NISTIR 8294

Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE)

Suzanne Lightman
Tanya Brewer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8294

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8294

Symposium on Federally Funded Research on Cybersecurity of Electric Vehicle Supply Equipment (EVSE)

Suzanne Lightman
Tanya Brewer
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8294

April 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8294
82 pages (April 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8294

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8294-comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Electric vehicles are becoming common on the Nation's roads, and the electric vehicle supply equipment infrastructure (EVSE) is being created to support that growth. The NIST Information Technology Lab (ITL) hosted a one-day symposium to showcase federally funded research into the potential cybersecurity implications of EVSE.

Keywords

Automotive cybersecurity; charging station cybersecurity; electric vehicles cybersecurity; electric vehicle infrastructure; electric vehicle supply equipment infrastructure (EVSE).

Acknowledgments

The NIST Information Technology Laboratory would like to acknowledge Lee Slezak of the Department of Energy, Christos Papadopoulos of the Department of Homeland Security, Kevin Harnett of the Department of Transportation, and James McCarthy of NIST for their contributions in putting together this symposium. NIST would also like to acknowledge the presenters for their participation. In addition, NIST would like to acknowledge Tim Weisenberger of SAE for chairing the discussion.

Table of Contents

List of Figures

1 Introduction

Over the last decade, electric vehicles have evolved from concept cars to an accepted technology with almost every major automobile manufacturer offering at least one electric model. Sales of electric vehicles have risen significantly in Europe[1] and 2 % of new vehicle sales in the U.S. were electric only.[2] Major companies like GM and Volvo have announced their intentions to phase out gas-only vehicles within the next 20 years.[3] There is also interest in the heavy trucking sector in electric trucks due, in part, to rising fuel costs and promised lower maintenance costs—so much so that cybersecurity guidelines for electric vehicle supply equipment infrastructure (EVSE) for heavy-duty trucks have been suggested.[4]

EVSE is supported by electronics, both for charging the vehicle and facilitating communications, so EVSE is susceptible to cybersecurity vulnerabilities and attacks. EVSE also ties together two critical sectors—transportation and energy (specifically, the electric grid)—that have never been connected electronically before. This creates the potential for attacks that could have significant impacts in terms of money, business disruptions, and human safety.

ELECTRIFY AMERICA'S IMPACT ON EVSE

As a result of the emissions scandal in 2016, Volkswagen funded Electrify America, which currently operates over 400 charging stations and is planning to invest another $2 billion in EVSE infrastructure.

https://www.electrifyamerica.com/our-plan

Because of this, there are multiple U.S. government agencies that are interested in this area, including:

- Department of Energy
- Department of Homeland Security
- Department of Transportation
- Department of Defense
- General Services Administration
- NIST

U.S. governmental concerns about cybersecurity of EVSE cover a range of issues. What impact would EVSE have on the stability of the electrical grid? Could EVSE serve as a vector for

[1] Irle V (2019) *Europe BEV and PHEV Sales for Q3-2019 + October*. Available at http://www.ev-volumes.com/country/total-euefta-plug-in-vehicle-volumes-2/

[2] Irle R (2019) *USA Plug-in Sales for 2019 YTD October*. Available at http://www.ev-volumes.com/country/usa/

[3] Roberts D (2017) *The world's largest car market just announced an imminent end to gas and diesel cars*. Available at https://www.vox.com/energy-and-environment/2017/9/13/16293258/ev-revolution; Hawkins AJ (2019) *Cadillac will lead General Motors' push into an electric future*. Available at https://www.theverge.com/2019/1/11/18178444/cadillac-general-motors-gm-electric-vehicle-ev

[4] National Motor Freight Traffic Association, Inc. (2019) *NMFTA Publishes Extreme Fast Charging Cybersecurity Requirements for Medium and Heavy Duty Electric Vehicles*. Available at http://www.nmfta.org/documents/newsletters/XFC%20Press%20Release.pdf

cybersecurity attacks impacting the Nation's economy? In addition, the U.S. Government, as a potential user of electric vehicles and EVSE, is concerned about how cybersecurity threats to the charging infrastructure might affect government activities. These concerns, as well as policy interests in the adoption of electric vehicles, have led to research efforts sponsored by federal agencies to examine potential cybersecurity issues.

Because of these concerns, the NIST Information Technology Lab (ITL) held a one-day meeting on September 12, 2019 as part of federal activities that are being undertaken to familiarize the Government and industry with the cybersecurity research done on EVSE infrastructure.

2 EVSE Structure

There are multiple components to the EVSE, and there are several possible architectures. For example, the EVSE may include the use of distributed energy resources (DERs), such as solar or wind, or it may use only conventional transmission. Some EVSEs may have energy storage systems (ESS), while others may not store power. There are EVSE architectures based on wireless power transfer (WPT) and others based on extreme fast charging stations (XFC).

