I Grid and Charging Infrastructure

I.1 Cyber Security

I.1.1 Securing Vehicle Charging Infrastructure

Jay Johnson, Principal Investigator
Sandia National Laboratories
P.O. Box 5800 MS1033
Albuquerque, NM 87185-1033
E-mail: jjohns2@sandia.gov

Lee Slezak, DOE Program Manager
U.S. Department of Energy
E-mail: Lee.Slezak@ee.doe.gov

Start Date October 1, 2018: End Date: September 30, 2021
Project Funding (FY19): $1,000,000 DOE share: $1,000,000 Non-DOE share: $0

Project Introduction

Cybersecurity is essential for interoperable power systems and transportation infrastructure in the US. As the US transitions to transportation electrification, cyber attacks on vehicle charging could impact nearly all US critical infrastructure. This is a growing area of concern as more charging stations communicate to a range of entities (grid operators, vehicles, OEM vendors, etc.), as shown in Figure I.1.1.1. The research challenges are extensive and complicated because there are many end users, stakeholders, and software and equipment vendors. Poorly implemented electric vehicle supply equipment (EVSE) cybersecurity is a major risk to electric vehicle (EV) adoption because the political, social, and financial impact of cyberattacks—or public perception of such—ripples across the industry and has lasting and devastating effects. Unfortunately, there is no comprehensive EVSE cybersecurity approach and limited best practices have been adopted by the EV/EVSE industry. For this reason, there is an incomplete industry understanding of the attack surface, interconnected assets, and unsecured interfaces. Thus, comprehensive cybersecurity recommendations founded on sound research are necessary to secure EV charging infrastructure. This project is providing the automotive industry with a strong technical basis for securing this infrastructure by developing threat models, prioritizing technology gaps, and developing effective countermeasures. Specifically, the team is creating a cybersecurity threat model and performing a technical risk assessment of EVSE assets, so that automotive, charging, and utility stakeholders can better protect customers, vehicles, and power systems in the face of new cyber threats.

Objectives

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

- conducting adversary-based assessments of charging equipment,
- creating a threat model of EV charging, and
- analyzing power system impact for different attack scenarios.

This will provide DOE and automotive, EVSE vendor, and utility stakeholders with:

- clear documentation of the gaps in EVSE cybersecurity and the path forward to address those weakness,
- a threat model for EVSEs and associated infrastructure and services,
- recommendations for the automotive industry based on EVSE penetration testing, and
- cyber attack impact analyses of the power system with remediation recommendations.

This project is also generating cybersecurity research solutions and collaborating closely with other government agencies and industry stakeholders to raise awareness of cybersecurity issues and solutions.

