SAND2007-5792, Sept. 2007.

3. THREAT MODEL

Pacific Northwest National Laboratory (PNNL) led the task to develop a threat model of high-power electric vehicle charging infrastructure and systemically analyze it for threats that have the potential to bring wide-ranging consequences to the electric grid and transportation systems. PNNL derived a novel consequence-driven variant of the STRIDE threat modeling methodology to: (i) discover consequences that potentially impact vehicles, the electric supply, and transportation; and (ii) focus subsequent modeling and analysis on threats that may precipitate the consequence.

Threat modelling is an industry-recognized approach to enumerate and characterize potential threats and vulnerabilities that, absent the appropriate safeguard, may lead to a security incident or compromise. Subsequent analysis of the threat model guides and informs countermeasures and prioritize mitigations to prevent or reduce the impact of incidents.

Numerous threat modelling methodologies exist which can be categorized by focus. Bao *et al.* employs an adversary-centric approach, profiling the adversary by identifying types, capabilities, and motivations[13]. Other work focuses on use cases and how the relevant standards address them[14]. In this project, a component-centric approach based on STRIDE was applied. STRIDE is a mature approach to threat modelling invented by Kohnfelder and Garg while at Microsoft to identify computer security threats[15]. Other researchers have successfully applied STRIDE to the threat modelling of cyber-physical systems[16,17]. STRIDE is an industry-accepted approach to threat modeling, first made popular for its application at Microsoft. Threats are categorized into one of the following, with the desired properties shown in Table 3-1:

i. Spoofing: masquerading as a legitimate user, process, or system element;
ii. Tampering: modification/editing of legitimate information;
iii. Repudiation: denying or disowning a certain action executed in the system;
iv. Information disclosure: data breach or unauthorized access to protected information;
v. Denial of Service: disruption of service for legitimate users; and
vi. Elevation of privilege: gaining higher privilege access to a system element by a user with restricted authority.

After threats are enumerated, safeguards and countermeasures can be identified to mitigate the vulnerabilities. In this project, insights were gained by focusing on consequences of the security and resiliency of the EV charging ecosystem. Importantly, the threat model analysis suggests that no single entity (for example, charging station vendor or charging network operator) is ideally situated to secure the ecosystem, but instead, requires the concerted effort of the ecosystem.

[13] Bao, K, Valev, H, Wagner, M, & Schmeck, H, 'A threat analysis of the vehicle-to-grid charging protocol ISO 15118', Comput. Sci. Res. Dev., vol. 33, pp. 3–12, 2018.
[14] Lee, S, Park, Y, Lim, H, & Shon, T, 'Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology', Proc. of the 2014 International Conference on IT Convergence and Security (ICITCS), 2014.
[15] Kohnfelder, L & Garg, P, 'The threats to our products', Microsoft Interface, 1999.
[16] Khan, R, McLaughlin, K, Laverty, D, & Sezer, S, 'STRIDE-based threat modeling for cyber-physical systems', Proc. of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGTEurope), 2017.
[17] Shevchenko, N, "Threat modeling: 12 available methods", viewed 26th May 2020, URL: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html, 2018.

Table 3-1. STRIDE Threats

STRIDE Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

STRIDE threat modelling begins by identifying and modelling the in-place system along with appropriate system boundaries. The system is then decomposed into its constituent components. A *flow diagram* is then constructed, dividing components into functional blocks and then illustrating the exchange or "flow" of information between the blocks. The vehicle charging infrastructure is a cyber-physical system, demanding more than information exchanges to be considered. Consequently, the system models were amended with electric power flows that illustrated how power moves between the components in the system. The next step is to identify trust boundaries. A *trust boundary* is a concept that aids in the reasoning of trust domains and how they may influence one another[18]. Flows that operate across trust domains deserve special attention as they suggest exposure to untrusted data. The next step is to analyze threats in the flow diagrams to help find system threats. For each of the six threat categories, PNNL considered how the threat manifests as a security incident and the consequences that may occur. The system modelling and the threat modelling are iterative, where observations in one model may inform modifications in the other. The threat modelling process is complete once the system is sufficiently expressed.

Unfortunately, initial attempts proved unsatisfactory. It was observed that the identified consequences were in context of the components, and the impacts to electric supply and the transportation sector went unrecognized. Recognizing impacts was important as there was an explicit goal to relate the threat model to ongoing work modelling high-power EVSE and their effects on electric distribution grids and transmission grids, bulk electricity generation, and the transportation sector. The issue was that the consequences were outside the definition of the system model. To bridge the gap, we inserted steps to explicitly connect the threat model to security requirements:

1. maintain human safety and environment,
2. maintain availability of the electric supply,
3. maintain availability of the transportation system,
4. maintain availability and integrity of vehicles,
5. maintain privacy (maintain the confidentiality of personal data),
6. maintain integrity and non-repudiation of financial and energy transactions, and
7. maintain confidentiality of corporate information.

When considered as a whole, the security requirements assure people's continued faith in EVs and vehicle charging infrastructure, the continued adoption of EVs.

[18] Miller, M, 'Modeling the trust boundaries created by securable objects', Proc. of the 2nd USENIX Workshop on Offensive Technologies (WOOT), 2008.

If a connection could not be established, then the impact was deemed outside the scope of concern and excluded from the exercise. The flow diagrams were then analyzed to identify threats that may precipitate the selected consequences. If a threat materializes without involving the infrastructure, it was reasoned the conditions to manifest the threat exist at present, and therefore, was deemed out of scope for this exercise. Several rounds of impact, consequence, system modelling and threat modelling were performed. Modelling was subjectively deemed complete once the model's explanatory powers did not further elucidate electricity or transportation impacts.

Three flow diagrams were created to comprise the system. In Figure 3-1, a data flow diagram of an EV is shown with the EV in the lower left area; the lower right is a coarse representation of the charging station; and the top lists external entities. A flow diagram is a graph and represents the system decomposed into a set of elements and the relationships between them. The relationships are represented by data or power flows. The representation is logical, meaning functions can be combined when implemented in the context of controllers. The shapes have meanings: an oval represents a unit of function, a block is an external entity, and two parallel lines represent storage. One may think of a function unit as process, controller, or subsystem. An external entity is a person, organization, etc. that interacts with the system, affects the operation of or is affected by the system. A connection between entities represents flow. The arrow indicates the direction of flow, pointing from source to receiver. Connection labels provide additional context, identifying aspects such as communication protocols, circuit types, and voltages. While data flows can be bidirectional, a power flow will likely be unidirectional. A dashed rectangle indicates a trust boundary; entities in the boundary operate in a trust domain. Attention needs to be given to flows crossing trust boundaries as the data originates from an untrusted source. While all data should be checked, input and data validation are particularly important for handling of data from untrusted sources.

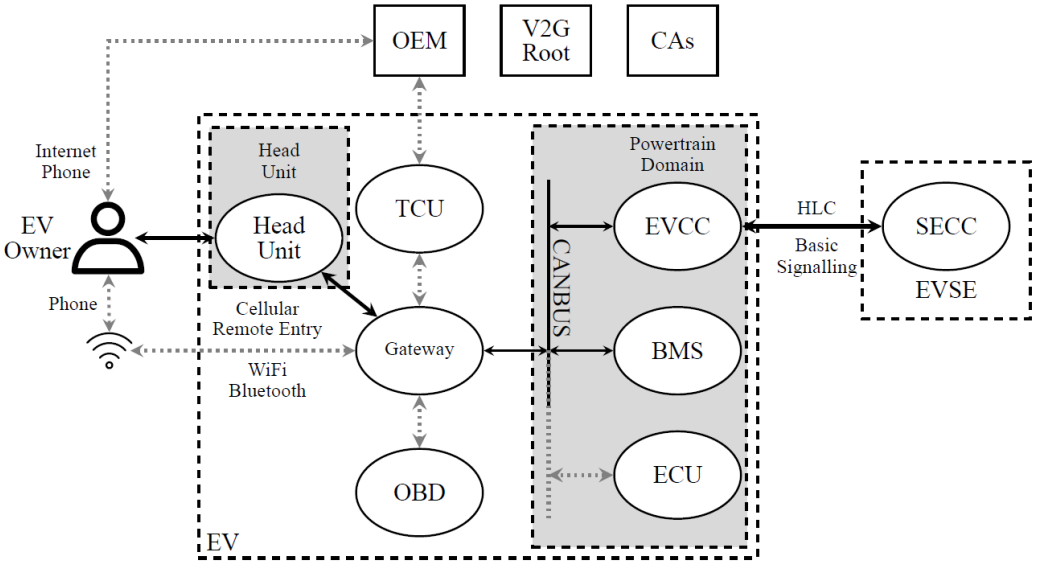

Figure 3-1. The EV data flow diagram.

The dark, solid connections are data flows that occur during the charging process. The light, dotted connections are data flows that may occur in addition with charging but are not critical exchanges for the charging itself. The vehicle representation is divided into three trust domains. The ``Powertrain

Domain" comprises the power plant, power transfer mechanisms, and electronic control units (ECUs) necessary for the generation and delivery of power to the driving wheels. It is reasonable to assume that the EV communication controller and the battery management system will be part of this domain. The EV communication controller facilitates communication between the EV and the charging station supply equipment communication controller. The Battery Management System (BMS) is a controller that monitors and protects the battery packs, controls charging, and calculates important ancillary data critical to the operation of the powertrain. The BMS and the batteries likely comprise tens to hundreds of other controllers[19] communicating using wired or wireless interfaces[20]. It is reasoned that documenting each controller is unnecessary; therefore, battery management, charge controlling, and related functionality are mapped to the BMS.

Much of the vehicle controller communications occur over controller area network (CAN). The CAN bus is a multi-master, message-based, broadcast-type intra-vehicle network designed to allow resource-constrained ECUs to efficiently communicate in real time. CAN bus is open and flexible, but lacks robust security[21]. The "Head Unit" comprises a user interface to control audio, navigation, and passenger cabin climate. It typically operates in a trust domain separate from other vehicle controllers. Current vehicles have several interfaces to communicate externally. The on-board diagnostic unit (OBD) is a diagnostic interface that allows access to vehicle subsystems. Additionally, the telematic control unit (TCU in the figure) sends diagnostics and other related information to the vehicle's original equipment manufacturer (OEM). As shown in Figure 3-1, contemporary vehicles are typically equipped with WiFi, Bluetooth, 4G/5G cellular modems, and other wireless communication interfaces. The interfaces substantially expand the vehicle's attack surface, allowing attackers external to it to access and influence its operation[22]. The gateway is responsible for mapping, translating, and routing messages between domains (such as between the powertrain CAN bus, TCU, and the passenger cabin network). Gateways are integral for secure vehicle communications, performing such functions as intrusion detection and prevention, firewalling, access control, key management, and secure time synchronization[23].

The V2G Root and subordinate certificate authorities (CAs) are external entities that identify and authenticate parties. Additionally, the certificate issued by the CAs identify the market roles of parties. The V2G Root CA is the top-level certificate authority that anchors the chain of trust. The V2G Root CA issues and digitally signs certificates for subordinate CAs; subordinate CAs then issue certificate for secondary subordinate CAs. The hierarchy establishes a trust relationship from any subordinate CA to the trusted V2G Root CA. The subordinate CA serves a role like publicly trusted CA that facilitate secure communications on the Internet. The secondary subordinate CAs perform all the necessary administrative functions to issue certificates to end users.

---

[19] Brandl, M, Gall, H, Wenger, M, Lorentz, V, et al., 'Batteries and battery management systems for electric vehicles', Proc. of the Design, Automation Test in Europe Conference Exhibition (DATE), pp. 971–976, 2012.
[20] Ulrich, L, 'Exclusive: GM can manage an EV's batteries wirelessly—and remotely', IEEE Spectrum: Technology, Engineering, and Science News, 2020.
[21] Hartzell, S & Stubel, C, Automobile CAN bus network security and vulnerabilities, URL: https://canvas.uw.edu/files/47669787/download, 2017.
[22] Sommer, F, Dürrwang, J, & Kriesten, R, 'Survey and classification of automotive security attacks', Information, vol. 10, no. 4, 2019.
[23] AUTOSAR 2018, Specification of secure onboard communication, Specification CP v4.4.0, AUTOSAR.

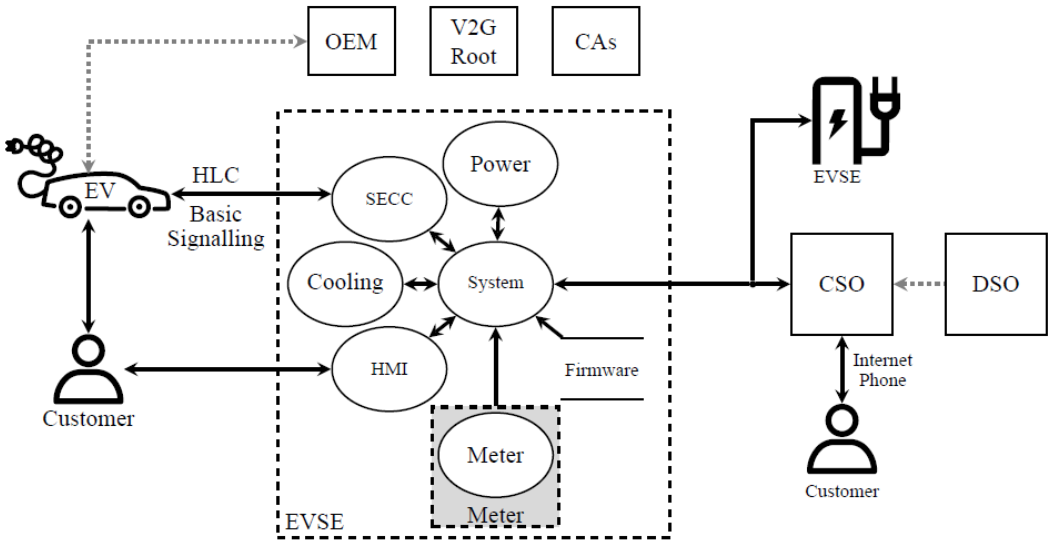

Figure 3-2. The EVSE data flow diagram.

The charging station data flow diagram is presented in Figure 3-2. The diagram can be divided into four regions. The left is the vehicle, the bottom center is the charging station, the right is the service provider, and the top portrays a list of external entities with charging infrastructure responsibilities. The charging station likely comprises multiple controllers. The System is the main charging station controller, providing the overall functionality of the charging station. The Power module controls and monitors the AC-to-DC conversion power electronics and protection circuits. The Supply Equipment Communication Controller (SECC) is the charging station ISO 15118 or other EV communication endpoint. High power transfers will generate large heat loads, so the cooling controller is instrumental for thermal management of the EVSE and ancillary components. The high-current power supply (≥400 A) necessitates large gauge cabling. To reduce bulk and make it less cumbersome, the cabling will likely be liquid cooled[24]. A human-machine interface (HMI) assists customer authorization and payment processing, and reports charging session metrics, such as the amount of power delivered and incurred fees. The meter reports usage and operates in a trust domain distinct from the System. Wireless communication (in particular, cellular) or a wired field network connect the EVSE to the charging service operator (CSO). The CSO will adjust its electric demand based on congestion and other smart charging signals received from the distribution system operator.

[24] Howell, D, Boyd, S, Cunningham, B, Gillard, S, & Slezak, L, Enabling fast charging: A technology gap assessment, 2017. URL: https://www.energy.gov/eere/vehicles/downloads/enabling-extreme-fast-charging-technology-gap-assessment

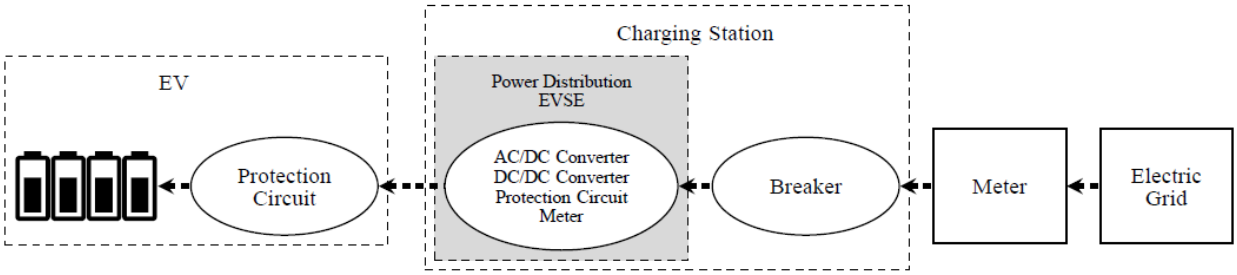

Figure 3-3. Charging infrastructure electric power flow diagram.