In addition, the EVSE architecture may include money exchange methods such as credit cards (equivalent to gas stations) and require the use of internet-enabled communications to make those transactions. EVSEs may be connected to building management systems when such systems are also responsible for heating or elevator operation.

The EVSE has multiple participants who are dependent on the cybersecurity of the EVSE. These participants have different cybersecurity interests and risk levels which should be considered in the design, installation, and use of EVSEs.

The parties involved may include:

- The vehicle owner/user who is recharging the vehicle
- The vehicle manufacturer
- The grid operator
- The charging station manufacturer
- The charging station owner
- Credit card company if used for payment purposes
- Building management systems

One EVSE architecture is illustrated in Figure 1 below. Other potential architectures are also illustrated in the attached presentations.

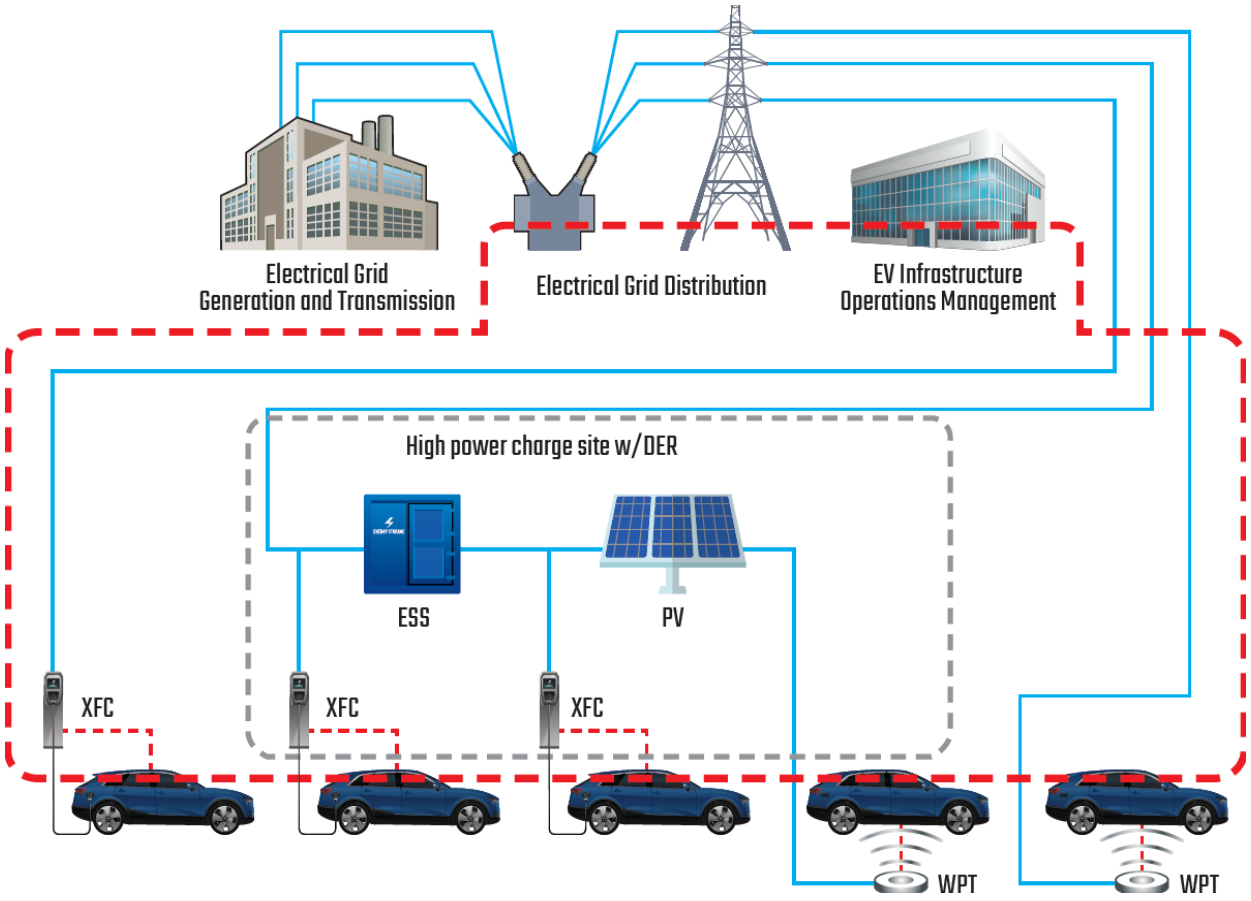


Figure 1: EVSE Architecture

Source: Rohde and Carlson, "Consequence-driven Cybersecurity for High-Power EV Charging Infrastructure." (Appendix B)

3 Concerns

At the workshop on September 12, 2019, the presenting researchers agreed that the EVSE infrastructure provides new targets for cybersecurity attacks. The implementation of EVSE creates connections between sectors (transportation and electrical grid) that are not common in the current gasoline-powered vehicle environment. The researchers also agreed that new targets for attackers and the potential for new vulnerabilities have been created. Among the possible consequences discussed were:

- Disruption of electrical grids
- Safety-adverse effects on vehicles
- Credit card or banking fraud
- Interference with building systems

It was also pointed out by several researchers that the power and transportation sectors are under different regulatory schemes and have different cybersecurity concerns, and misalignment in cybersecurity approaches could cause unintentional exposures. Moreover, neither sector is developing or implementing EVSE in the majority of cases. Therefore, EVSE designs may not be addressing the cybersecurity risks of these sectors. To add to these concerns, there is currently no forum where these different industries can come together to discuss these issues.