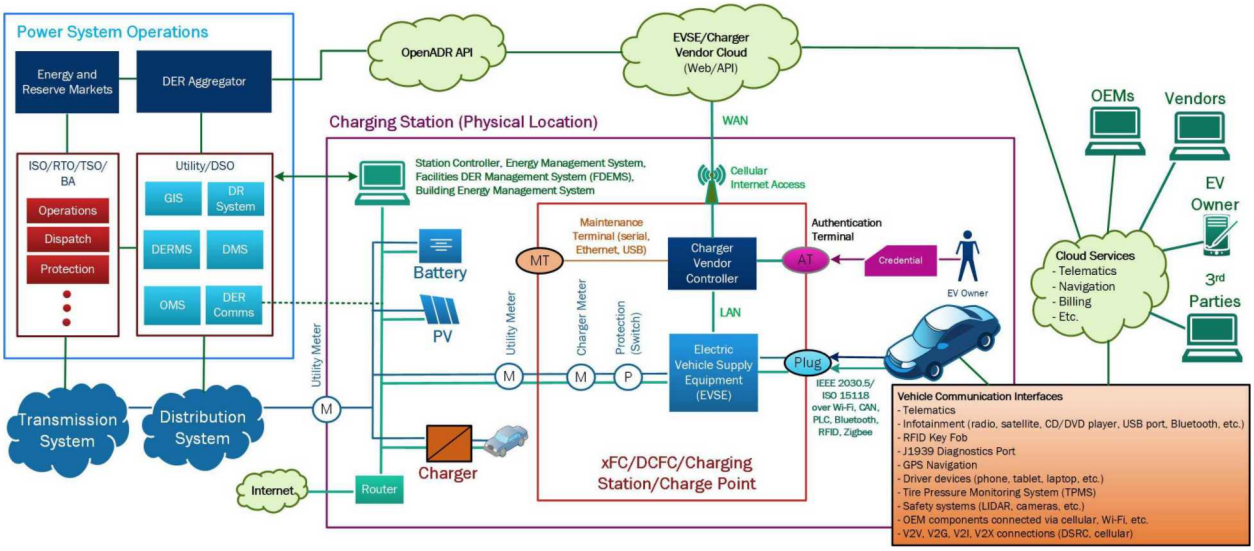

Figure I.1.1.1 Electric vehicle communication systems to different components and entities.

Approach

The team is executing on the following integrated cybersecurity R&D tasks:

1. conduct threat modelling based on the STRIDE methodology for electric vehicles to understand what potential cyber hazards exist with EVSE communications;
2. assess the current state-of-the-art cyber security posture of EVSE equipment using authorized, adversary-based assessment techniques (red teaming);
3. establish credible attack vectors based on the red teaming assessments and threat model;
4. determine the impact of current and potential vulnerabilities on distribution and transmission power systems; and
5. create a risk matrix to prioritize mitigations that reduce the number of high-consequence/low-threat level attacks.

The task structure of this project is shown in Figure I.1.1.2, 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 particular attack is the combination of the likelihood and impact of the attack. By studying a range of scenarios, optimal mitigations can be determined to prevent these attacks at specific points in the attack kill chain (i.e., the steps to accomplish adversary goals).

Results

In the first year of the project, the team 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. A detailed threat model was created for different EVSE chargers with connections to external entities. Attack graphs were revised based on penetration testing of multiple EVSEs. A distribution simulation of EVSE charging with and without vehicle-to-grid (V2G) functionality was conducted to determine if malicious control of EVSEs could cause high or low voltages on feeder circuits. Transmission simulations of coordinated charging of using the WECC were also performed to understand bulk system impact from coordinated cyber attacks.

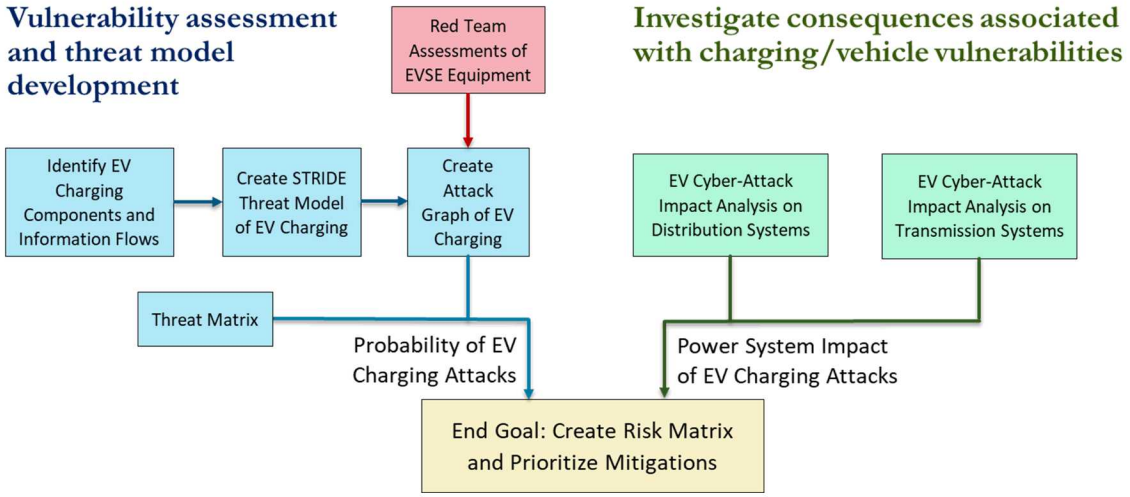

Figure I.1.1.2 Project tasking.