The final system model, Figure 3-3, illustrates the relationships imposed by power connections. An HPC charging station is likely supplied by 480 V to 35 kV distribution network connection. A utility monitors the electricity consumption at the station meter, which is distinct from the EVSE meters, which measures the power transferred to the vehicle and is used to bill the customer. The station's power distribution unit supplies power to one or more EVSE, which in turn, transfers power to EVs. A remote-controllable breaker (independent or incorporated in the power distribution unit) can disrupt power to the station. Additional local protection circuits may trip and disrupt a charging session. While not depicted in the figure, it is reasonable to assume that onsite storage and generation will supplement the electric grid supply[25].

The system models were analyzed independently and combined using the threat modelling methodology described in the previous section. The consequences and threats are enumerated below. Remote threats are defined as a threat that can be executed entirely through internet communications. Local threats are defined as a threat that requires a physical presence to the targeted components to execute some portion of an attack. The Remote designation suggests greater risk as the attacker can assault the systems from anywhere in the world.

Consequence #1: Loss of financial/energy transaction integrity or nonrepudiation.
Attacker Payoff: Power is stolen or misbilled.
Threat: An actor siphons electricity by impersonating an authorized consumer:

- Intercepting and tampering with EVCC-to-SECC data flows:
  - **(Local)** Using a modified charging cable[26]
  - **(Local)** Inserting a false SECC that intercepts and proxies messages (especially applicable to "remote" ISO 15118 architectures)
  - **(Local)** Using a software-defined radio to intercept and inject messages[27]
- **(Remote)** Clone or replay identification/payment token.
- **(Local)** Spoof the EVCC, for example, by substituting the EVCC from a wrecked vehicle

Threat: An actor tampers with the tariff schedule:

- **(Remote)** Intercept and tamper with the EVCC-to-SECC data flow (EVCC may optionally ignore signatures. See V2G2-307 and Note 6 on page 115 in ISO 15118-2.

[25] Bohn, T, "Multiport, 1+MW charging system for medium- and heavy-duty EVs: What we know and what is on the horizon?," 2020.
[26] Falk, R & Fries, S, 'Electric vehicle charging infrastructure: Security considerations and approaches', Proc. of the 4th Int. Conf. on Evolving Internet (INTERNET), IARIA, 2012.
[27] Baker, R & Martinovic, I, 'Losing the car keys: Wireless PHYlayer insecurity in EV charging', Proc. of the 28th USENIX Security Symposium SEC '19, pp. 407–422, 2019.

- **(Remote)** Intercept and tamper with EVSE-to-CSO data flow or spoof the CSO
- **(Local)** Tamper with charger firmware, storage or memory, targeting cached schedules (ISO 2014, pp. 121, note 5 addresses schedule caching)

Threat: An actor repudiates power transfers:

- **(Remote)** Tamper with logs in the charger's memory or storage
- **(Remote)** Tamper with the meter or the meter-charger data flow
- **(Local)** Intercept charger-to-CSO data flows, tampering with transaction details (attacker access field network equipment)
- **(Local)** Tamper with EVCC-to-SECC data flows, disabling metering receipts
- **(Remote)** Spoof the EVCC, SECC, or both to manipulate and obscure transaction details
- **(Local)** Tamper with HMI, accessing privileged functions

Consequence #2: Trip breaker or trigger protection circuit action.

Attacker Payoff: EVs are incompletely charged, limiting their range. Transportation system availability is reduced when performed at scale.

Threat: An actor denies charging:

- **(Local)** Tampers with the BMS firmware, configuration, or memory Tampers with the EVCC-to-SECC data flow:
  - **(Local)** Induce false charging state or settings
  - **(Remote)** Impersonate the charger and transmit false power measurements
- **(Local)** Physically tamper with power electronics

Threat: An actor administratively opens breaker:

- **(Remote)** Compromises privileged CSO, charger vendor, or similar account via phishing
- **(Remote)** Tampers with HMI or controller storage, memory, or firmware
- **(Remote)** Spoofs the CSO or tampers with charger-to-CSO data flows

Consequence #3: Induce electric disturbances across the grid, such as voltage oscillations (See Section 6.1.2), under voltage[28], low power factor[29], over frequency[30], and under frequency events[31].

Attacker Payoff: Increase grid stress that may lead to outages.

Threat: An actor steals account credentials:

- **(Remote)** Compromises charging application user level accounts, commands charging halt
- **(Remote)** Compromises developer account to insert malicious functions into smartphone apps, firmware, or related vector
- **(Remote)** Compromises CSO, charging station equipment vendor, or breaker privilege account to update equipment with improper settings or firmware, or invoke immediate stop charge function. As an example, consider that Fairley reports a vendor rapidly updating

[28] Khan, OGM, El-Saadany, E, Youssef, A, & Shaaban, M, 'Impact of Electric Vehicles Botnets on the Power Grid', 2019 IEEE Electrical Power and Energy Conference (EPEC), pp. 1–5, 2019.

[29] Rohde, KW, Cyber security of DC Fast Charging: Potential impacts to the electric grid, Technical Report INL/CON-18-52242-Revision-0, Idaho National Laboratory, 2019.

[30] Acharya, S, Dvorkin, Y, & Karri, R, 'Public Plugin Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?', IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5099–5113, 2020.

[31] Morrison, G, Threats and mitigation of DDoS cyberattacks against the U.S. power grid via EV charging, Master's thesis, Wright State University, 2018.

many devices[32]. Carlson and Rohde[33] and Lyngaas[34] discusses a relevant stop charge attack and the consequences. When both elements are considered together, a large-scale attack is conceivable.

Threat: An actor tampers with EV ECUs:

- **(Remote)** Compromised TCU provides vector to tamper with BMS or other ECU[35]
- **(Remote)** EVCC commands incorrect voltage or current set-points
- **(Remote)** Modified ECU firmware at supply chain source

Threat: An actor alters the charger behavior or state:

- **(Remote)** Tampers with controller firmware, storage, or memory
- **(Remote)** Accesses privileged interface to alter set-points

Threat: An actor coordinates the disruption of the charging processes:

- **(Remote)** Denial of Service attack against the CSO or the charger-to-CSO data flow
- **(Remote)** Deny trust store update, certificate revocation list update, or time synchronization

Consequence #4: Insufficient power delivery to the EVs
Attacker Payoff: EVs are incompletely charged, leading to the unavailability of transportation.
Threat: An actor tampers with power delivery:

- **(Remote)** Compromised developer or admin account pushes invalid configuration
- **(Remote)** Compromises EVSE's system shell and disrupts communication among EVSE power electronic modules (Rohde 2019)
- **(Local)** Tampering with charger's memory, storage, and firmware or compromising system shell to modify configuration parameters or code
- **(Local)** Tampering with chargers to introduce electrical conditions (e.g., electrical shorts)

Threat: An actor interferes with the SECC:

- **(Local)** Denies or intercepts and tampers with the EVCC-SECC or the charger-CSP dataflows
- **(Remote)** Spoofs the charger or the CSP
- **(Remote)** Denies CSP certificate revocation distribution or secure time synchronization

Attacker Payoff: People are injured while utilizing an EVSE
Threat: An actor tampers with the charger:

- **(Local)** Tampered cooling controller causes customer to burn hand when touching connector or cabling
- **(Local)** Tampered circuit contactor is welded closed, causing electric shock

Consequence #5: Employ infrastructure for purposes other than charging
Attacker Payoff: Gain access to additional computational and network resources
Threat: An actor repurposes CSP or charger computing and network resources:

---

[32] Fairley, P, "800,000 microinverters remotely retrofitted on oahu—in one day," viewed 11th August 2021, https://spectrum.ieee.org/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu, 2015.
[33] Carlson, B & Rohde, K, Consequence-driven cybersecurity for high power EV charging infrastructure, viewed 8th July 2021, 2020. URL: https://www.energy.gov/sites/default/files/2020/06/f75/elt199_Carlson_2020_o_5.1.20_1.12PM_JL_0.pdf .
[34] Lyngaas, S, Power struggle: Government-funded researchers investigate vulnerabilities in EV charging stations, viewed 11th August 2021, 2019. URL: https://www.cyberscoop.com/ev-charging-stations-hacked-idaho-national-laboratory/
[35] Oyler, A & Saiedian, H, 'Security in automotive telematics: a survey of threats and risk mitigation strategies to counter the existing and emerging attack vectors', Security Comm. Networks, vol. 9, pp. 4330–4340, 2016.

- **(Remote)** Tampering with the charger or related systems to mine cryptocurrency
- **(Remote)** Exploiting CSP or CSO systems to execute DDoS attacks

Consequence #6: Information disclosure and loss of privacy
Attacker Payoff: Information that can be sold for money
Threat: An actor illicitly accesses business-competitive information, such as customer data:

- **(Local)** Tampers with CSO database, using charging station field network access
- **(Remote)** EV vulnerabilities or misconfigurations allow remote access to driver/vehicle information

3.1. ISO 15118-2 PKI

A critical look at the public key cryptography and the public key infrastructure (PKI) components of the ISO 15118-2 standard were included in the threat modelling effort as these security requirements are the underpinnings for EV-to-EVSE communications and "plug-and-charge" (PnC), where the vehicle automatically identifies itself and authorizes power reception. EVSE threat modelling was valuable because the exercise illuminated weaknesses and security concerns that appear in ISO 15118 and would likely be encountered in vehicle charging infrastructure regardless of the charging regulation protocol. The ISO 15118 committee deliberately limited the scope of the standard to normalizing the EV-to-charger interfaces. Infrastructure is more than just chargers and charging stations; it comprises a multitude of secondary actors to handle charging session authorization, billing, and payment processing, charging station operation and maintenance, vehicle registration, electric grid congestion and capacity management, station reservation, roaming and smart charging. Roles and responsibilities of secondary actors and the associated interactions are addressed informally in ISO 15118. While addressing the entire vehicle infrastructure would certainly be ambitious, it would not provide the flexibility to address emerging technical and business requirements and challenges. Instead, complementary standards must fill in the gaps. Given the limited scope, the charging station is assumed to be trusted and is the hub of all communications between the EV and infrastructure. Consequently, end-to-end communication security is unavailable[35] as the charging station must route messages between the vehicle and, for example, the charging station operator. Some of the concerns are ameliorated with data security mechanisms. Contracts, tariff schedules, and metering receipts are signed and provide a means for the EV and third parties to ensure the authenticity and integrity of the data. Unfortunately, data security is not extensive because many interactions are outside the purview of ISO 15118. Moreover, while communication and data security are required for PnC, their use remains optional when alternate authorizations schemes are employed. This remains an issue because PnC capability is not widely available, with most charging sessions authorized with external identification means, such as RFID and NFC.

Electric vehicle charging security presents a significant challenge that is complicated by capital-intensive infrastructure, long vehicle service lifetimes (ten years and longer), and memory and computationally-constrained devices that participant in charging regulation. Technical design had to balance the trade-offs among functionality, interoperability, cost, and security. The choices made may have security repercussions. The ISO 15118-2 digital signature scheme is NIST standard curve P-256, an elliptic curve digital signature algorithm extensively used in many compute-constrained applications. The algorithm and the long lifespan of V2G root certificates (which are valid for forty years) will collide headlong with the large-scale quantum computing epoch. The quantum computing resources to factor P-256 is estimated as 2330 logical (error-corrected) qubits, 8.05×10^6 physical qubits,

and 10.5 hours of compute time[36, 37]. Quantum computing at such a scale may be attainable sometime in the next decade[38]. ISO 15118-20, the communication standard designed to supplant ISO 15118-2, has adopted the elliptic curve digital signature algorithms NIST standard curve P-521 and Ed448[39], both of which increase the difficulty to break the cryptography. Unfortunately, the changes are not backward compatible with ISO 15118-2 and still may not offer sufficient margin of security given vehicle lifespans and anticipated quantum computing advancements. (The resources to crack P-521 is estimated to be 4719 logical qubits, 1.13x107 physical qubits, and 55 hours[40].) Crypto-agility, the capacity to switch to alternate cryptographic primitives without inducing significant system changes, is seen as an imperative to prepare for the coming quantum computing era[41]. ISO 15118 exhibits limited crypto-agility; instead, it specifies hard requirements and parameters. As ISO 15118 lacks a meaningful future-proofing mechanism (such as algorithm negotiation for digital signature schemes), protocol and parameter substitutions will need to be had in subsequent revisions of the standard, which will bring incompatibilities. This is witnessed with the development of ISO 15118-20[42] which introduced cryptographic algorithm and parameter substitutions that are incompatible with ISO 15118-2. To address backward compatibility, a future update to ISO 15118-2 is possible that would harmonize it with ISO 15118-20[43]. Manufacturers, vendors, and operators will face an intractable choice: either prevent some vehicle models from charging as they cannot be modified to inter-operate; or allow vehicles to charge utilizing vulnerable algorithms, protocols, and parameters, a practice that is widely considered to be highly insecure. Migration to TLS 1.3 (and possibly hybrid post quantum cryptography) will serve to highlight the challenges of transitioning current EV charging to a more future proof, secure variant.

ISO 15118-20 is expected to be published in 2022. Its authentication and data security are more robust and have greater security margins than what is available with ISO 15118-2:2014. Consequently, the public key cryptosystems and infrastructure of ISO 15118-20 is preferred over the ISO 15118-2:2014 equivalent. As on-the-road vehicles—notably Ford MACH-E—already realize ISO 15118-2 PnC. Therefore, it is foreseeable in the near term for both standards to reasonably co-exist, each with its own PKI. Some fear ISO 15118-20 adoption will be slow and may never be fully embraced by the marketplace. To avoid this from happening, the EV ecosystem should make a concerted effort to adopt ISO 15118-20. With ISO 15118-20 acting as the default communication protocol, ISO 15118-2—stripped of the TLS, PKI and PnC—could function as fallback when either the vehicle, charging station, or both don't support ISO 15118-20. If the industry determines that moving to ISO 15118-20 is necessary, clear time schedules must be defined to deprecate and retire ISO 15118-2.

Charging infrastructure security cannot be an afterthought as cyberattacks will have severe consequences to individuals and societies. The threat model activity was undertaken to recognize, identify, and characterize security objectives, threats, and vulnerabilities. Work is underway to investigate and develop relevant countermeasures and safeguards to prevent or mitigate the threats. Technology alone cannot solve the issue. As vehicles become more connected, vehicles, charging infrastructure, and the electric grid can no longer assume that they are isolated from the outside world. Due to the tight coupling between charging infrastructure and electric grid, and since no entity is ideally positioned to address security challenges, electric utilities, vehicle manufacturers, charging station equipment vendors, operators, and service providers will need to collaborate in assuring the electric supply and EV charging services. Establishing a consortium to define and demarcate responsibilities and roles, facilitate information sharing, and coordinate activities would support the undertaking of the enterprise and beyond the resources of any single member. Moreover, the

collaboration could support the development of components critical to the safe and secure operation of charging infrastructure[36].

Research is required to develop countermeasures and safeguards to mitigate the novel threats identified in this work and that account for the character of charging infrastructure and services. Work conducted by the community is actively underway. For instance, Fuchs proposes a hardware security module for EVs to ensure the secure generation and storage of credentials[37]. Idaho National Laboratory[38] is developing the *safety instrumented system* framework to monitor EV charger operation and properties. van den Broek *et al.* propose securing the information instead of the communication channel[39]. Additionally, secondary actor confirmations can thwart spoofing[40]. Charging security research is critical as the United States sets a year 2030 target for half of all new light duty vehicles sales as EVs[41].

Following a whitepaper titled "Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem"[42] published by DigiCert, ChargePoint, and eonTi, there was considerable interest to evaluate weaknesses in the ISO 15118 PKI requirements[43]. SAE started a Cooperative Research Program (CRP) to investigate the concerns the industry identified[44], such as how security certificates would be exchanged between entities. Then SAE created a work group to address the governance concerns raised in the whitepaper by establishing an "industry joint venture [to] design and test a secure, trusted, and scalable EV charging Public Key Infrastructure (PKI)"[45,46].

In the whitepaper, the authors laid out perceived weaknesses in governance, technology, and operations focus areas with sub-areas that are critical to the implementation of a practical and realization of secured ISO 15118 based EV charging infrastructure. As with all standards, the ISO standards development organization made specific compromises to establish an operational PKI framework that would work for all stakeholders. The ISO 15118-2 standard alone is not sufficient to address all the requirements for an operational PKI system, and the U.S. needs operational guidance and a formal certificate policy—similar to the content in the German Verband der Elektrotechnik,

---

[36] Metere, R, Neaimeh, M, Morisset, C, Maple, C, et al. 2021, 'Securing the electric vehicle charging infrastructure', CoRR, vol. abs/2105.02905, https://arxiv.org/abs/2105.02905.

[37] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova, "HIP: HSM-based identities for plug-and-charge", Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1–6, 2020.

[38] B. Carlson, Consequence-driven cybersecurity for high-power EV charging infrastructure, viewed 28th August 2021, https://www.energy.gov/sites/default/files/2021-06/elt199_carlson_2021_o_5-12_351pm_LR_TM.pdf .