Another concern that was raised is the speed of rollout of EVSE infrastructure. Electrify America, for example, plans to invest over $230 million in EVSE infrastructure in the United States through 2021.[5] Most of the researchers believe that there will be a significant jump in the adoption of electric vehicles in the coming years, especially once charging stations become widely available. The concern is that the speed of the rollout may result in an EVSE infrastructure that has not had cybersecurity "built in," which will then need to be addressed later. Additionally, it was pointed out by several attendees that, although multiple federal agencies are interested in the issue, none of them have regulatory authority. Without a nationwide approach, EVSE could be implemented across the Nation with widely varying methods and levels of cybersecurity.

Because EVSE is a relatively new infrastructure, multiple researchers pointed out the lack of understanding of the risks and necessary controls. As a result, multiple researchers devoted significant attention to the development of threat models. Reliable threat models are needed to help determine what risks exist and what controls might mitigate such risks. Without threat models, it is difficult for manufacturers, users, and the Government to make risk-based decisions on the controls needed.

4 Federal Research in the Area

Six projects, supported by federal dollars, presented their research:

- Threat Model of Vehicle Charging Infrastructure *(Sandia National Labs)*
- Enabling Secure and Resilient XFC: A Software/Hardware-Security Co-Design Approach (*Virginia Tech)*
- Consequence-Driven Cybersecurity for High-Power Charging Infrastructure (*Idaho National Labs)*
- Cybersecurity for Grid Connected eXtreme Fast Charging (XFC) Station (CyberX) *(ABB)*

[5] National ZEV Investment Plan: Cycle 2 Public Version – February 4, 2019, Electrify America https://elam-cms-assets.s3.amazonaws.com/inline-files/Cycle%202%20National%20ZEV%20Investment%20Plan%20-%20Public%20Version%20vF.pdf

- EVSE Cybersecurity Projects *(National Motor Freight Traffic Association/DOT Volpe Center)*
- Developing a Reference Architecture XFC-Integrated Charging Security Infrastructure Ecosystem (*The Electric Power Research Institute EPRI)*

The full agenda is included in Appendix A, and presentation slides may be found in Appendix B.

5 Overall Points

There were multiple points that were agreed to both by the researchers and participants. All participants agreed that there are cybersecurity concerns, and it will require multiple sectors and organizations to come together to address these concerns. However, the participants could not agree on the existence of a forum in which all of the different interests could be discussed or a consensus reached on cybersecurity for EVSE.

The participants were also in agreement that international standards might be helpful if they were developed by a wide group that represented the disparate interests. There were concerns raised that, in the absence of industry-driven consensus standards, there may be conflicting regulatory requirements across the globe. This would increase costs for the EVSE industry.

There was discussion on the lack of coordination among the sectors involved (automotive, energy, and financial). Beyond not having a common forum, it was generally agreed by participants that there was a lack of familiarity between the electric and automotive sectors. As a result, the sectors had very little understanding of each other's concerns and approaches to cybersecurity. This complicates the development of cybersecurity models for EVSE since it is difficult to establish a reasonable cybersecurity response or even agree upon forum of discussion to develop such a response without a common understanding of risks and concerns.

There is significant work being done on multiple threat models in the federally funded research projects, and all participants agreed that this work was valuable and a good use of federal funding. It was suggested that it would help to have some coordination among researchers to increase the usefulness of the threat models. Coordination would also allow industry to work across multiple models to build a comprehensive protection schema.

A common concern for participants was that the two major industries that are involved in EVSE (i.e., automobile and electrical grid) are both heavily regulated. For automobiles, the regulations are in the areas of safety, anti-pollution, and energy consumption. For the electrical sector, the regulations oversee safety and reliability. Therefore, both industries work within a framework of requirements that was not developed with each other's operations in mind. Participants were concerned that this could lead to confusion and conflict over cybersecurity as the industries are focused on different requirements and goals.

An example of this conflict was the suggestion to develop a model of where to put EVSE and at what charging level. Transportation sector participants assumed that such a model would use the

movement of vehicles to determine placement. However, the electric sector participants assumed that such a model would be based on power load. As a result, representatives from the energy sector objected to the development of such a model as it would contain extremely sensitive information that they would not be comfortable with providing to non-grid entities. However, there was general agreement that such a model was needed.