STRIDE Threat Model

STRIDE is a threat modeling methodology used to help identify threats to systems operating in an environment. The team used this methodology to understand the threats to the electric vehicle charging ecosystem, including the plug-in electric vehicle, the charging station, charging station owners, and utilities. The threat model, shown in Figure I.1.1.3, graphically depicts data flows between components of the electric vehicle charging system. The figure has been simplified to reduce the number of flows and components. The dashed boxes indicate trust boundaries, where the level of trust changes from untrusted (outside the boundary) to trusted (inside the boundary). Components inside the boundary share the same of degree of trust. Using the model, we can reason that a vulnerability to, for example, *P-06 EV Vendor App with Battery Data* can potentially influence EV charging rates. The model also indicates where to mitigate vulnerabilities. For instance, *P-59 EVSE Controller EVSP and DSO* may be an opportune position to implement a mitigation that limits the consequences of an aggregate *App* vulnerability. The team employed the model to consider the potential threat exposed by every data flow through the trust boundaries, and the potential consequence to the ecosystem for these threats.

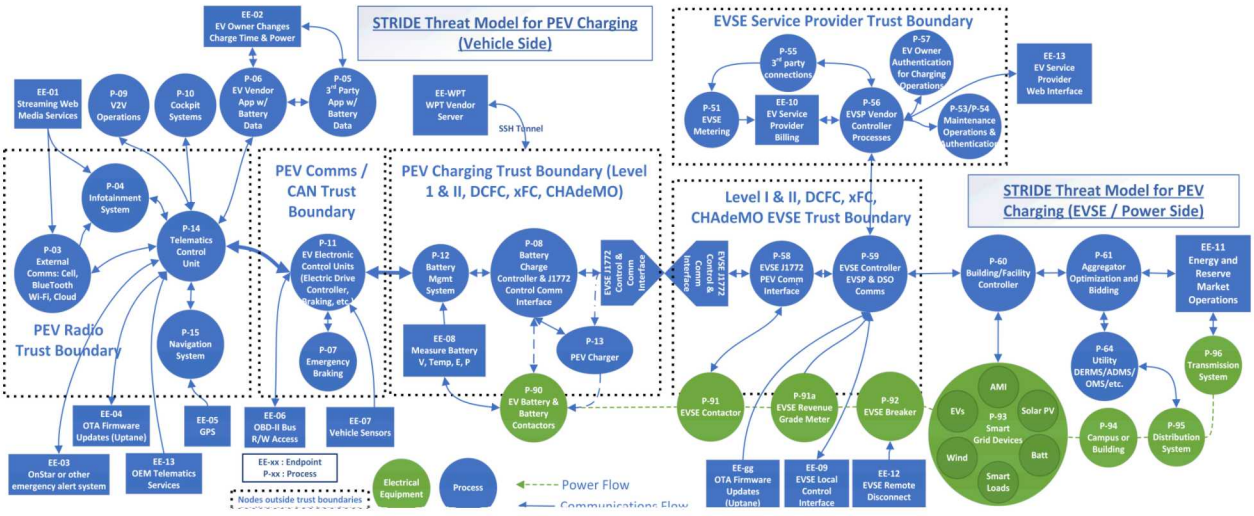

Figure I.1.1.3 Threat Model.

Attack Graphs

Attack graphs show the steps an attacker must take to move from a system/network access point to a particular consequence or objective. Figure I.1.1.4 illustrates access points, staging areas, and consequences of concern related to a generic EV charger network. The team used the information gathered from their assessments, publicly available information regarding vulnerabilities, and knowledge regarding the tools, tactics 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 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 that the answer to both questions is "Yes" which means an attacker *could* manipulate large fleets of EVSEs and cause distribution and transmission impacts. Importantly, the assessment team provided the EVSE partner with the findings and potential mitigations for identified vulnerabilities.