[39] F. van den Broek, E. Poll, B. Vieira, "Securing the Information Infrastructure for EV Charging", Wireless and Satellite Systems, pp. 61–74, 2015.

[40] S. Lee, Y. Park, H. Lim, T. Shon, "Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology", Proc. of the 2014 International Conference on IT Convergence and Security (ICITCS), 2014.

[41] United States, Executive Office of the President 2021, Executive Order on strengthening American Leadership in clean cars and trucks, August 5, 2021.

[42] "Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem," DigiCert, ChargePoint, and eonTi whitepaper, May 14, 2019.

[43] B. Sidles, "ISO 15118 Plug&Charge", EPRI IWC Meeting, White Plains, NY, Oct 23, 2019.

[44] B. Berman, "The ISO standard for electric-vehicle 'Plug-and-Charge' faces security concerns," 2020-08-11, URL: https://www.sae.org/news/2020/08/iso-ev-plug-and-charge-standard-faces-security-concerns

[45] SAE, "SAE kicks off project to develop cyber-secure EV charging, 2020-09-25," URL: https://www.sae.org/news/2020/09/sae-pki-secure-ev-charging-project

[46] SAE, "SAE International to Launch Industry-Driven SAE EV Charging Public Key Infrastructure Project," 2020-05-14, URL: https://www.sae.org/news/press-room/2020/05/sae-international-to-launch-industry-driven-sae-ev-charging-public-key-infrastructure-project

Elektronik und Informationstechnik (VDE) Guide, VDE-AR-E 2802-100-1[47] and Hubject Plug&Charge Certificate Policy[48]—in order to effectively cover the governance, technology, and operations requirements. Hubject, a German joint venture of BMW, Bosch, Daimler, EnBW, innogy, Siemens, and Volkswagen, is currently the only V2G Root CA operator. Although the standard allows for others to be establish (e.g., in North America)[49]. With respect to the white paper, the following comments are presented to further the dialog on V2G PKI security:

1. **Certificate Policy.** A certificate policy and Certification Practice Statement must be created, but it does not necessarily need to be included in the standard. Arguably, ISO 15118 is not the appropriate venue to establish certificate authority roles, responsibilities, and practices, and the certificate policy could be established by the certificate authority (e.g., Hubject) as they are responsible for administrating it. Using the Internet as a model, TLS is an Internet Engineering Task Force (IETF) standard that describes the protocol to communicate securely between two parties. It defines the technical mechanisms to accomplish the communications but does not issue policies. The CA/Browser Forum[50] is a voluntary industry consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of digital certificates. CA/Browser forum defines the roles, responsibilities, and practices, along with establishing cryptographic requirements[51,52]. These policies do adopt technical requirements, for example, establishing minimum key length, hash length, and required certificate extensions, deprecating and obsoleting cryptographic algorithms, etc. Additionally, NIST proffers guidance on multiple technical fronts, such as for key management[53].

   ISO 15118 standard recommends limiting the number of V2G Root CA certificates, with a minimum number of 5 Root CAs (roughly 1 per continent). Even under that scenario, multi-root issues may appear since each continent would have its own PKI ecosystem and vehicles may be shipped between them. Consideration of cross-certification is a good idea for those cases. Providing specific governance may be difficult due to different identity/privacy regulations and legal requirements across jurisdictions.

   The final draft of ISO 15118-20 now assumes the existence of a policy authority that would provide the governance for the PKI ecosystem.

2. **Algorithms and Protocols.** The PKI/TLS foundations employed in 15118 is well-established and employed globally at Internet scales. The foundations—and their corresponding standards—are exhaustively evaluated to find defects. In terms of practice, these foundations

[47] VDE-AR-E 2802-100-1, "Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118", Dec 2019. URL: https://standards.globalspec.com/std/14246231/VDE-AR-E%202802-100-1

[48] Hubject GmbH, "Hubject Plug&Charge Certificate Policy for the Hubject ISO 15118 V2G PKI" Version 1.6. August 2019.

[49] ElaadNL, Exploring the Public Key Infrastructure for ISO 15118 in the EV Charging Ecosystem, Arnhem, The Netherlands, November 2018.

[50] CA/Browser Forum, URL: https://cabforum.org/, accessed 9/21/21.

[51] CA/Browser Forum, "Network and Certificate Security Requirements," Forum Guideline, Version 1.2, URL: https://cabforum.org/wp-content/uploads/CABForum-Network-Security-Controls-1.2.pdf, accessed 11-1-2019.

[52] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates," Version 1.6.6, URL: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.6.pdf, accessed 11-1-2019.

[53] E. Barker, SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management: Part 1 – General," May 2020.

serve many world-wide applications. It is the best tools available to address the challenges of identity, confidentiality, integrity, and non-repudiation. These foundations are not perfect. There have been defects in these foundations requiring response, such as, patching, change of parameters, etc. Moreover, some defects have required changes to the protocol. The most recent version of TLS, TLS 1.3[54], has been engineered and mathematically proven to satisfy many desirable security properties.

We note that public key cryptography and transport security is only utilized in the "plug and charge" use case. The conditional use of transport security was eradicated in the drafting of the ISO 15118-20 standard. Digging into the cryptographic algorithms and parameters, we find V2G2-201 (minimum SHA-256 cryptographic hash), V2G2-202 (ECDSA or ECGDSA signature schemes), V2G2-203 (256-bit key length providing 128-bit strength), and V2G2-256 (mandatory cipher suites). The mandatory cipher suites conflict with TLS 1.3 as TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 and TLS_ECDHE_WITH_AES_128_CBC_SHA256 are obsoleted and excised from the standard. Text in ISO 15118 is necessary to address TLS 1.2 vs TLS 1.3. Notably, ISO 15118 specifies mandatory minimum cryptographic requirements. We note that these requirements are a *minimum*; the standard does not contain language suggesting that stronger cryptography cannot be used.

Increasing the strength of the cryptography will likely introduce backward incompatibilities. The public key cryptography in ISO 15118-2 is founded on elliptic curve P-256, which provides 128-bit security against cryptoanalysis. The final draft of ISO 15118-20 relies on different set of curves, Ed448 and P-521, which offer 224-bit and 256-bit strength, respectively, against cryptoanalysis. These differences introduce notable changes to the X.509 certificates, such that a certificate compliant with one will not interoperate with the other. For a vehicle or charger to be compliant with both, the entity will need to be issued two distinct certificates.

For an embedded system, involving hard to update vehicles and charging stations, using a fixed set of cryptographic standards is a tradeoff between engineering and assessed risk. The endpoints may not be fully capable modern computers and are instead closer to an embedded endpoint with limited storage or processing capabilities. Fixing the cryptographic approach allows implementers to use fixed function hardware that can be cheaper and more reliable for handling cryptographic functions if they wish. The primary weakness in defining specific hash algorithms, signature algorithms, and protocols for use in the ecosystem is preventing crypto-agility in the future. The allowance for updates to the cryptographic approach in newer versions of the standard will be necessary with the development of quantum computing.

3. **PKI Hierarchy.** In the current design the CA hierarchy is well-defined. In the whitepaper, changes to the hierarchy were considered. Before that decision is made, it is recommended to fully evaluate the benefits of reducing the CA hierarchy depth—and consequently, the flexibility of the PKI system**.** The work performed in the SAE EV Charging Public Key Infrastructure (PKI) project has added a new root, the Certificate Policy Authority, which authorizes the V2G Root certificate authorities[55]. The addition limits the opportunity to reduce the depth of the CA hierarchy.

[54] RFC 8446, "The Transport Layer Security (TLS) Protocol Version 1.3", URL: https://tools.ietf.org/html/rfc8446, accessed 10-31-2019.
[55] Weisenberger, T et al. 2021 SAE EV Charging PKI Industry Ecosystem Review

4. **Key Management.** Secure storage for keys is a hardware implementation issue outside the scope of the standard. There are many complications with EVs in the commissioning process because this is a multi-party environment (various EV vendors, charging companies, e-mobility service providers, etc.), but these challenges can be overcome with effective guidelines. In an Enterprise environment, a dedicated IT staff can perform the necessary provisioning, configuration, and update activities. However, with an EV, that is left to the owner who may not even be aware of the functionality that they are using in their daily operations.
5. **Certificate Revocation Policy.** There is a robust ISO 15118 certification revocation process that uses Online Certificate Status Protocol (OCSP) to get the revocation status of the X. 509 digital certificates. This is state-of-the-art, but considerations for the operations of the system when the OCSP server is unavailable or unreachable are necessary.
6. **Identity and Access Management.** It is unclear that requirements for proving the identity of subscribers belong in ISO 15118. If a particular EV can be linked to a particular service provider for billing, the details of customer identification should be left to the relevant service providers. Some service providers may wish to support cryptocurrencies or other pseudonymous payment services and may not care about the customer identity beyond a simple numbered account with value present. Requiring strict identity validation to use a charging system may also be used to unfairly prevent certain groups from charging.
7. **Business Continuity.** ISO 15118 includes contingencies for when the charging station is offline. However, if the CA is offline, system operation may be indeterministic. Since chargers are often deployed in areas with poor communications, the inability to verify certificates will already be included in business processes.
8. **Audit Policy.** Formal audit policies should be formulated in additional implementation guides, best practices, or standards.
9. **Incident Response, PKI Auditing, and Physical Security.** These are considered out of scope for the standard but need to be addressed in the certificate polity or another formal standardization process.

4. ATTACK GRAPHS

Attack graphs show the steps an attacker must take to move from a system/network access point to a consequence or objective. The use of attack graphs simplifies the identification of key steps an attacker must take to achieve their objectives, allowing those actions to be detected or prevented. Figure 4-1 illustrates access points, staging areas, and consequences of concern related to a generic EV charger network. In this figure, one of the attack paths involves an attacker using an initial compromise of an EVSE provider's business network to impact the bulk power system. By analyzing the steps in this attack path, detective or preventive controls – such as monitoring for unusual Network Time Protocol traffic or requiring code signing of EVSE updates – can be implemented. The team used the information gathered from their assessments, publicly available information regarding vulnerabilities, and knowledge regarding the tactics, techniques, and procedures used by attackers to advise the attack graph. In the case of coordinated EVSE attacks that disrupt the power system, there were two major questions:

- Can the attacker "pivot" between the components, systems, and networks in the EV/EVSE ecosystem to compromise the necessary information flows?
- Can an attacker synchronize their attack to affect large portions of the grid simultaneously?

From the assessment activities, it appears both are possible so an attacker *could* manipulate large networks of EVSE and cause distribution and transmission impacts.[56]

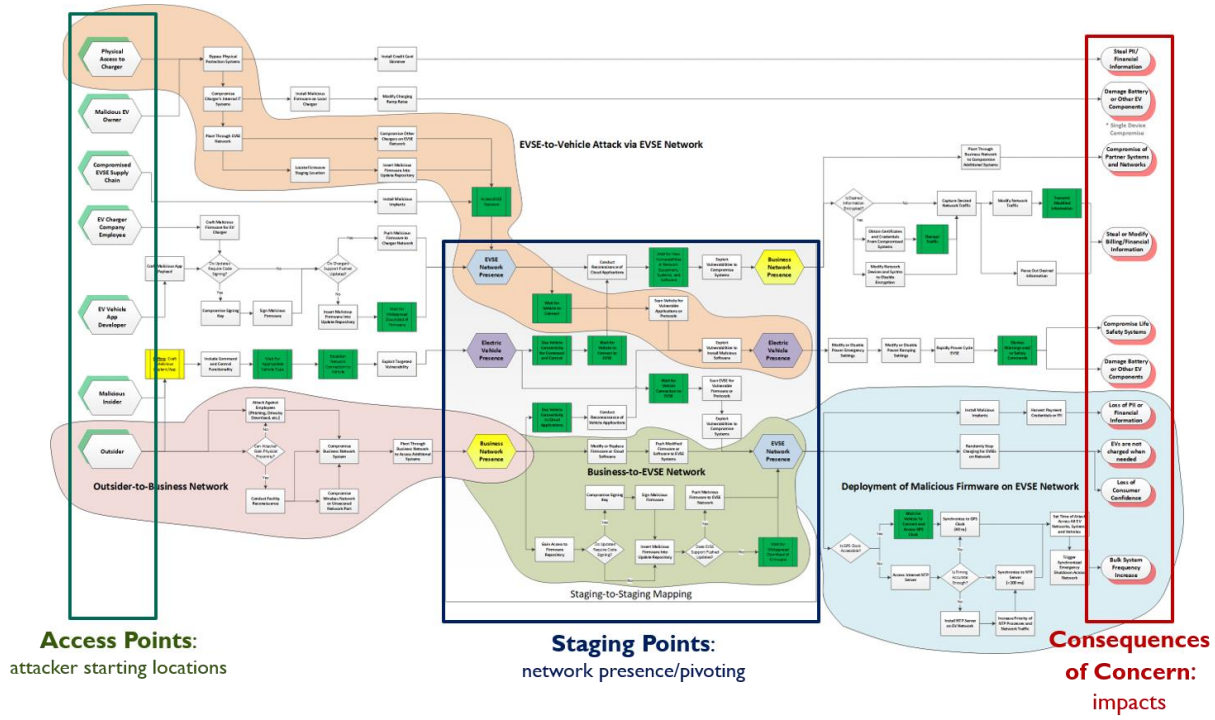

Figure 4-1. EVSE Ecosystem Attack Graph.

[56] B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020. URL: https://www.researchgate.net/publication/339053631_Securing_Vehicle_Charging_Infrastructure_Against_Cybersecurity_Threats

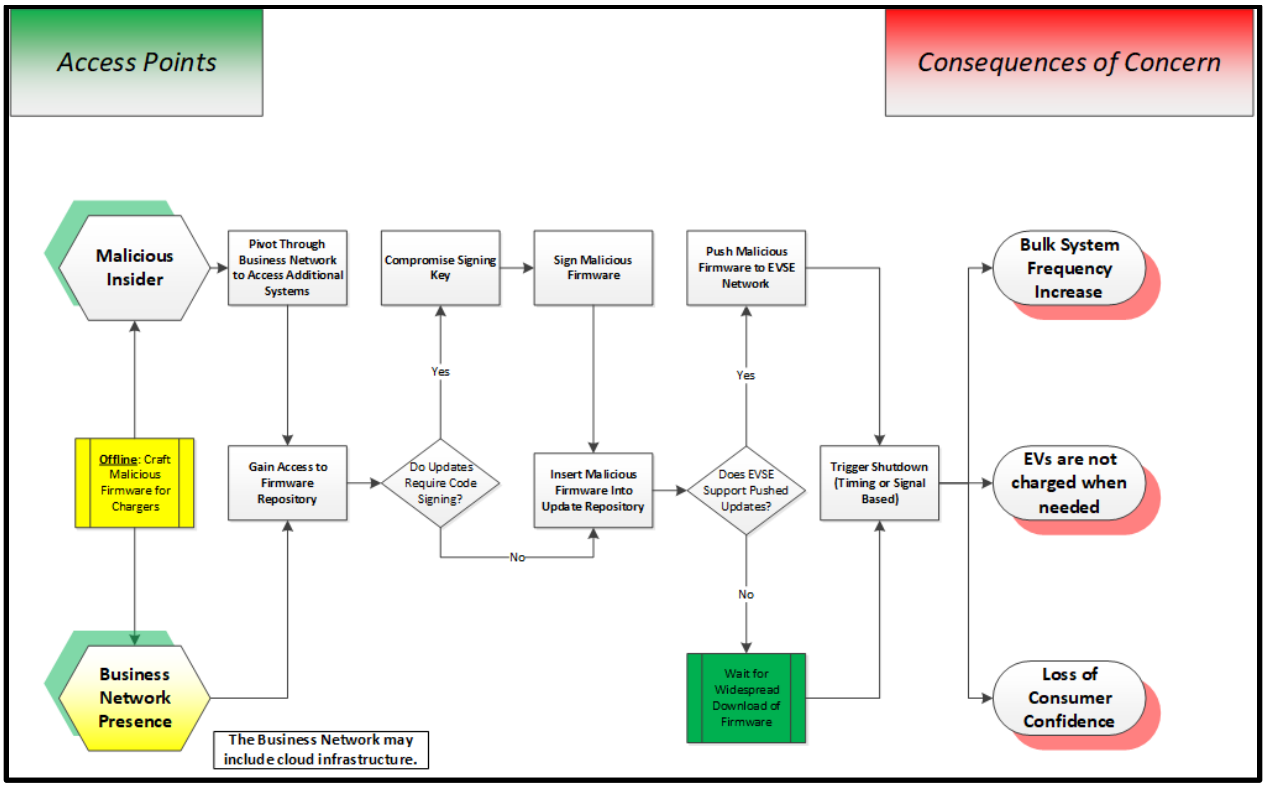

Figure 4-2. Deployment of Malicious Firmware

The first step in this attack path is for the malicious actor to craft the payload that will be delivered to the deployed EVSE. This reduces the amount of time the attacker needs to be present on the target's systems, reducing the chance of detection prior to delivering the malicious firmware update.