Repeatedly, the need for private sector leadership to oversee the effort was raised. The reasons for such a need included:

- Multiple sectors with competing missions and concerns
- Need for coordination to maximize scarce resources
- No established fora for discussion

The current EVSE manufacturing industry has only two major players and multiple smaller companies. The industry has no trade association or accepted standards development organization. As a result, it is unclear, even to the companies concerned, who and where they could look to for leadership or even for participation in larger conversations.

There was a call for more federal leadership in this area by the major agencies represented: DoD, DoE, DoT, and DHS. However, there was a counter concern that regulation would not be helpful in this early stage. There were requests for assistance from NIST to aid in the development of standards. The discussion was chaired by SAE International, and there was some interest in using that organization as the standards development organization for EVSE.

Appendix A—Agenda

Federal Research in EVSE Cybersecurity

September 12, 2019

National Center for Cybersecurity Excellence
9700 Great Seneca Hwy, Rockville, MD

AGENDA

8:30 – 9:00 am	Registration
9:00 – 9:30 am	Introductions and Opening Address
9:30 – 10:00 am	**Threat Model of Vehicle Charging Infrastructure** *Brian Wright, Sandia National Labs*
10:00 – 10:30 am	**Enabling Secure and Resilient XFC: A Software/Hardware-Security Co-Design Approach** *Ryan Gerdes, Virginia Tech*
10:30 – 11:00 am	Break
11:00 – 11:30 am	**Consequence-Driven Cybersecurity for High-Power EV Charging Infrastructure** *Kenneth Rohde and Barney Carlson, Idaho National Laboratory*
11:30 – 12:00 am	**Cybersecurity for Grid Connected eXtreme Fast Charging (XFC) Station (CyberX)** *David Coats, ABB*
12:00 – 1:00 pm	Lunch
1:00 – 1:45 pm	**National Motor Freight Traffic Association (NMFTA) Medium Duty and Heavy-Duty Electric Vehicle (MD/HDEV) Extreme Fast Charging (XFC) Cybersecurity Working Group** *Graham Watson, DOT-Volpe/KBRwyle* **NAVFAC Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report** *Gus Brown, DOT-Volpe/KBRwyle*
1:45 – 2:15 pm	**Reference Architecture for Securing XFC-Integrated Charging Infrastructure** *Tobias Whitney, EPRI*
2:15 – 2:45 pm	Break
2:45 – 4:15 pm	Open discussion and next steps
4:15 – 4:30 pm	Close

Appendix B—Presentations

This appendix contains the slides submitted by each presenter at the symposium and follow the order in the agenda in Appendix A.

2

Overview

Primary goal: protect US critical infrastructure and improve energy security through technical analysis of the risk landscape presented by massive deployment of interoperable electric vehicle chargers.

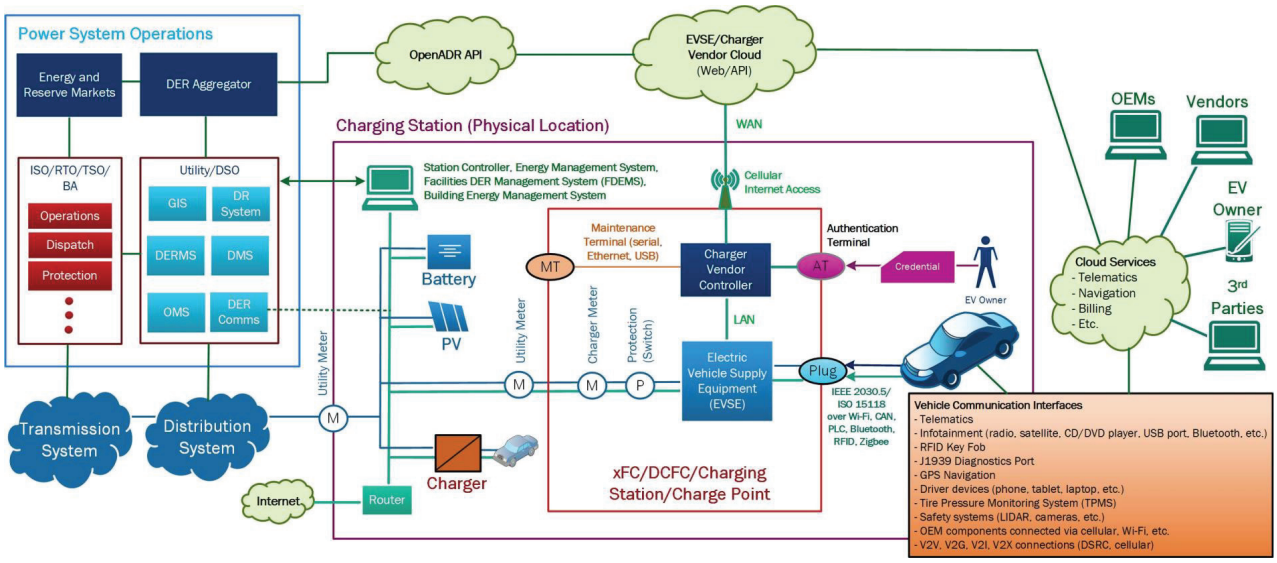
- As the US transitions to transportation electrification, **cyber attacks on vehicle charging could impact nearly all US critical infrastructure**.