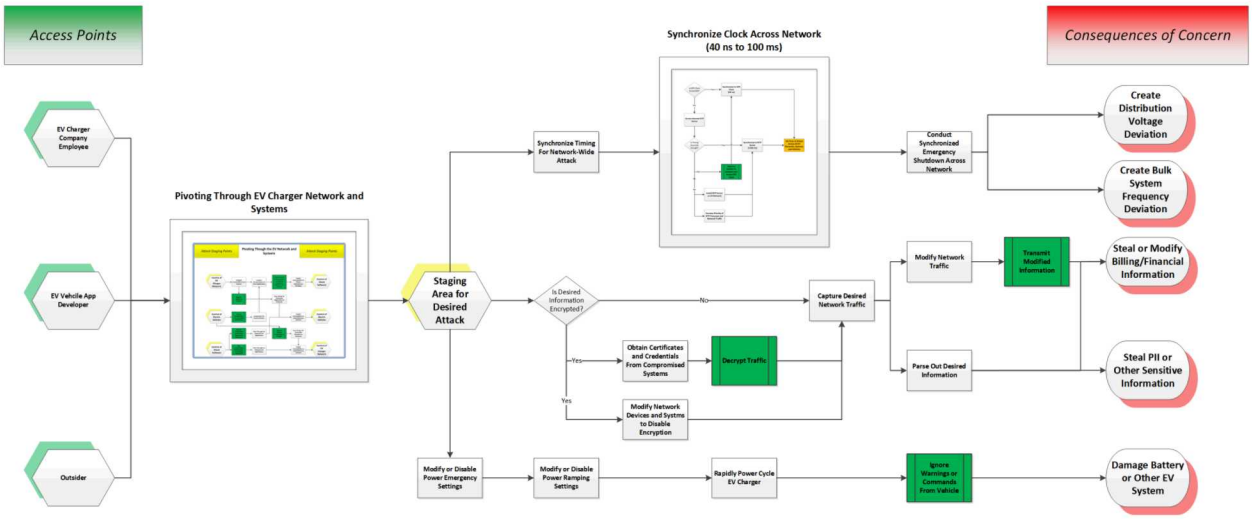

Figure I.1.1.4 Attack graph.

Distribution System Simulations

To better understand the impact on the power system for different penetrations of EVSEs 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., EVSEs reached full output in ~13 seconds). The results for steady-state charging and discharging with different power factors are shown in Figure I.1.1.5. 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.

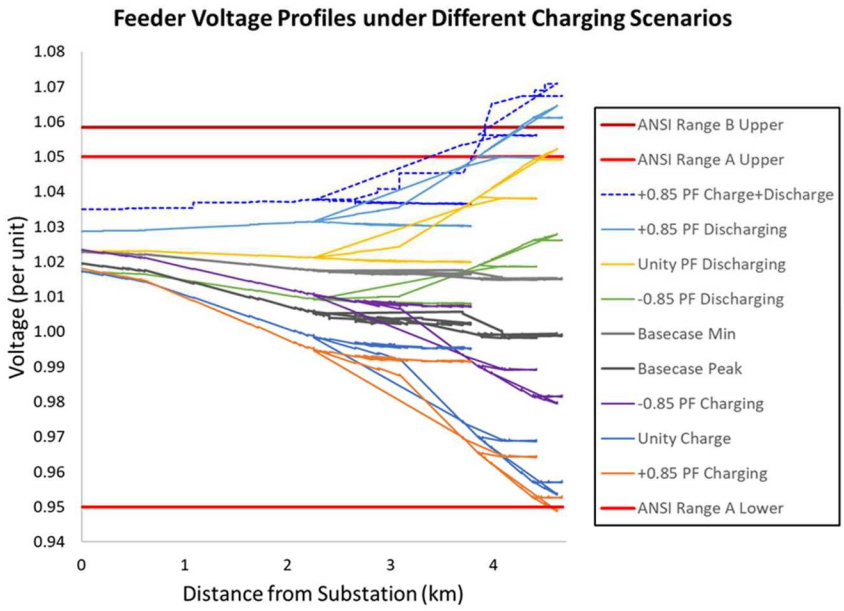

Figure I.1.1.5 Different distribution voltage profiles for coordinated charging/discharging of EVSEs totaling 2.25 MW.

Transmission System Simulations

With projections of high EV penetration in the US [1], 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. The team evaluated worst-case scenarios in which EV loads were manipulated on a realistic 20,000+-bus representation of the Western Electricity Coordinating Council (WECC) simulated in GE's PSLF 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. (Forecasted EV loads were based on each state attaining a 16.3% conversion from internal combustion engine vehicles to EVs by 2030, calculated based on the percentage of EVs for California to reach its target of five million zero-emission vehicles.)