Once that is accomplished, the attacker gains access to the business network using either a malicious insider or using remote attack techniques. For the insider, this could be accomplished by identifying a disgruntled worker, finding an unwitting accomplice, or using more direct methods like bribery. For a remote attack, this could be accomplished through a phishing attacker, watering hole attack, or other standard attack technique.

Once the attacker has a network presence, they need to pivot through the business network until they have access to the firmware repository. Once they have compromised the repository, if the EVSE do not require code signing on updates, the attacker can simply replace the legitimate version of the firmware with their own, malicious version. If the EVSE do require code signing, the attacker will have to take the additional step of compromising the signing key, either by gaining access to it directly, or injecting the malicious code at a point in the deployment process where standard procedures will result in it being signed. Once the malicious code is signed, the attacker can stage it for deployment to the EVSE. At this point, if the EVSE network allows updates to be pushed to the systems, the attacker can choose that route to immediately infect the systems. If they don't want to risk detection, or the system requires the EVSE to initiate an update, the attacker can simply wait for the systems in the EVSE network to download their malicious firmware.

Once deployed throughout the network, the method of triggering the payload will depend on the best mechanism that will achieve the attacker's objective. For example, it could be logic-based where the EVSE does not charge an EV if it is below a certain power threshold. This would ensure the

EVs are not charged when needed and, if widespread, could impact consumer confidence. Alternatively, it could be a prearranged time, allowing all of the compromised EVSE to coordinate their attack to achieve a grid-level impact. For example, in the early weekday morning (when demand is high[57]) at a specific time – coordinated through GPS or NTP clock synchronization – all of the EVSE could stop charging at the same moment, impacting the grid usage. If necessary, the EVSE could also alternate, at precise intervals, between full charging and no charging, creating surges throughout the grid, impacting the bulk system frequency.

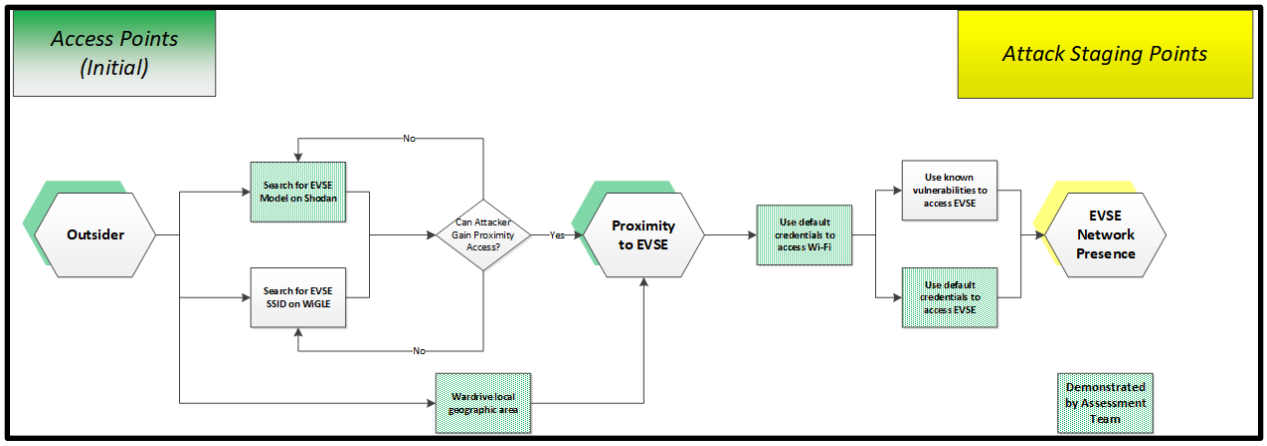

Figure 4-3. Assessment Attack Graph

This attack graph illustrates the steps achieved by the assessment team on a variety of EVSE equipment from multiple manufacturers. These steps are identified by green shading in Figure 4-3. Working without any kind of insider access, the team was able to identify specific models of EVSE using the Shodan search engine and was also able to detect a wireless access point (WAP) installed inside a local EV charger. The team did not travel to the EVSE located by Shodan but, since the team had an existing partnership with the local EV charger owner, they obtained permission to conduct a penetration test against the WAP. The default credentials for the system were easily found and were still valid for the wireless network. Since the wireless network architecture included a connection to the EVSE network, from the WAP the team was able to monitor EVSE network traffic.

After discussing the wireless network with the system owner, the assessment team discovered they were not aware the charger came equipped with wireless networking. Without awareness of the capability, the EVSE owner did not perform any administration to harden the wireless network, or the WAP itself.

[57] B. Roy, Z. Ivanic, P. Windover, A. Ruder, and M. Shirk, "New York State EV Charging Station Deployment," World Electric Vehicle Journal, vol. 8, no. 4, pp. 877–887, Dec. 2016, doi: 10.3390/wevj8040877.

5. EVSE ASSESSMENTS

This project sought to improve the strategy for mitigating cybersecurity risk with multiple assessment activities that included visits to manufacturing facilities, development and testing labs, and assessments of fielded EVSE systems. This approach allowed the assessment team to identify potential vulnerabilities not only with the EVSE, but also potential vulnerabilities in supply chains, business operations, cloud systems, and development processes and procedures. Given the tightly coupled nature of the EVSE ecosystem, vulnerabilities in one area can affect multiple areas of the ecosystem. Potential attack paths that could be used to pivot between different areas of the ecosystem can be seen in Figure 4-1.

These assessments which included multiple, fielded EVSE systems allowed the assessment team to determine the most prevalent vulnerabilities across the industry. Then, by working closely with the appropriate EVSE vendors, the team could understand the risks these vulnerabilities posed to the EVSE and associated networks. In addition, since the team identified the potential to pivot between different areas of the ecosystem, the second year of this project focused on supporting IT systems. This focus was to identify vulnerabilities in remote access controls, the use of insecure protocols, and the ability to fingerprint devices from their online presence. This involved working with the threat models and attack graphs from year one and validating some of the approaches. The findings from these activities, which included network traffic analysis, forensic analysis, and open source information gathering, led to vulnerability enumeration in both the EVSE as well as their supporting infrastructure.

As part of the final year of this project, a list of best practices was generated from these assessments, shown in Figure 8-1. In addition, this document is providing an anonymized set of findings for distribution to the wider community. Recommendations on mitigating the various findings are included in Figure 8-2.

5.1. Anonymized Assessment Results

The results in this section have been anonymized to ensure malicious actors do not use these results to target specific makes or models of EVSE. However, the assessment team did provide detailed feedback with industry partners to ensure they could mitigate the weaknesses related to their EVSE and supporting IT systems.

This section covers the weaknesses discovered by the assessment team which are procedures, controls, implementation details, or vulnerabilities that could provide an attack vector, contribute to successful attacks using other vectors, or prevent the timely detection of an attack. These are provided to inform organizations about these risks and vulnerabilities to enable corrective actions.

Each weakness also includes a rating of High, Moderate, or Low to represent the team's overall evaluation of the severity of that specific weakness. To perform this evaluation, the team uses a modified version of the DREAD rating system. The DREAD system has five main questions:

- Damage – What level of damage could be expected from a successful attack?
- Reproducibility – What skill level is required to reproduce an attack?
- Exploitability – What skill level is required to perform the attack?
- Affected users – How widespread is the damage from the attack? (Single user/system, single facility, Domain-wide, etc.)
- Discoverability – What level of knowledge is required, or how difficult is it to discover the threat?

However, the assessment team goes beyond these basic questions to apply a variety of additional rating systems that are based on the adversary of concern and their motivations and capabilities; potential for alternative attack targets that could achieve the same goal; and other reality filters that are informed by their experience and threat intelligence. The outputs of these various rating systems are combined by the team members and relevant subject matter experts in a qualitative process to obtain the overall rating.

These weaknesses have been divided into four categories based on their location or role in the overall EVSE ecosystem. These categories are: Business Network & Operations, EVSE Security, EVSE Network and Operations, and Electric Vehicle Operations. Each of these categories is addressed in the corresponding sub-section below. Detailed information on the weaknesses, including the justification for the rating and discussion of the potential mitigations, can be found in Appendix A on Page 58.

5.1.1. Business Network & Operations

[A.1] (High) Software development practices do not utilize industry best practices.

[A.2] (Moderate) Physical security of some facilities could allow unauthorized access to EV chargers being tested, manufacturing areas, and office spaces.

[A.3] (Low) The state of the EVSE is not standardized when shipping across manufacturing locations.

5.1.2. EVSE Security

[B.1] (High) EVSE enclosures do not provide adequate physical protections against unauthorized access.

[B.2] (High) Login and provisioning credentials are posted inside the EVSE.

[B.3] (High) Internal information systems do not use encrypted hard drives.

[B.4] (Low) Debug ports and unused services are enabled.

5.1.3. EVSE Network & Operations

[C.1] (High) Verification of firmware and software is not performed prior to deployment and installation.

[C.2] (High) EVSE networks (internal and external) do not follow network security best practices.

[C.3] (High) EVSE providers utilize the same credentials throughout their charging network.

[C.4] (High) Default credentials are used on internal information system components.

[C.5] (High) Insecure remote access tools are used to configure and troubleshoot deployed EVSE.

[C.6] (High) EVSE are Internet connected and discoverable by search engines.

[C.7] (Moderate) Logs are stored locally instead of being uploaded for analysis

[C.8] (Moderate) Some EVSE equipment can be reflashed with a USB stick.

[C.9] (Moderate) Updates to the EVSE firmware and software are not routinely scheduled or deployed.

[C.10] (Moderate) EVSE use outdated and insecure protocol versions.

5.1.4. Electric Vehicle Operations

The team did not study electric vehicles as part of this assessment.

6. POWER SYSTEM CONSEQUENCES

With projections of high EV penetration in the US[58], it is imperative that studies are conducted to fully understand the effect of potential future cyber-attacks on EVs on the North American electric power system. Extreme fast charging stations are poised to provide high-power charging to rapidly meet the demands of light-duty passenger vehicles. Unlike low-power charging, high-power charging requires communication between vehicle and charger and charger and infrastructure to sequence and manage the charging process, along with local and distributed load management. This creates an interdependency between the historically distinct electrical and transportation systems. Consequently, the reach of and risk of power grids being manipulated and adversely affected by means of nefarious control and use of modern communications systems are significantly increased.

6.1. Transmission Impacts

The team explored the impact of load manipulation on the power grid with high-power charging infrastructure using a full Western Electricity Coordinating Council (WECC) planning model. Two different types of studies were conducted: a large discrete WECC-wide EV load drop across the region intended to raise frequency, and several smaller EV load modulation events intended to excite system inter-area oscillations along the California Oregon Intertie (COI). PNNL's Consequence Analysis results indicated for the specific events studied in this work, the impact on the WECC system is minimal. The events would likely induce additional stress, complicating grid management and operations. Furthermore, they may also trigger generator protective relaying causing some generators to trip offline.

A significant amount of bulk-grid generation resource protection is modeled within the WECC planning case. While there are North American Electric Reliability Corporation (NERC) requirements to stay online during transient events, these requirements are *only* applicable to transmission components that meet the Bulk Electric System (BES) definition[59], which includes 1) facilities operating at 100 kV and above and 2) generator connected at a high-side voltage of 100 kV and above. For the latter, these generators must also be greater than 20 MVA nameplate for a single generator or greater than 75 MVA nameplate for the entire generation facility. For this reason, only the protections on BES elements are considered. PRC-024-2[60], developed by NERC, defines generator frequency and voltage protective relay ride-through settings. However, ride-through settings only regulate when generation *must* stay online. Additional or more restrictive voltage protective settings than those in the original base case WECC planning model are not included. Only BES generator bus frequency and voltage are monitored in this work.

In addition to a discrete, system-wide load drop event, a second potential concern is the modulation of loads (i.e., switching loads off and on) targeting the grid resonant frequencies. In this scenario, a single load, or potentially many loads at critical locations, are modulated with the purpose of exciting an existing inter-area oscillation mode on the electric power grid. Inter-area oscillations on an electric power grid are typically characterized by one set of generators oscillating against a second set of

[58] Edison Electric Institute, "Electric Vehicle Sales Forecast and the Charging Infrastructure Required Through 2030," 2018.
[59] NERC, "Bulk Electric System Definition Reference Document v2," 2014.
[60] NERC, "Standard PRC-024-2 — Generator Frequency and Voltage Protective Relay Settings," Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-024-2.pdf. [Accessed 7 Aug 2019].

generators through a weak electrical connection at relatively low frequency (0.15 to 1.0 Hz)[61]. The generators oscillating against each other can in turn cause elevated powerflows on the tie lines connecting them.

In the single, large, discrete, simultaneous load drop occurring across the Western Interconnect (WI), minimal generation tripping occurs on smaller units and some load shedding occurs because of the composite load model's internal protection and load modulation. The frequency and voltage at BES generator buses, except for one bus, stay within reasonable per unit ranges of 0.9 to 1.1 after the event.

The second simulation considers load modulation. A forced oscillation using load is applied with the intention of targeting a natural frequency of the system, specifically, an inter-area oscillation. Inter-area oscillations put the grid in an elevated state of risk during system events, causing protective actions[62] or making it difficult to achieve ideal transfer capacities and optimal power flows[63]. For the simulations under study, *impact factor*, defined as

$$IF = \frac{\text{peak} - \text{to} - \text{peak path flow (MW)}}{\text{controllable load (MW)}}$$

is used to measure the relative increase in power flows along the COI given a specific amount of modulated load. The peak-to-peak path flow is the maximum observed flow minus the minimum observed flow over a 10-second window on the COI, where the system response has reached a steady-state magnitude. For example, a 1000 MW oscillation on the COI given 500 MW of modulated load would correspond to an impact factor of 2.

There are two operating conditions considered, one with Alberta connect and another where Alberta is disconnected. The overall system stability condition changes with the presence of Alberta. With Alberta connected, impact factors are observed on the COI of ~2.5 and ~1. 5 for single-point and multipoint events. For simulations with Alberta disconnected, the impact factors observed are still elevated but much smaller than with Alberta connected. Single-point and multipoint events resulted in impact factors of ~1.4 and ~1.15 on the COI.

The transmission studies did not find significant adverse effects caused by the events in the scenarios. While there was some generation and distributed load tripping in the static load drop event and impact factors of ~2.5 on the COI in the dynamic single-point load modulation event, neither of these by itself appears to cause significant system-wide cascading outages. The authors recognize that the full space of potential power system events due to controlling load is larger than the scope of the studies, however, and future work should focus on understanding better the full space of load modulation events with respect to EV infrastructure to try to determine the extent of their impact on bulk electric power grids.

---

[61] North American Electric Reliability Corporation, "Reliability Guideline Forced Oscillation Monitoring & Mitigation," North American Electric Reliability Corporation, 9 2017. [Online]. Available: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_Forced_Oscillations_-_2017-07-31_-_FINAL.pdf. [Accessed 10 2020].

[62] D. N. Kosterev, C. W. Taylor and W. A. Mittelstadt, "Model Validation for the August 10,1996 WSCC System Outage," IEEE Transactions on Power Systems, vol. 14, no. 3, pp. 967-979, 1999.

[63] J. Lian, S. Wang, M. A. Elizondo, J. Hansen, R. Huang, R. Fan, H. Kirkham, L. D. Marinovici, D. Schoenwald and F. Wilches-Bernal, "Universal Wide-area Damping Control for Mitigating Inter-area Oscillations in Power Systems," US Department of Energy, 2017.

6.1.1. Load Drop Scenario

The team evaluated worst-case scenarios in which EV loads were manipulated on a realistic 20,000+-bus representation of the WECC simulated in PowerWorld's simulator software. The model contained a high-fidelity composite load model that represented motors, lighting, electronic, and associated distribution feeders. The team focused on the stability of the WECC model following the sudden loss of forecasted XFC load. Impacts are analyzed for load distributed system-wide and for load localized in specific areas of interest.

An EV load forecast was adapted from Kinter-Meyer *et al.*[64], which projects electric vehicle loads in the year 2028. This is based on the work of EPRI[65] and corresponds to 23.6 million electric vehicles nationwide. The 2028 WECC case used by Kinter-Meyer divides load onto 41 different areas typically used in WECC's production cost model simulations. The charging was predominately L2, home and work applications; DCFC was limited and consists of a worst-case 22 percent of the peak load demand. This work creates a mapping to translate the EV load in those 41 different load areas into a new set of 22 load areas used by this works' transient simulations. After obtaining EV load by area for the transient simulations, we scaled the size of the total EV load to match the medium trend given by Kinter-Meyer of 10.8 million electric vehicles nationwide forecasted for 2028. WECC's incremental evening peak load attributed to EV charging is 18,768 MW, so we calculated our new WECC incremental peak EV load as ~8,600 MW, based on the prior work. Finally, within each transient simulation load area, each downsized cumulative EV area load was added to its corresponding area base case load by scaling the total load size in each area to match the area base case load plus the addition of the downsized EV area load.. The distribution of the additional 8,600 MW load across the continental United States in the WECC model by percent is shown in Figure 6-1 with the 22 transient load areas given across its x-axis. New EV loads are added to the base case powerflow used by transient simulations by iteratively adding load and solving the new powerflow configuration. It should be noted that one limitation of the dataset used by Kinter-Meyer *et al.* is that it only considers EV load in the continental United States.