This project is **laying a foundation for securing critical infrastructure** by:

- Conducting adversary-based assessments of charging equipment
- Creating a threat model of EV charging
- Analyzing power system impact for different attack scenarios

3 EV Charging Components and Information Flows

Created common nomenclature and enumerate assets and interfaces.



4 STRIDE Threat Model of EV Charging

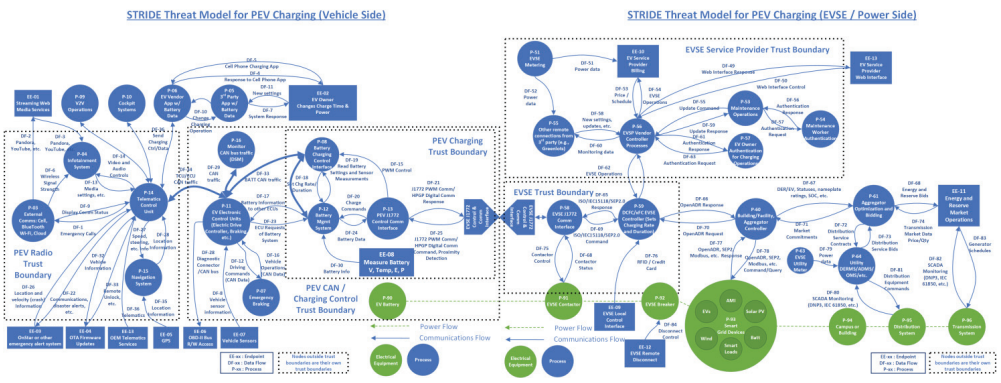
STRIDE Threat Modelling (by Microsoft)

- Helps identify potential vulnerabilities in products/systems
- Step 1: Identify assets, access points, and information flows
- Step 2: List all potential STRIDE threats
- Step 3: Create mitigation plan

Model Inputs

- EV Information Flow Chart
- VTO workshop ES-C2M2 results
- Vulnerability/CVE announcements/disclosures
- DOT Volpe Threat Model

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



Threat model includes:

- Processes (P)
- Data Flows (DFs)
- Endpoint (EE)
- Trust Boundaries (dashed)
- Electrical Equipment (green)