The load drop disturbance occurred at $t = 1$ second and the transients were captured for 9 more seconds at a 0.125 s time step to record the primary frequency response. All simulations were run using snapshots of the WECC corresponding to two different operational (seasonal) setpoints: a light spring load profile, and a heavy summer load profile. For the WECC-wide simultaneous EV load tripping events, moderate frequency deviations were observed. Location-specific events corresponding to Los Angeles and Seattle registered much smaller frequency deviations. Given that the light spring load profile will have less generation dispatched initially, we observe that for the same GW load trip, the lightly-loaded spring case will have a larger frequency deviation than the heavy summer load case. When the "emergency stop charging" command is issued to all EVs in the light spring loading case (worst-case scenario), there is a substantial impact to the power system. A plot of average system frequency, total generation, and total load is shown in Figure I.1.1.6 for the cyber-attack. After the attack, the frequency quickly climbs to 60.6 Hz.

In the model, all transmission protection and remedial action schemes were modeled. The North American Electric Reliability Corporation (NERC) defines generator frequency and voltage protective relay settings in PRC-024-2 [2]. In the WECC, relays are set to instantaneously trip for frequency deviations less than 57 Hz and greater than 61.7 Hz. Per unit (pu) voltage limits are also defined in PRC-024, where sustained voltages outside of 0.9 pu and 1.1 pu will initiate tripping events to mitigate voltage deviations outside of this range. Fortunately, the does not reach the PRC-024 generator relay trip settings and the power system returns to

normal operation by throttling down the synchronous generators. Therefore, the impact to customers is minimal and the generator controls were able to compensate for the XFC disconnect disturbance.

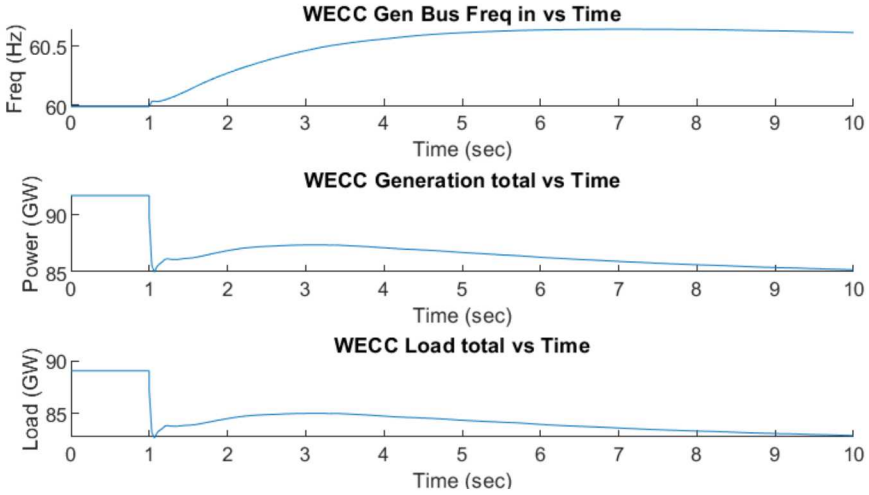

Figure I.1.1.6 WECC light spring: system values through time.

Conclusions

This project is helping identify potential EV charger vulnerabilities and quantify the risk to critical infrastructure when vehicle chargers are maliciously controlled. This risk assessment is only an initial step in a continuous process of hardening charging infrastructure against cyber-attacks though. There is much more work to secure charging infrastructure from cyber attacks, including:

- Developing standardized policies for managing chargers and other assets in the charging ecosystem
- Designing effective perimeter defenses to protect the assets including: firewalls, access control lists, data-in-flight requirements (encryption, node authentication), etc.
- Creating situational awareness systems, intrusion detection systems, and intrusion prevention systems.
- 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.

Key Publications

N/A

References

[1] Edison Electric Institute, “Electric Vehicle Sales Forecast and the Charging Infrastructure Required Through 2030,” 2018.
[2] 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].

Acknowledgements

DOE and the PI wish to thank the multi-laboratory team for this work: SNL (Brian Wright, Ben Anderson, Russell Graves, Jimmy Quiroz), PNNL (Rick Pratt, Tom Carroll, Lori O’Neil, David Gotthold) and ANL (Roland Varriale, Ted Bohn, and Keith Hardy).

Sandia National Laboratories is a multimission laboratory operated by National Technology and 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.