[64] M. Kinter-Meyer, S. Davis, S. Sridhar, D. Bhatnagar, S. Mahserejian and M. Ghosal, "Electric Vehicles at Scale – Phase I: High EV Adoption Impacts on the Western U.S. Power Grid," PNNL, Richland, 2020.

[65] M. Alexander, "Plug-in Electric Vehicle Market Projections. Scenarios and Impacts, 3002011613," Electric Power Research Institute, Palo Alto, CA, 2017.

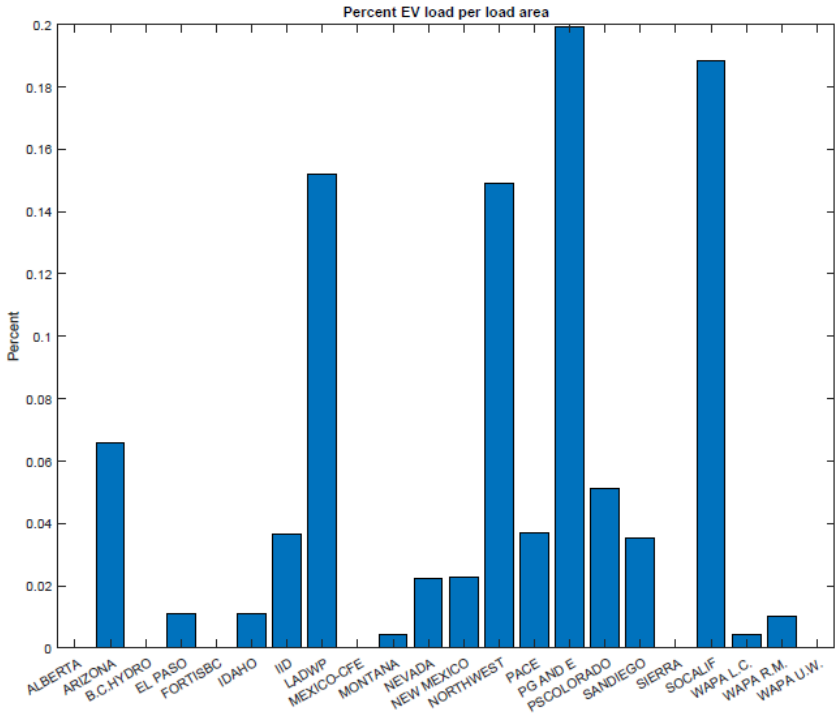

Figure 6-1. Percent EV load distributed to each load area in 2028 WECC planning model.

For discrete load drop studies, approximately 8,600 MW of EV load was lost and observed for 10 seconds to capture the main features of the initial dynamic response, which include inertia and governor response.

The case is configured with several modifications to transformer tap ratios and automatic voltage regulation after adding the EV load to lower several system initial voltages. This same effect might also be achieved with appropriate generator redispatch. Frequency and voltages and voltage deviations from initial voltages corresponding to BES generators (>20 MVA base values) with positive MW output are given in Figure 6-2, Figure 6-3, and Figure 6-4. As a result of the 8,600 MW load drop, there is some relatively small generator and load losses due to their respective generator and load protective systems (~30 MW of total generation and ~466 MW of total load). The full WECC system case prior to the event has ~169 GW of generation production servicing ~163 GW of load so the percent of the WECC's generation and load dropped due to protective systems with respect to the pre-event system state values are both less than 0.3%.

While generation trips, the generators are small and their absence has negligible effect on the security of the BES. As previously stated, the largest generator tripped is less than 6 MW. In Figure 6-2 and Figure 6-3, the system's frequency and voltage response for the generator buses producing power with BES generators attached are observed. In terms of frequency, at no point do any bus frequencies approach the PRC-024-2 BES's lowest over-frequency threshold of 60.6 Hz, which has a ride-through duration of 180 seconds. Keep in mind the starting case is a heavy summer case that is already stressed. Some of the BES generator bus voltages near the fringe of 0.9-1.1 pu may be allowed to run at higher or lower voltages under close surveillance during peak operating conditions. In Figure 6-3, a single voltage just under 0.9 pu gets pushed above 0.9 pu by the event. Given the overlap of voltage trends in Figure 6-3, Figure 6-4 helps visualize the range of voltage deviations during the event. Ultimately,

the impact to customers is minimal and the generator controls are expected to fully compensate for the XFC disconnect disturbance.

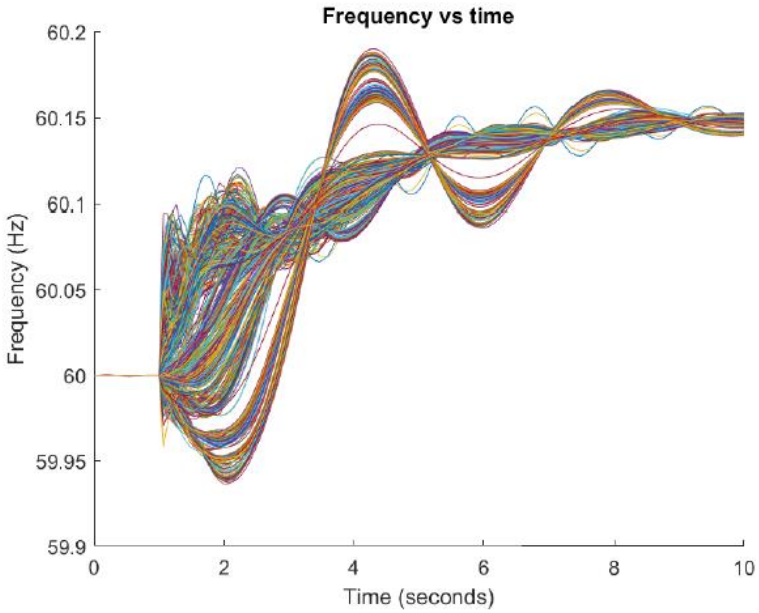

Figure 6-2. Frequency vs. time for operational BES generator buses with >20 MVA base.

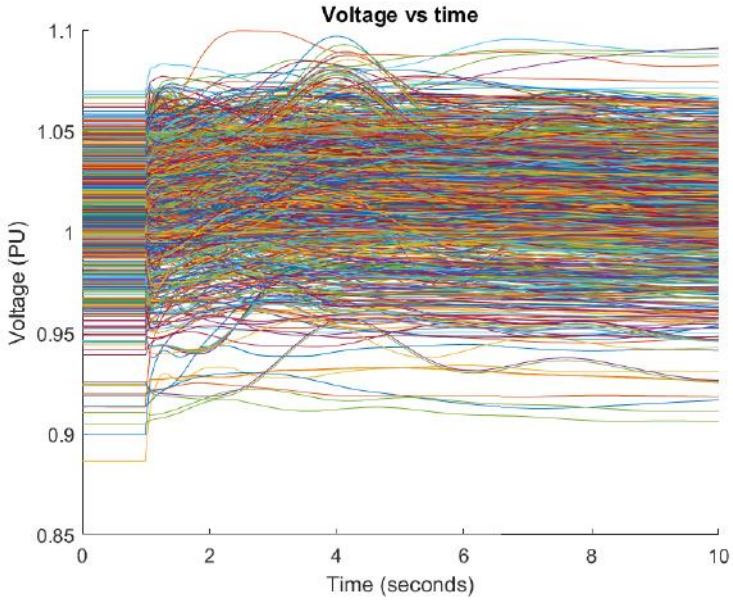

Figure 6-3. Voltage vs. time for operating BES generator buses and >20 MVA base.

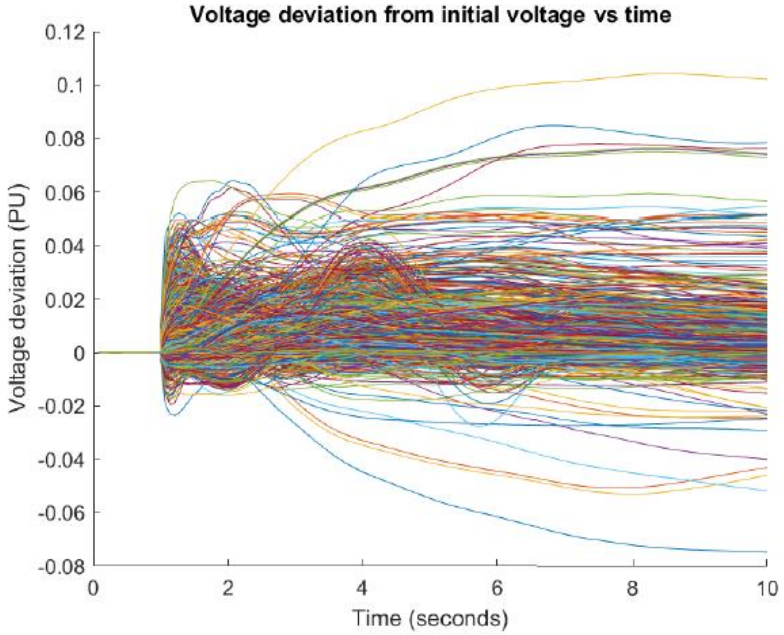

Figure 6-4. Voltage deviation vs. time for operating BES generator buses and >20 MVA base.

6.1.2. Load Modulation Event Scenarios

Inter-area modulations have occurred in both the Western Interconnection (WI) and Eastern Interconnection (EI). For example, in 2005, a failed control system at a power plant in Alberta, Canada, resulted in a 20 MW peak-to-peak forced oscillation close to the WI's resonant frequency. This forced oscillation resulted in 200 MW of peak-to-peak oscillations on the California Oregon Intertie[66]. Similarly, in 2016, a 200 MW forced oscillation at Grand Gulf Nuclear Station in Mississippi occurred because of a failed control system. This fault caused a 40 MW New York tie line oscillation approximately 1,400 miles away[67].

With regard to the WI case, the system simulated in this work, a variety of modes have been reported; however, the two dominant modes are typically labeled the North-South A (NSA) mode and North-South B (NSB) mode[68]. The NSA mode is a lower frequency mode that primarily involves generators in Alberta oscillating against generators in Southern California and the United States Southwest. The NSB mode is higher frequency than the NSA mode and includes generators in British Columbia, the Pacific Northwest, Montana, and Northern California oscillating against generators in Southern California, the United States Southwest, and Alberta[69]. A consequence of generators in the north oscillating against generators in the south is fluctuations in the powerflows along the lines connecting the generators. A good location to monitor the power fluctuations caused by the NSA and NSB is

[66] North American Electric Reliabiltiy Corporation, "Interconnection Oscillation Analysis: Reliability Assessment," North American Electric Reliabiltiy Corporation, 11 2018. [Online]. Available: https://www.wecc.org/Administrative/InterconnectionOscillationAnalysis.pdf. [Accessed 10 2020].
[67] Ibid.
[68] D. Trudnowski, "wecc.org," WECC, 2012. [Online]. Available: https://www.wecc.org/Reliability/WECCmodesPaper130113Trudnowski.pdf. [Accessed 10 2020].
[69] Ibid.

along the California Oregon Intertie (COI), a critical WECC path, which is approximately the midpoint between the affected generation. WECC paths are a simplified way of describing flows between regions of a power system and consist of aggregations of transmission lines transferring power from one region to another[70]. The COI, or path 66, consists of three 500 kV transmission lines which are largely responsible for connecting and transferring power between Southern Oregon and Northern California. Studies addressing forced load manipulation with the intent of adversely affecting the power grid tend to fall into several classifications[71] listed below:

- Static vs. dynamic: Static load manipulation refers to discrete one-time load modification events, whereas dynamic load manipulation[72,73] may vary load magnitude through time.
- Single point vs. multipoint: Single point studies[74] evaluate load manipulation at a single bus, while multipoint studies allow load manipulation simultaneously at multiple buses.
- Open loop vs. closed loop: Closed loop load manipulation uses sensors to monitor some aspect of the system state when determining how to change system load, while open loop load manipulation does not[75].

Load manipulation studies also tend to focus on some combination of design and demonstration of load manipulation methods[76,77] or extend these studies to detection/mitigation of load manipulation[78,79,80]. This study evaluated both static and dynamic load manipulation from both single and multipoint perspectives using an open loop control. In terms of model fidelity, the model differentiates itself from earlier studies in that (a) it uses a full 20,000+ bus WECC planning model with an AC powerflow, (b) it includes standard machine controls with machine, governor, exciter, and power system stabilizer models[81], and (c) it contains models for remedial action schemes and standard

---

[70] Western Electric Coordinating Council, "WECC Joint Synchronized Information Subcommittee," Western Electric Coordinating Council, 11 2013. [Online]. Available: https://www.wecc.org/Reliability/WECC%20JSIS%20Modes%20of%20Inter-Area%20Oscillations-2013-12-REV1.1.pdf. [Accessed 11 2020].

[71] Western Electric Coordinating Council, "WECC Joint Synchronized Information Subcommittee," Western Electric Coordinating Council, 11 2013. [Online]. Available: https://www.wecc.org/Reliability/WECC%20JSIS%20Modes%20of%20Inter-Area%20Oscillations-2013-12-REV1.1.pdf. [Accessed 11 2020].

[72] S. Amini, F. Pasqualetti and H. Mohsenian-Rad, "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes," IEEE Trans. Smart Grid, vol. 9, no. 4, pp. 2862 - 2872, 2018

[73] H. E. Brown and C. L. Demarco, "Risk of Cyber-Physical Attack via Load With Emulated Inertia Control".

[74] S. Amini, H. Mohsenian-Rad and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington DC, 2015.

[75] Ibid.

[76] 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.

[77] A. Patel and S. Purwar, "Destabilizing smart grid by dynamic load altering attack using PI controller," in International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, 2017.

[78] R. Germana, A. Giuseppi and A. Di Giorgio, "Ensuring the Stability of Power Systems Against Dynamic Load Altering Ensuring the Stability of Power Systems Against Dynamic Load Altering," in *European Control Conference*, Saint Petersburg, 2020.

[79] S. Yankson and M. Ghamkhari, "Transactive Energy to Thwart Load Altering Attacks on Power Distribution Systems," Future Internet, vol. 12, no. 1, 2019.

[80] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 667 - 674, 2011.

[81] Exciters are an important control system for maintaining power system stability in that they can be used to automatically control voltage at a generators terminal. Power system stabilizers also promote system stability, specifically

generation protection provided in the WECC planning model. Furthermore, this work introduces and tests a heuristic method for discovering high-impact candidate buses for load manipulation based on frequency response and applies it to a 2028 EV forecast based on early work[82,83]. The transmission study is adapted from prior work[84] but improves simulations by moving simulations to a 2028 system instead of a 2018 system, updates the EV forecasting method to better represent regional differences in EV penetration, and tests both load drop and load modulation simulations.

There are advanced controls in BES generation known as Power System Stabilizers (PSS) that modulate the power output of the generator out of phase with a sensed oscillation. In this way, the PSS makes the generator "resist" changes in the system causing a positive impact on system damping. With all generation in the BES having the PSS enabled, the overall damping for the system may result in the limited response, such that oscillating the loads at resonant frequencies may not result in significant power system inter-area oscillations. It has also been demonstrated that system topology[85] can also significantly affect system damping. To examine the scenario most likely to cause issues, we simulated topologies that resulted in lower system damping.

To analyze the risk, the following analysis was performed:

1. Exposes the system to a discrete event. For this work, a 1,000 MW braking resistor was used as the discrete event.
2. System modes are determined using PowerWorld's modal analysis tool by analyzing 500 kV bus voltage angle profiles generated in step 1 using PowerWorld's iterative matrix pencil algorithm. Key outputs of the modal analysis include estimates of damping percent, frequency, and the magnitude of the mode's real portion of its eigenvalue.
3. Expose the system to a forced oscillation of 500 MW at one of the discovered modal frequencies by modeling at load at a single bus in the system. Given the well-known NSA and NSB modes of the WI, we chose a bus in southern California as this area contains one of the oscillating sets of generators for both modes and is an area of potentially high EV growth.
4. Analyze single load modulation by looking at the frequency response of all load buses and ranking them according to the magnitude of their frequency deviations. Select the bus that appears to be most affected by the modulated 500 MW load selected in step 3.
5. Simulate the system with sensitive load buses modulated at the mode of interest.