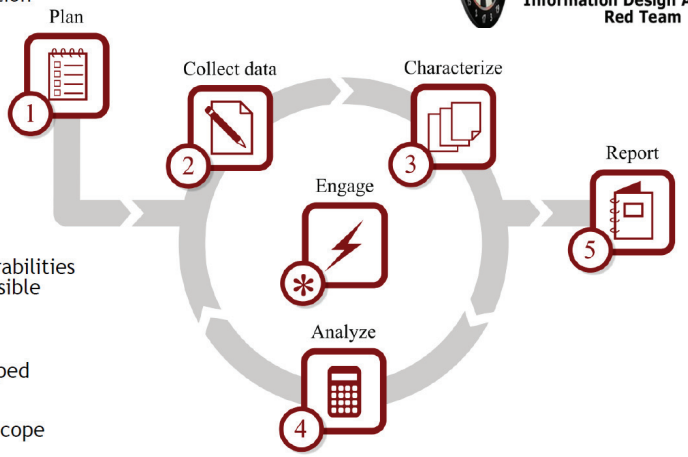
5

Red Teaming

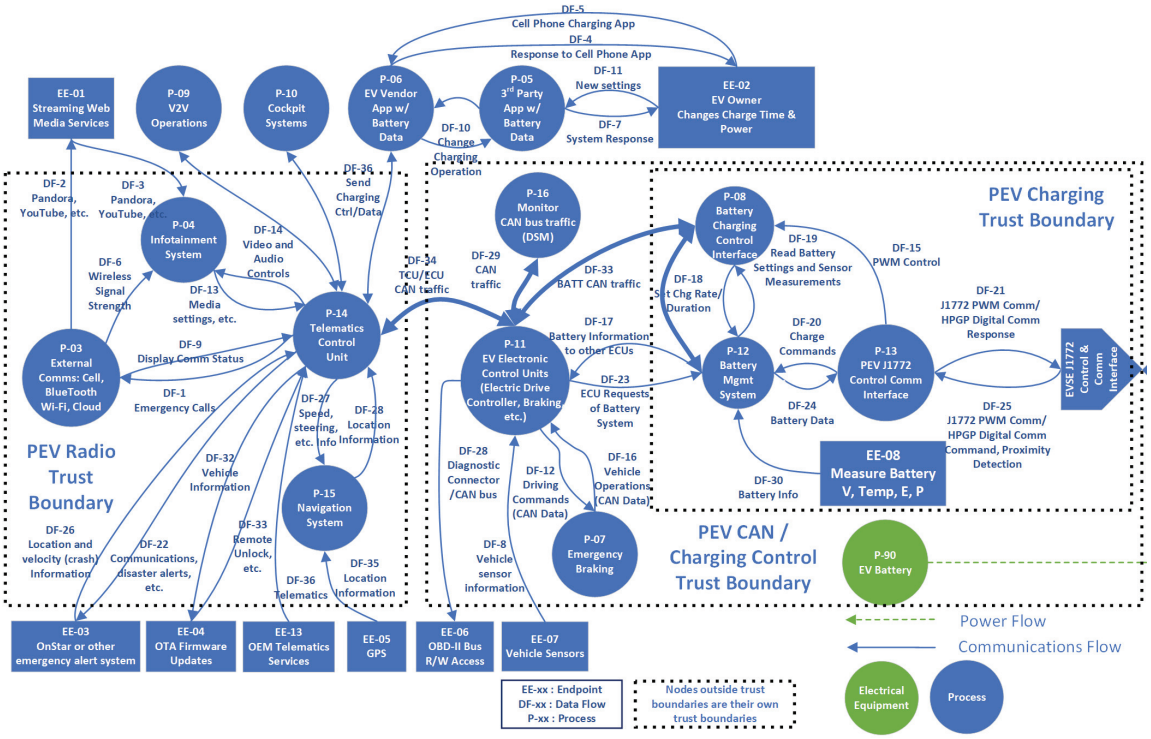
Provides hands-on input to threat model/attack graph

- **Planning**
  - Negotiate work
  - Identify and procure resources
- **Data Collection**
  - Scoping visit activities and information requests
  - Open source information gathering
- **Characterization**
  - Refine understanding of system given data collected
  - Generate/refine views to facilitate discussion
- **Analysis**
  - If needed, collect more data and re-characterize
  - Otherwise, determine where vulnerabilities may exist and what attacks are possible
- **Reporting & Closeout**
  - Compile final report
  - Complete other deliverables as scoped
- **Demos & Experiments**
  - These are optional and depend on scope
  - Obtain special authorization
  - Formulate risk management plan
  - Test the exploitability of identified vulnerabilities

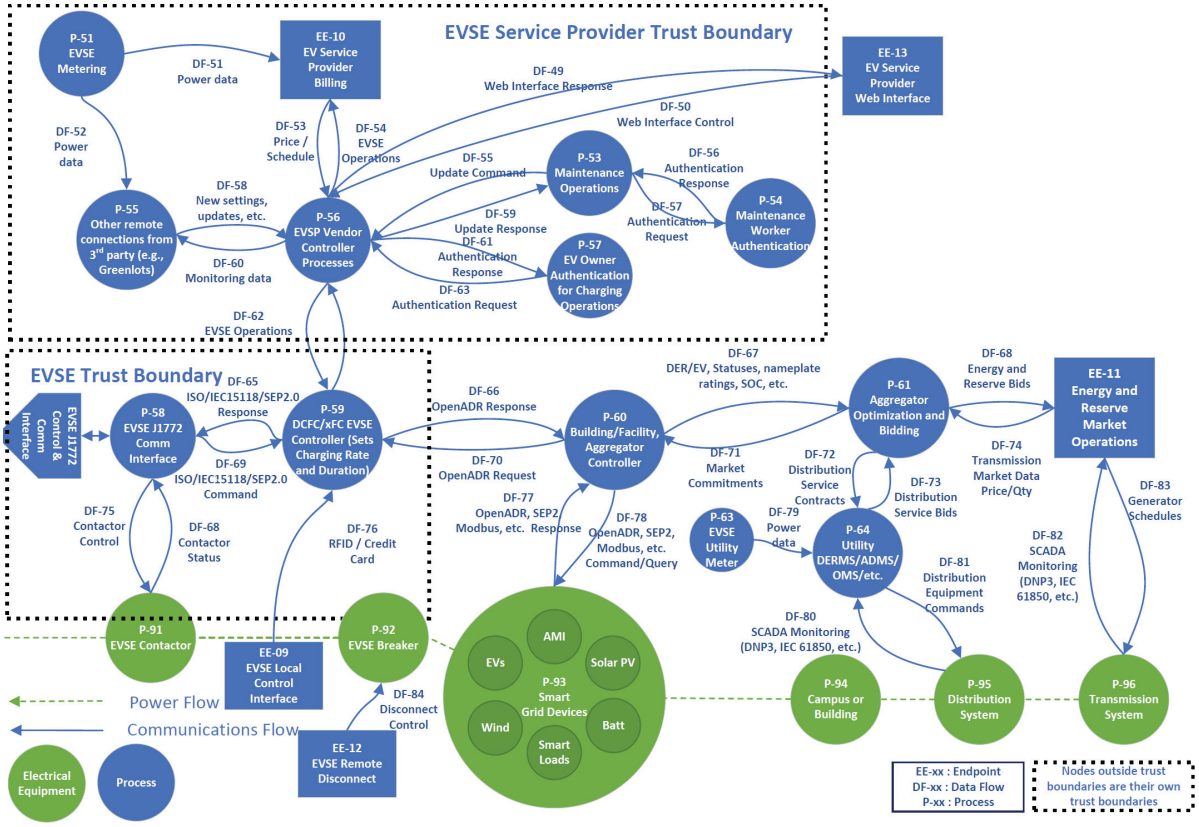
IDART
Information Design Assurance Red Team