Simulations were conducted on the WI with Alberta connected and disconnected. The team studied the North-South Mode A with the following parameters:

1. Simulations on full WI investigating North-South Mode A
    a. Single-Load Southern California (SLSC): 500 MW oscillating a single bus. This bus was in Southern California.

by damping local and interarea oscillations, which is accomplished by providing an additional input to a generator's exciter.

[82] M. Alexander, "Plug-in Electric Vehicle Market Projections. Scenarios and Impacts, 3002011613," Electric Power Research Institute, Palo Alto, CA, 2017.

[83] M. Kinter-Meyer, S. Davis, S. Sridhar, D. Bhatnagar, S. Mahserejian and M. Ghosal, "Electric Vehicles at Scale – Phase I: High EV Adoption Impacts on the Western U.S. Power Grid," PNNL, Richland, 2020.

[84] J. G. O'Brien, P. R. Maloney, U. Agrawal, T. E. Carroll and R. M. Pratt, "Electric Vehicle Infrastructure Consequence Assessment - Revision 2. PNNL-29514," Pacific Northwest National Laboratory, Richland, WA, 2020.

[85] Y. Chen, J. Fuller, R. Diao, N. Zhou, Z. Huang and F. Tuffner, "The influence of topology changes on inter-area oscillation modes and mode shapes," in 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, 2011.

b. Single-Load Frequency Response (SLFR): 500 MW oscillating load at bus with largest frequency response. This bus is in Alberta, Canada.
c. Distributed-Load Frequency Response (DLFR): 500 MW of oscillating load at 20 buses each of size 25 MW. Phase groups in the ranges $140 < \theta < 150$ and $330 < \theta < 350$ were chosen based on several tests.

2. Simulations on WI with Alberta disconnected
   a. SLSC: 500 MW oscillating a single bus. This bus was in Southern California.
   b. SLFR: 500 MW oscillating load at bus with largest frequency response. The bus was in British Columbia, Canada.
   c. DLFR: 500 MW of oscillating load at 20 buses each of size 25 MW. Phase groups in the ranges $170 < \theta < 190$ and $340 < \theta < 360$ were chosen based on several tests.

Figure 6-5 illustrates the concept of the Distributed-Load Frequency Response studies: the green and blue dots indicate a distributed load to modulate on either side of the COI. The graph above the map shows that the loads are ~180 degrees out of phase. Conceptually, if loads in the north are high and loads in the south are low, this will create a flow north along the COI. Similarly, when loads are low in the north and high in the south, this will tend to generate flows south along the COI.

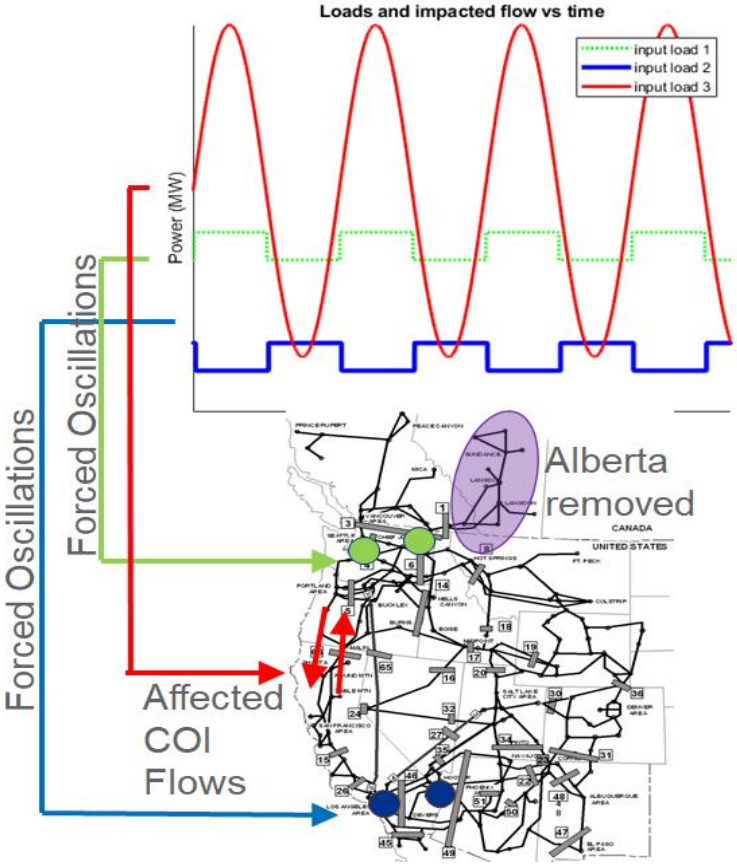

Figure 6-5. Load oscillation simulation.

Load modulation simulations were conducted over a 50-second interval to allow the impact of low-frequency oscillations to reach an approximate steady-state response. Inter-area oscillations, the feature of interest in these studies, are well documented as taking place within the 0.15-1.0 Hz range.

The impact factor, defined as the peak-to-peak path flow divided by controllable load, is shown in Figure 6-6. For simulation set 1, we observe an impact factor of slightly less than 0.75 on the COI for 1-SLSC when choosing a bus in Southern California to place 500 MW of modulated load. However, in 1-SLFR and 1-DLFR, where loads are selected by the frequency analysis method, we observe elevated COI flows. 1-SLFR has the largest impact factor of almost 2.5, while 1-DLFR has an impact factor of almost 1.5. These results indicate that modulating relatively low levels of load can have significant impact on system flows. We also observed that other critical WECC paths also experience oscillating power flows; however, the COI oscillations appear to be the most pronounced.

In simulation set 2, slightly elevated impact factors are observed in 2-SLFR and 2-DLFR, but they are significantly smaller than those found in 1-SLFR and 1-DLFR. In 2-SLSC, an impact factor of slightly less than 1 is observed on the COI when choosing a bus in southern California to place 500 MW of modulated load. However, in 2-SLFR and 2-DLFR, COI flow impacts larger than 1 are observed. In 2-DLFR, the impact factor comes out to ~1.15, and in 2-SLFR, the impact factor is almost 1.4.

In simulation sets 1 and 2, placing all 500 MW of modulated load on a single bus has the largest impact factor (SLFR) when choosing buses with the largest frequency response. However, both distributed load modulation events (DLFR) resulted in minor load shedding because of the composite load model's internal protection, shown in Table 2. This lends credibility to the feasibility of being able to adversely affect the grid by coordinating many smaller loads rather than by using a large single load. A distributed event with many smaller loads instead of a single large load is also likely easier to map to real EV loads on the power system.

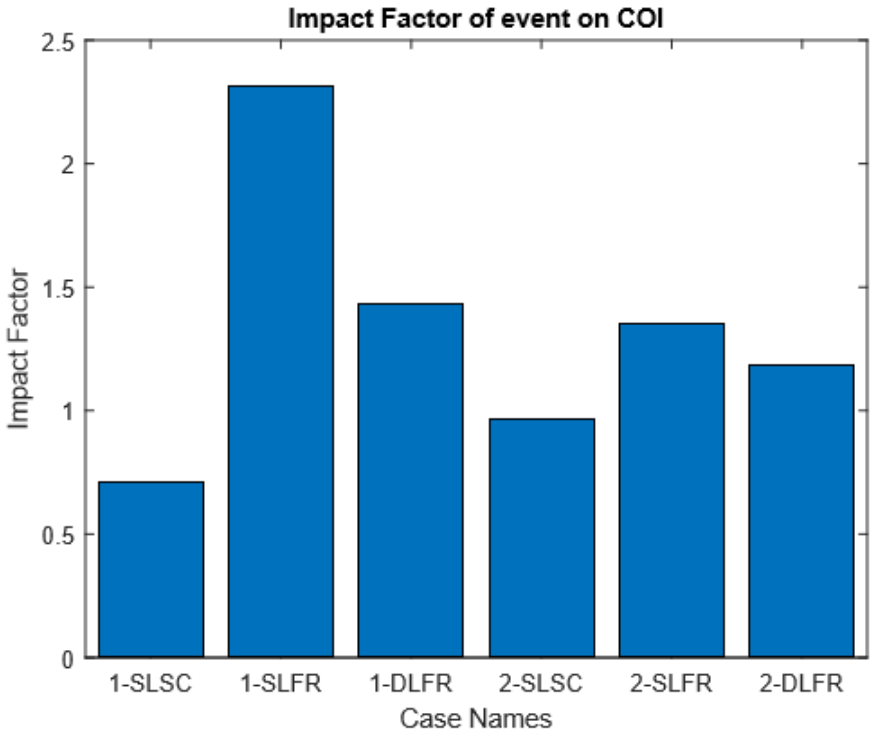

Figure 6-6. Impact factors by case names

Table 2: Summary of generation and load tripped for the load modulation in simulations.

Case	Generation Tripped (MW)	Load Tripped (MW)
1–Single Load Southern California (SLSC)	0.0	0.0
1–Single Load Frequency Response (SLFR)	0.0	0.0
1–Distributed Load Frequency Response (DLFR)	0.0	22.2
2–Single Load Southern California (SLSC)	0.0	0.0
2–Single Load Frequency Response (SLFR)	0.0	0.0
2–Distributed Load Frequency Response (DLFR)	0.0	19.9

No significant adverse effects were observed in either set of simulations, however, COI flows of 2x the oscillating load size were observed in the load modulation studies and approximately 20 MW of load was dropped in the DLFR cases. No generation tripped, there would be no significant system-wide cascading outages, and the system should quickly recover from this event. Inter-area oscillations are currently monitored operationally and are of concern in that they put the grid in elevated state of risk during system events as well as making it difficult to achieve ideal transfer capacities and optimal power flows.

Furthermore, several aspects of coordinating a SLFR or DLFR were not considered in this work. Physically coordinating a successful SLFR or DLFR must consider:

- That resonant modes of a grid change as system topology, dispatch, and load changes throughout the day.
- For DLFR, correctly accounting for latencies in control signals to ensure loads are being modulated at the correct times is important as significant offsets from the resonant frequency across the controlled loads would attenuate system oscillations.
- The following work assumes a step function is possible for modulating load whereas electric vehicle chargers ramp up to their peak MW transfer capacity over time. Thus, the amount of EV chargers required to approximate the amplitude of a step function is significantly larger than their MW capacity. The longer the ramp up time, the greater the number of EV chargers required.

However, despite these challenges, as EV charging load increases and its technology continues to mature, further transient simulation studies should be considered to ensure the system is not vulnerable to these types of attacks.

6.2. Distribution Impacts

In addition to bulk power system impacts, it is possible that EVSE operations at the distribution level could result in poor power quality. The largest risk is that voltages will be perturbed to levels that increase equipment wear, trip DER equipment, or decrease power delivery efficiency from low power factors. EVSE misoperation that causes voltages to reaching levels that cause pumps to stall or other load failures is unlikely as utility planning will prevent these significant issues by installing appropriate voltage regulation equipment like on-load tap-changers in transformers and capacitor banks.

Two distribution studies were conducted to understand the risk of cyberattack or other misoperation of EVSE equipment at the distribution level using EPRI's Open Distribution System Simulator (OpenDSS):

8. Four-quadrant vehicle-to-grid (V2G) EVSE stations were operated at different power factors at the end of a rural feeder.
9. The voltage oscillations from the transient model were modeled at the distribution system to investigate the potential to trip distributed energy resource (DER) equipment interconnected to the distribution system.

These scenarios are presented in the following subsections.

6.2.1. Vehicle-to-Grid EVSE at End of Feeder

To better understand the impact on the distribution power system for different penetrations of EVSE and attack strategies, simulations were conducted on a rural 12 kV distribution feeder in a highly commercial load area. The OpenDSS model contained 215 buses and 39 service transformers and was run for 3-minutes for different charging profiles with reactive power support functionality. The feeder voltage was regulated via substation transformer load tap changer (LTC). Nine 250 kW, 3-phase, 480 V stations were simulated at the end of the feeder. Scenarios included 2.25 MW charging sequences with and without V2G capabilities to generate high and low feeder voltages during peak and min load periods. XFC charging was limited to the SAE J2894/1 ramp rate of 40 amp/sec (i.e., EVSE reached full output in ~13 seconds).

The results for steady-state charging and discharging with different power factors are shown in Figure 6-7. The "+0.85 PF Charge+Discharge" scenario was designed to cause the worst overvoltage profile by first charging the EVs, which caused the LTC to tap up, and then discharging the EVs to drive the voltage higher than the steady state solution. In multiple scenarios, the distribution voltage profile exited ANSI C84.1 *American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hz)* voltage ranges. In those cases, the utility would be in violation of the standard, and the high and low voltage cases would likely accelerate degradation of loads and decrease the overall efficiency of power delivery[86], but there would be no impact on grid reliability or resilience from such an event. It's important to note this is an extreme case, in which all chargers are in use at the same time and all the stations are located at the end of the feeder.

[86] R. Seguin, et al. "High-Penetration PV Integration Handbook for Distribution Engineers," NREL/TP-5D00-63114, January 2016.

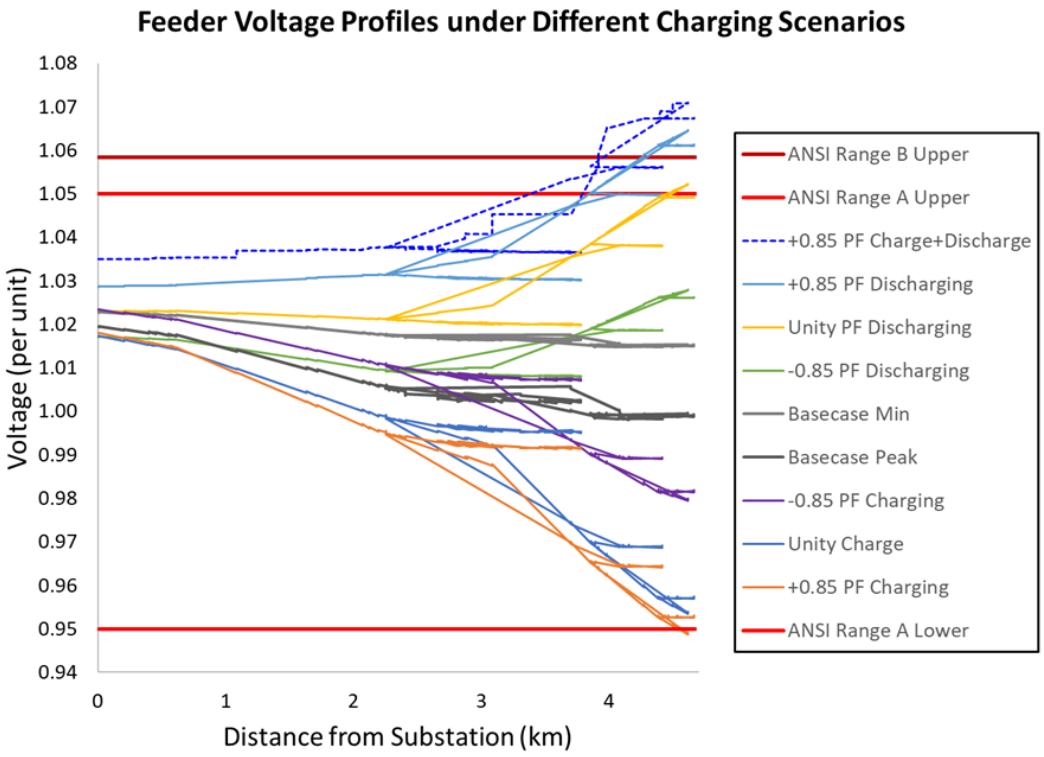

Figure 6-7. Different distribution voltage profiles for coordinated charging/discharging of EVSE totaling 2.25 MW.

6.2.2. Oscillations on the Distribution System

There was a concern that the transmission system oscillations from Section 6.1.2 could lead to DER devices tripping and cause greater grid instabilities. To predict the distribution voltage profiles from those transmission events, OpenDSS time-series simulations were conducted on 10 representative feeders located in the U.S. with the transmission voltages presented at the primary coil of the distribution substation transformer. The impacts were studied with quasi-static time series (QSTS) power flow simulations[87] on the distribution feeder models. The highest (NWV_RES) and lowest (RMN_RES) transmission bus voltage profiles were chosen to simulate the most extreme voltages possible on the high-side of the distribution transformer, as shown in Figure 6-8. Ten anonymous distribution feeders obtained from various utilities within the WECC were studied for both the highest and lowest impact voltages. To produce the highest voltage possible, the highest voltage point on the feeder, usually the feeder head, was monitored under simulation of the feeder minimum demand coupled with the highest transmission voltage profile. By contrast, the lowest voltage point on the feeder, usually the end of a secondary service line, was monitored under the peak feeder demand with the lowest transmission voltage profile implemented.

[87] R. J. Broderick, J. E. Quiroz, M. J. Reno, A. Ellis, J. Smith, and R. Dugan, "Time Series Power Flow Analysis for Distribution Connected PV Generation," Sandia National Laboratories SAND2013-0537, 2013.

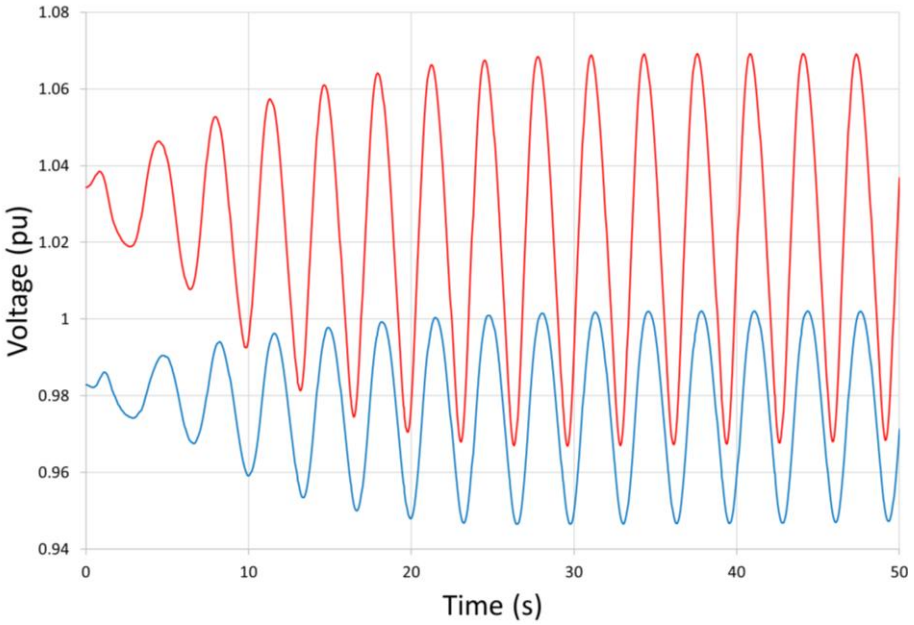

Figure 6-8. The highest (NWV_RES) and lowest (RMN_RES) of the transmission voltage profiles used in the distribution system simulations.

The QSTS simulations were set up to run for the 50 seconds recorded from the transmission voltage profiles with a resolution of 15 points/second (~66.667 ms time step). The 15-minute or 30-minute resolution load demand data for the feeder models was selected to produce the highest and lowest distribution voltages. Control settings such as those for voltage regulators and switching capacitors remained active during the simulations, allowing for regulation changes when appropriate. The four following cases were simulated for each feeder and results recorded:

1. Peak load with low transmission voltage profile
2. Minimum load with high transmission voltage profile

The voltage profiles at all the critical points on the feeders were recorded for the four cases simulated on each feeder. From these, the highest and lowest voltage levels observed in the transmission voltage profile cases were recorded. Table 3 lists the maximum and minimum voltages recorded for the 10 study feeders, in order of highest to lowest maximum voltage, identified by the public code names used by Sandia.

Table 3. Maximum and minimum voltages recorded for each study feeder in per unit.

Public Name	Maximum Voltage Recorded (pu)	Minimum Voltage Recorded (pu)
DA2	1.090	0.833
DV1	1.077	0.917
QN1	1.061	0.894
QB1	1.061	0.902
UT16	1.060	0.944
DC2	1.058	0.944
DA1	1.055	0.929
QL1	1.047	0.855
QL2	1.045	0.919
DC1	1.045	0.912

As shown in Table 1, feeder "DA2" experienced both the highest and lowest voltages recorded across all simulations. This could be due to several factors, including it being a long feeder with high impedance conductors requiring multiple line voltage regulators along the backbone of the feeder to maintain acceptable voltages. It shows some pre-existing voltages outside of the ANSI Range A limits, but these can be acceptable, especially those above the upper limit where no loads are served, for the sake of maintaining service voltages. Figure 6-9 is a plot of the highest and lowest point voltage profiles for DA2 under the implementation of the transmission voltage profiles.

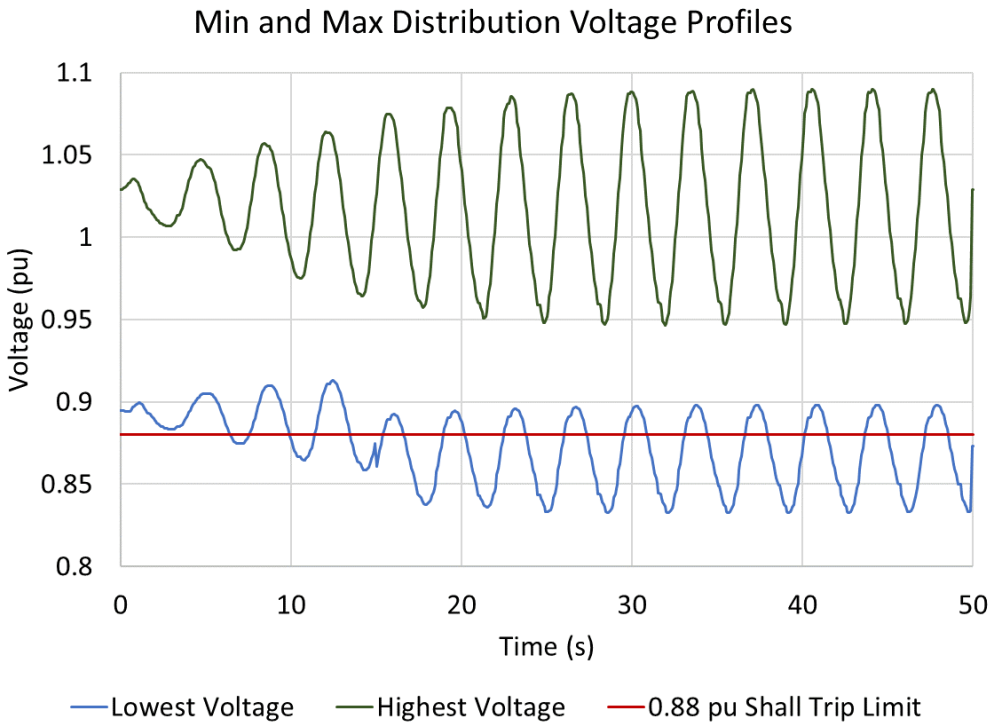

Figure 6-9. Highest and lowest voltage profiles for feeder DA2 under the implementation of the transmission voltage profiles.

The must-trip requirements for DER equipment is defined in the US Interconnection Standard, IEEE 1547. Legacy equipment would be listed to the requirements in either IEEE 1547-2003 or IEEE 1547a-2014, whereas new products will be listed to requirements in IEEE 1547-2018. Each of these standards include requirements for when DER equipment must trip due to abnormal voltage conditions. The default settings for each of these standards is included in Table 4. The Area Electric Power System (EPS) operator may extend the trip times in the cases of IEEE 1547a and IEEE 1547-2018 devices. IEEE 1547-2018 also includes different categories of DER equipment based on their fault response characteristics. Cat I and II are typically associated with synchronous or other non-inverter-based generators. Cat III is for inverter-based DER equipment. Since Cat III devices are far more common on distribution systems and because their requirements for tripping are more stringent, they are included in Table 4.

Table 4: Must trip requirements for DER equipment for abnormal voltage conditions.

IEEE 1547-2003		IEEE 1547a-2014		IEEE 1547-2018, Cat III	
Voltage (% of base)	**Clearing time (s)**	**Voltage (% of base)**	**Default Clearing time (s)**	**Voltage (% of base)**	**Default Clearing time (s)**
V<50	0.16	V<45	0.16	V<45	2.00
50≤V<88	2.00	45≤V<60	1.00	50≤V<88	21.00
110≤V<120	1.00	60≤V<88	2.00	110≤V<120	13.00
V≥120	0.16	110≤V<120	1.00	V≥120	0.16
		V≥120	0.16		

As can be seen from Figure 6-9, legacy and newly installed DER equipment will not trip from overvoltage conditions since the voltages do not exceed 1.1 pu. However, the voltage does dip below 0.88 pu for 2.07-2.20 seconds for some of the oscillations—as shown by the *0.88 pu Shall Trip Limit* line in Figure 6-9—so legacy DER equipment may trip offline if they were interconnected at the end of the feeder under the load modulation transmission attack scenario. Note this is the worst-case scenario for both the transmission and distribution cases. At the distribution level, only one of the feeders had a voltage below 0.88 pu for longer than 2.0 seconds and this was under the worst loading case and at the end of the feeder. Therefore, it can be concluded that there is virtually no risk of DER equipment tripping from a load modulation event.

7. POWER SYSTEM RISK

The project team has evaluated probable attacks based on hands-on cybersecurity assessments with partner organizations and evaluated the probability of success against the skill level required to conduct the attack. For each theoretical attack scenario, the likelihood of success and potential power system impact were used to estimate risk using the basic premise that risk is a function of probability and impact. The probability was estimated from the attack graphs and red team assessments; and the impact or consequence was determined from power system simulations.

Likelihood (Threats + Vulnerabilities)	Consequence (Power System Impact)					
		Insignificant No Observable Impact to Power System	**Minor** Local Power System Impacts	**Moderate** Regional (Distribution) Blackout	**Major** Widespread (Transmission) Blackout	**Severe** Widespread Outage for Extended Period
	Almost Certain Vulnerability Exploitable By Attacker: Script Kiddie Funding: None Time: Days	Medium	High	High	Extreme	Extreme
	Likely Vulnerability Exploitable By Attacker: Skilled Actor Funding: Little Time: Weeks	Medium	Medium	High	Extreme	Extreme
	Possible Vulnerability Exploitable By Attackers: Moderately-Skilled Team Funding: Some Time: Months	Low	Medium	Medium	High	Extreme
	Unlikely Vulnerability Exploitable By Attackers: Skilled Team Funding: Substantial Time: Years	Low	Low	Medium	High	High
	Rare Vulnerability Exploitable By Attackers: Nation State Funding: Substantial Time: Decades	Low	Low	Low	Medium	High

Figure 7-1. EVSE Cybersecurity Risk Matrix

Figure 7-1 shows the risk matrix. The likelihood axis advised by the work of Matesk et al.[88] and Duggan et al.[89] The consequence axis was advised by the power system simulations in Section 6 and prior work on assessing the power system impact from distributed energy systems[90]. It should be noted that there are many other impacts outside of the power system that should be considered when considering

[88] M. Mateski, et al. "Cyber Threat Metrics" SAND2012-2427.
[89] D.P. Duggan, S.R. Thomas, C.K.K. Veitch, L. Woodard. "Categorizing Threat: Building and Using a Generic Threat Matrix." SAND2007-5791.
[90] J. Johnson, et al., "Power System Effects and Mitigation Recommendations for DER Cyber Attacks," IET Cyber-Physical Systems: Theory & Applications, Jan 2019.

a more comprehensive risk assessment. These would include damage to equipment, personnel safety risks, denial of charging, data theft, etc.[91]

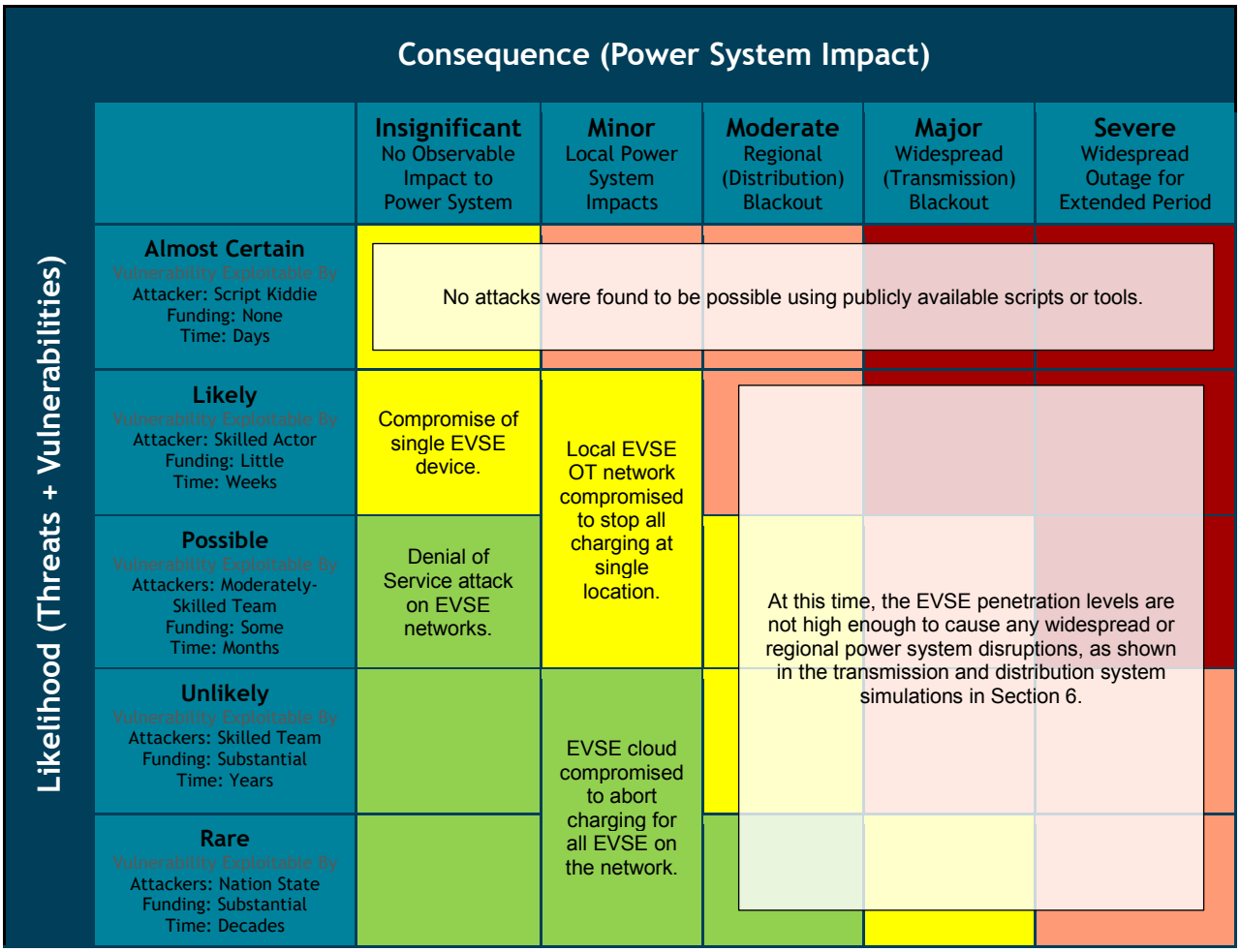

Figure 7-2. EVSE Cybersecurity Attacks Mapped onto the Risk Matrix

Taking the knowledge learned throughout this project, we placed generic attack types on the risk matrix shown in Figure 7-2. The team found that there were no attacks that are possible using public hacking tools, like those found on Kali Linux, so the Almost Certain attacks were removed. The team also showed there is little risk at the distribution or transmission levels of the power system for EVSE manipulation so cyberattacks on EVSE devices or networks are not possible of reaching the Moderate-Severe consequence levels. Throughout our penetration testing there were many relatively simple attacks that could allow local access to an EVSE device which would result in a Medium Risk because it is likely, even though the consequence is insignificant. Similarly, a moderately skilled team could DoS or DDoS EVSE networks, which could disrupt charging operations for thousands of drivers, but from the power system perspective, this would be insignificant. It is also possible that an attacker

[91] K. Rohde, B. Carlson, "Consequence-driven Cybersecurity for High Power EV Charging Infrastructure," INL/MIS-19-55540 in NISTIR 8294, Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE), Sept. 12, 2019.

could gain local or remote access to the EVSE operational technology network and shut down all charging at that location (e.g., fleet disruption). This could cause a minor impact to the power system, so it is a Medium risk. Lastly, a more skilled team, given enough time, would be able to compromise the cloud-based systems for an EVSE operator and abort all charging on that network. This is considered a low risk because it would only cause minor local power system impacts and would require a higher skill level

Based on this assessment, the highest risk scenarios were analyzed and a collection of industry recommendations were created. These attack mitigation priorities are presented in the next section.

8. MITIGATIONS AND RECOMMENDATIONS

This section summarizes the mitigations for the findings discussed in Section 5.1 and includes two infographics that were developed to provide recommendations to the EV/EVSE industry.

8.1. Mitigations

This section provides a list of mitigations for the findings that are described in Section 5.1. A more complete description of these mitigations, along with the expanded description of the findings, can be found in Appendix A on page 58.