PEV STRIDE Threat Model

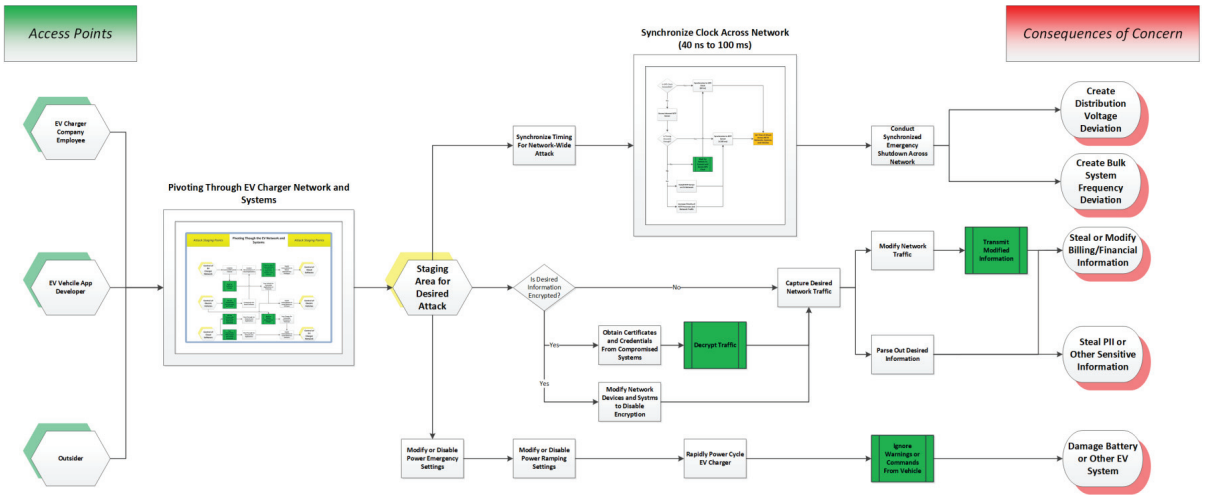


EVSE STRIDE Threat Model



EV Charging Attack Graph

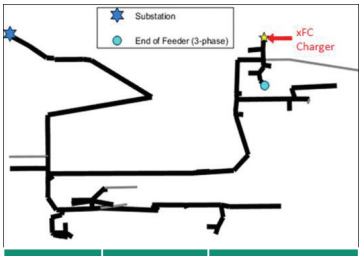
- Attack graphs show attacker actions to achieve an objective
  - Illustrates access points, staging areas, and consequences of concern
  - Graphically illustrates the steps an attacker must take to move from system/network access to the consequences of concern
  - Complex steps are displayed as images
  - Public vulnerabilities and red team results will further advise attack graph
- Two Major Concerns in Large-scale Attack:
  - **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?



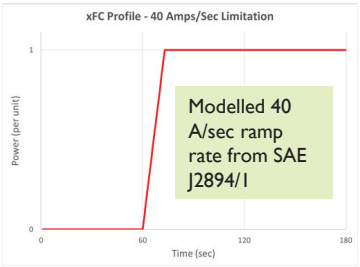
Distribution system impact analysis

Distribution Feeder Simulation

- System: Rural 12 kV distribution feeder, highly commercial load area
- Model containing 215 buses, 39 service transformers.
- 3-minute OpenDSS simulations
- Feeder voltage regulated via substation transformer load tap changer (LTC).