8.1.1. Business Network & Operations

- Review all software development processes to incorporate industry best practices including secure deployment practices. [Addresses: A.1]
- Ensure proper physical security measures such as locked doors, visitor monitoring/escorting, perimeter barriers are installed. [Addresses: A.2]
- Ensure EVSE manufacturing and business staff are trained to notify security personnel in the event an unknown individual is in the facility. [Addresses: A.2]
- Establish a formal administrative, quality assurance, and inspection process to ensure EVSE is not tampered with in transit between manufacturing and provisioning facilities. [Addresses: A.3]

8.1.2. EVSE Security

- Improve the physical security of the EVSE enclosure by including a robust locking mechanism, sensors, and tamper-evident seals to prevent or detect access to the interior components. [Addresses: B.1]
- Do not allow the posting of login credentials, or other sensitive information in the interior of the EVSE. [Addresses: B.2]
- Internal hard drives and other storage devices should be encrypted to protect the data at rest. [Addresses: B.3]
- Internal systems should use a password protected BIOS and secure boot process to ensure drive encryption is not bypassed. [Addresses: B.3]
- Utilize a bootloader that is configured to verify digital signatures on all firmware updates and supports secure boot operations. [Addresses: B.4]
- Debug ports should be disabled, configured to prevent display of sensitive information, or require authentication. [Addresses: B.5]
- Unused services on internal EVSE systems should be disabled. [Addresses: B.5]

8.1.3. EVSE Network & Operations

- Require digital signatures on all new software or software updates. [Addresses: C.1]

- Apply network best practices on the EVSE network including the use of network segmentation, and installation of intrusion detection systems, firewalls, etc. at appropriate network locations. [Addresses: C.2]
- Encrypt all communications between internal EVSE components. [Addresses: C.2]
- Encrypt all communications with external systems (ex. cloud systems.) [Addresses: C.2]
- Implement two-factor authentication to prevent the compromise of common credentials from a single EVSE to allow widespread access across the entire EVSE network. [Addresses: C.3]
- Create an alert, that is immediately uploaded to the Security Operations Center (SOC) when a system is being accessed to ensure access is part of expected maintenance operations. [Addresses: C.3]
- Ensure internal information systems are configured with passwords compliant with NIST guidance and, if possible, two-factor authentication. [Addresses: C.4]
- Permissions for editing and running scripts or applications on internal systems should be reviewed for accuracy. [Addresses: C.4]
- Utilize industry best practices to secure remote access tools which includes requiring two-factor authentication, logging usage and anomalies, and ensuring that all network traffic is encrypted. [Addresses: C.5]
- Unless required, EVSE should not be Internet facing and, if required, should be hardened to prevent remote attacks. [Addresses: C.6]
- Ensure that log entries for "Door Open" alarms, system login notifications, and other critical events are prioritized and uploaded immediately to the EVSE cloud. [Addresses: C.7]
- Security policies related to firmware updates and configuration should be reviewed by the manufacturer to ensure these meet their desired behavior and security posture. [Addresses: C.8]
- EVSE systems should require authentication to apply updates or configuration changes. [Addresses: C.8]
- Ensure EVSE are included in a system update plan that ensures they receive updates in a timely manner, and include critical updates are received in a timely manner. [Addresses: C.9]
- EVSE should use secure configurations that do not allow the use of outdated and insecure communication protocols. [Addresses: C.10]

8.1.4. Electric Vehicle Operations

The team did not study electric vehicles as part of this assessment.

8.2. Best Practices

From the specific mitigations that were identified and shared with industry partners, the team also developed a list of industry best practices that should be applied in all areas of EVSE development, deployment, operations, and maintenance.

These practices address the domains that were identified in the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), developed by the Department of Energy and the Department of Homeland Security. They are captured in the infographic in Figure 8-1 and Figure 8-2.

Figure 8-1. EVSE Best Practices.

Figure 8-2. EVSE vendor recommendations based on penetration tests of EVSE equipment and networks.

9. CONCLUSIONS

This project helped identify potential EV charger vulnerabilities and quantify the risk when vehicle charging infrastructure is maliciously controlled. This risk assessment is only a first step in a comprehensive approach to cybersecurity that includes a continuous process of reviewing system weaknesses and hardening charging infrastructure. Additional work must include:

- Developing standardized policies for managing EVSE and other assets in the charging ecosystem.
- Designing effective perimeter defenses to protect EVSE assets including firewalls, access control lists, data-in-flight requirements (encryption, node authentication), etc.
- Creating situational awareness systems, intrusion detection/prevention systems, and anomaly detection.
- Researching response mechanisms to prevent further adversary actions on the system, nonrepudiation technologies, and dynamic responses.
- Creating hardware- and software-based fallback and contingency operating modes.

To meet these challenges, it is recommended that public-private partnerships, good information sharing platforms, and strong cybersecurity research programs are established within the EV charging community.

APPENDIX A. DETAILED ASSESSMENT RESULTS

A.1. Business Network and Operations

[A.1] (High) Software development practices do not utilize industry best practices.

Justification: At some organizations, critical points in the software development lifecycle – such as staging software updates for deployment – do not have an official approval process and can be performed by any of the developers. In addition, the assessment team discovered that some key credentials are not maintained as part of a backup, COOP, or DR process – and are stored on a single machine. In some of the testing labs, login credentials were posted on multiple laptops, allowing anyone with physical access to the space (ex. Facility, maintenance, or custodial personnel) to log into those systems.

Mitigations: Review all software development processes to incorporate industry best practices. This would include:

- Having a formal process for uploading code to a repository
- Including an approval process for staging updates for deployment
- Implementing a 2-person rule at critical locations during the update process to protect against the insider threat
- Requiring individual credentials are required for logging into system; or, if an entity account is required, that it is shared only among those who need access
- Ensure critical credentials, keys, or other "secret" items are properly secured and backed-up in case of personnel departure or system failure
- Ensure critical roles have proper redundancy in personnel

[A.2] (Moderate) Physical security of some facilities could allow unauthorized access to EV chargers being tested, manufacturing areas, and office spaces.

Justification: At one facility, it was reported that rideshare drivers would use the test chargers overnight to get free power. In addition, the assessment team noted that, while badge-based access controls were installed to prevent access to the interior of a facility, the system was not operational. Finally, given the lack of staff in the reception area of the building and the building layout, an attacker could simply walk into the building and access the business or manufacturing area without being observed by staff.

Mitigations: Enable the badging system to secure the doors to the facility, or station personnel in the reception area. In addition, add secured doors to separate the reception, office, and manufacturing spaces. Update training and corporate policies to encourage personnel to challenge anyone they don't recognize at the facility and ensure that they are authorized to be there.

To protect the EVSE located exterior to the building, fencing could be installed, or security personnel should be utilized to provide some measure of protection. If the exterior of the

building is not secured, surveillance cameras should be installed, and the footage reviewed on a regular basis, to identify any malicious activity.

[A.3] (Low) The state of the EVSE is not standardized when shipping across manufacturing locations.

Justification: Multiple EVSE manufacturers utilize manufacturing located outside the US, including overseas production. For some manufacturers, there was not a formal quality assurance check, or standardized state of the EVSE when it is shipped. The assessment team also observed that one manufacturer used a handwritten form attached to the side of the EVSE when shipped from an overseas location to indicate missing components, which could allow for theft of hardware. In addition, when arriving to the U.S. the EVSE is provisioned and operationally tested, but there are no inspections to verify genuine parts, or that malicious components have not been added.

Mitigations: Establish a formal process for preparing EVSE for shipping, including formalizing the paperwork used to designate the exact state of the EVSE when it leaves the facility. In addition, quality assurance should be performed at each step of the manufacturing process to ensure the appropriate components are being used, and malicious hardware is not present. This should be augmented by an inspection or tear down of a statistical sample of EVSE that arrives in the U.S.

A.2. EVSE Security

[B.1] (High) EVSE enclosures do not provide adequate physical protections against unauthorized access.

Justification: Many of the EVSE examined by the assessment team did not have locks or sensors to prevent access to the internal system components. In addition, EVSE are not always deployed in high-traffic areas, or areas with surveillance or protection mechanisms. This combination would allow for an attacker to access the EVSE undetected.

In addition, for EVSE that do integrate locks and sensors, the assessment team found the locks are often commonly keyed, or are inexpensive and relatively easy to bypass. In addition, it was common to see a single sensor detecting the enclosure being opened and were often vulnerable to shimming or other bypass attacks. e.g. Plunger sensor.

Mitigations: Improve the locking mechanism on the door to help prevent picking or other bypass techniques. In addition, door sensors should be protected and positioned to prevent an attacker from bypassing them; or an additional sensor should be installed to detect other signs of the enclosure being opened.

Tamper-evident seals, similar to those used at gas pumps, should be used on the enclosure and internal covers to allow detection of unauthorized access. In addition, inspection of these seals, and the internal hardware components should be added to the maintenance procedures to ensure malicious hardware (such as a credit card skimmer) can be detected if they were added to the EVSE.

[B.2] (High) Login and provisioning credentials are posted inside the EVSE.

Justification: Several of the EVSE examined by the assessment team had usernames, passwords, or provisioning credentials posted inside of the EVSE enclosure. This would allow anyone accessing the enclosure to have the necessary credentials to modify or configure the EVSE. Since these are generally common across an EVSE provider, the compromise of a single EVSE installation would compromise all the EVSE for a specific provider.

Mitigations: While common credentials may be required to facilitate maintenance operations, these should not be stored inside the enclosure itself. If necessary, they can be provided directly to authorized maintenance personnel.

[B.3] (High) Internal information systems do not use encrypted hard drives.

Justification: The assessment team was able to remove drives from the EVSE, copy them, and search it for hardcoded credentials, or other sensitive information. In addition, since these hard drives include the applications providing services for the EVSE, an attacker would be able to modify these applications to exfiltrate financial information, PII, or override safety features.

Mitigations: Ensure all the internal information systems use encrypted hard drives to protect their applications and data. In addition, a secure boot process should also be used for all internal systems to ensure malicious firmware is unable to disable encryption or compromise the operating system to exfiltrate the information.

[B.4] (High) Verification of firmware and software is not performed prior to deployment on EVSE.

Justification: The assessment found that the bootloader being used by multiple EVSE either does not support, or was not configured to require, digital signatures on any updates. Without verifying a digital signature, the EVSE will not be able to detect if the updated package has been modified, or if it is an update from the manufacturer.

Mitigations: Utilize a bootloader that is configured to verify digital signatures on all updates and support other secure boot operations.

[B.5] (Low) Debug ports and unused services are enabled.

Justification: The assessment team was able to receive debug information through an enabled port, and network scans of EVSE showed multiple, unused services were enabled. This finding is rated "Low" since the assessment team did not perform testing to see if there were vulnerabilities in the running services, or if the ports allowed for two-way communication.

Mitigations: Ensure that debug ports are disabled or, if necessary for provisioning and maintenance, that they do not provide sensitive information. In addition, the debug ports should require authentication if they are going to be used to interact with the system. Unused services should be disabled.

A.3. EVSE Network and Operations

[C.1] (High) Verification of firmware and software is not performed prior to deployment and installation.

Justification: Multiple EVSE did not require digital signatures on updates. Without verifying a digital signature, the EVSE will not be able to detect if the updated package has been modified, or if it is an update from the manufacturer.

Mitigations: Utilize digital signatures on all updates.

[C.2] (High) EVSE networks (internal and external) do not follow network security best practices.

Justification: The assessment team found that network traffic between internal components of multiple EVSE is not encrypted, allowing the information to be intercepted and/or modified. In addition, the EVSE network external to the enclosure did not use segmentation, VPNs, or include protection devices such as an IDS or firewall. This would allow an attacker who compromises a single EVSE to have access to the entire EVSE network without being detected. Even with the proposed use of a "dedicated" cellular network, this only prevents outsiders from accessing the network and does not provide protections against a compromise of an EVSE already connected to the network.

Mitigations: All communications, both internal to the EVSE and with external systems should be encrypted. The external network should apply network best practices such as use of network segmentation, and inclusion of security systems such as an IDS in appropriate locations supported by appropriate firewalls. In addition, each EVSE should establish a VPN to the system server, which would then block direct communication between two EVSE systems.

[C.3] (High) EVSE providers utilize the same credentials throughout their charging network.

Justification: To support maintenance operations, the same credentials are used for all the EVSE deployed in a charger network. Therefore, the compromise of these credentials would allow an attacker access to all of the EVSE in the network. In addition, these credentials are essentially permanent since they are not changed as part of the maintenance procedures or for personnel turnover. While this may simplify maintenance operations, and is a common practice in some sectors, it still represents a vulnerability.

Mitigations: Two-factor authentication should be implemented to prevent the compromise of the credentials from giving an attacker access. If this is not possible due to system or network restrictions, the assessment team recommends immediately uploading an alert that the system is being accessed. If this occurs outside of normal maintenance operations, then that system should be disabled and isolated from the network until it can be inspected and serviced by authorized personnel to prevent any malicious modifications to the equipment and network.

[C.4] (High) Default credentials are used on internal information system components.

Justification: Internal information systems were observed to have default, easily guessed username/password combinations. In addition, the user account found to have this vulnerability had permission to edit a script that was executed as the root user after a reboot, effectively giving complete control of the machine to this user account.

Mitigations: Ensure internal information systems are configured with passwords compliant with NIST guidance and, if possible, two-factor authentication. In addition, the EVSE scripts

and applications should be reviewed to ensure that the permissions are set to prevent an unprivileged user from executing code as the root user.

[C.5] (High) Insecure remote access tools are used to configure and troubleshoot deployed EVSE.

Justification: Some remote access tools allow for the complete control of the EVSE in the charger network to support maintenance and troubleshooting operations. However, the assessment team found communications are unencrypted, allowing an attacker to capture or replay traffic over the network. In addition, it was unclear if common credentials were used for the remote access tools, which would allow anyone to log into the EVSE and take complete control

Mitigations: To prevent an attacker from using remote access tools to take control of the EVSE, industry best practices should be used. These include requiring two-factor authentication, logging usage and anomalies, and ensuring that all network traffic is encrypted.

[C.6] (High) EVSE are Internet connected and discoverable by search engines.

Justification: Many of the EVSE were using outdated software and protocols – including those with known vulnerabilities. In addition, many of these systems are easily discoverable using Google and the Shodan search engine, which also allowed for the generation of a system "fingerprint" to search for additional EVSE systems. This combination of easily discoverable, accessible, and the ability to use existing exploits and tools would allow an attacker to conduct remote attacks that would give them complete control of the EVSE.

Mitigations: Unless required, EVSE should not be Internet facing. If it is required for them to be directly accessible from the Internet, the system should be hardened to prevent remote attacks. This would include the use of two-factor authentication, shutting down all unused services and ports, ensuring updates are applied in a timely manner, and encrypting communications.

[C.7] (Moderate) Logs are stored locally instead of being uploaded for analysis

Justification: Logs are stored on the local systems instead of being uploaded to a server in the EVSE network. Keeping the logs locally allows an attacker to perform their malicious activity and then delete the log entries related to the malicious actions. In addition, it was not clear if downloading the logs and/or analysis of them was performed during maintenance operations. However, even if they are examined during maintenance operations, on-site maintenance is only expected to occur every 2-3 years.

Mitigations: Ensure that "Door Open" alarms, system login notifications, and other critical events are prioritized and uploaded immediately to the EVSE cloud. This will allow analysis of the log entries to determine if they are part of expected maintenance activities. If the logs show unauthorized activity, remediation steps can be taken immediately.

[C.8] (Moderate) Some EVSE equipment can be reflashed with a USB stick.

Justification: One brand of EVSE has been designed to be reflashed with a USB stick without requiring any authentication. In addition, the manufacturer provides a wizard to assist in the creation of the USB stick.
Mitigations: The security policy related to the EVSE should be reviewed by the manufacturer to ensure this is the desired behavior and security posture. If it is determined that this strategy does not meet their security needs, or that it introduces an unacceptable level of risk, the system should be modified to require authentication to reconfigure the EVSE, and it should only apply a digitally signed update package.

[C.9] (Moderate) Updates to the EVSE firmware and software are not routinely scheduled or deployed.

Justification: Not all EVSE manufacturers have a plan for applying regular updates to the EVSE, and historically updates are rarely deployed. This means that any vulnerabilities found in the firmware or software may not be patched in deployed EVSE. While cellular data caps are the underlying issue with pushing updates, this limitation does not prevent this from being a potential vulnerability.

Mitigations: Establish a plan where updates are provided to the deployed EVSE, including additional on-site maintenance activities for critical patches.

[C.10] (Moderate) EVSE use outdated and insecure protocol versions.

Justification: Older and insecure protocols, such as OCPP 1.6 and MQTT, were found to be in use on EVSE connected to the Internet. This would allow remote attackers to compromise the EVSE or the communications utilizing those protocols.

Mitigations: EVSE should use secure configurations that do not allow the use of outdated and insecure communication protocols. Allowing backwards compatibility should include security risks as well as usability concerns.

A.4. Electric Vehicle Operations

The team did not study electric vehicles as part of this assessment.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Jay Johnson	08812	jjohns2@sandia.gov
Summer Ferreira	08812	srferre@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Lee Slezak	lee.slezak@ee.doe.gov	Department of Energy Vehicle Technologies Office

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.