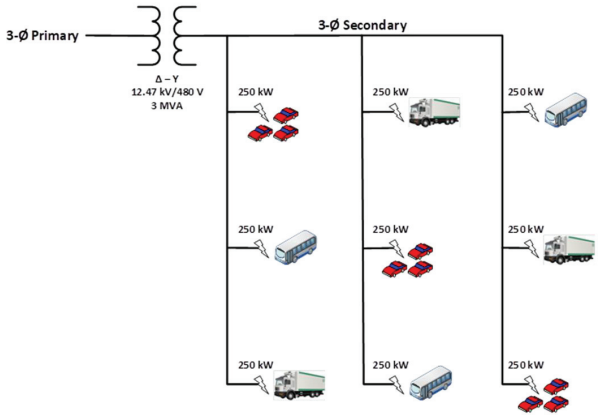


Load Period	Date/Time	Feeder Demand (kW)
Peak	7/22 @ 13:00	3946
Minimum	3/22 @ 23:00	1483



xFC Interconnection Model

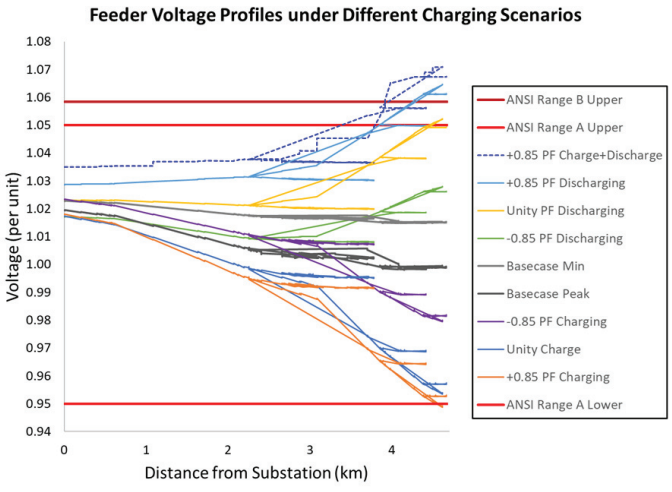
- 9x250 kW, 3-phase, 480 V stations simulated at the end of the feeder (2.25 MW total)
- Scenarios include charging sequences with and without V2G capabilities to generate high and low feeder voltages during peak and min load periods.
- Limited to ramp rate of 40 amp/sec, i.e. chargers get to full output in ~13 seconds.



Distribution System Impact Analysis

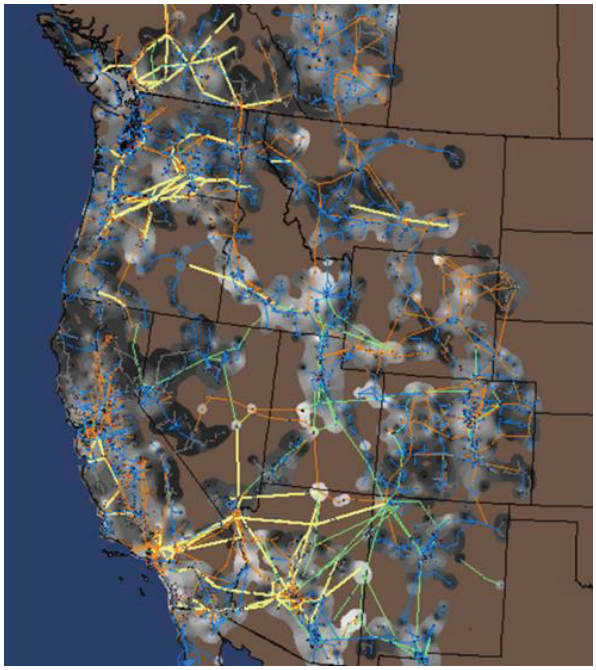
- Simulation cases:
  - Base cases with no chargers at each feeder load period (peak and min load)
  - Charging or discharging at unity PF and ±0.85 PF (i.e., with grid-support capabilities)
  - 150 s charge and then discharge case at 0.85 PF
    - charging causes the load tap changing transformer (LTC) to tap up so EV discharge creates higher voltages
- **Unity charging is within utility feeder voltage limits** defined by ANSI C84.1
- Grid-support features can help improve (or hurt) the voltage profile
- Several cases outside of ANSI C84.1 Range A, two cases outside of ANSI C84.1 Range B

Case	xFC Station Status	Load Period	Grid Impact	PCC Primary Voltage (120 V Base)	Charger Voltage (120 V Base)
LV_BC	N/A	Peak	Low voltage (basecase)	119.8	N/A
LV_Unity	All charging at unity PF	Peak	Low voltage (unity)	114.3	113.7
LV_85pf	All charging at 0.85 PF (absorbing VArs)	Peak	Low voltage (worst case PF)	113.1	110.7
LV_-85pf	All charging at -0.85 PF (providing VArs)	Peak	Low voltage (mitigation PF)	117.5	118.7
HV_BC	N/A	Min	High voltage (basecase)	121.8	N/A
HV_Unity	All discharging at unity PF	Min	High voltage (unity)	126.3	126.8
HV_85pf	All discharging at 0.85 PF (providing VArs)	Min	High voltage (worst case PF)	127.8	129.9
HV_-85pf	All discharging at -0.85 PF (absorbing VArs)	Min	High voltage (mitigation PF)	123.4	122.1
Dyn_HV 85pf	Charge+Discharge at 0.85 PF (providing VArs)	Min	High voltage (worst case PF)	128.5	130.6



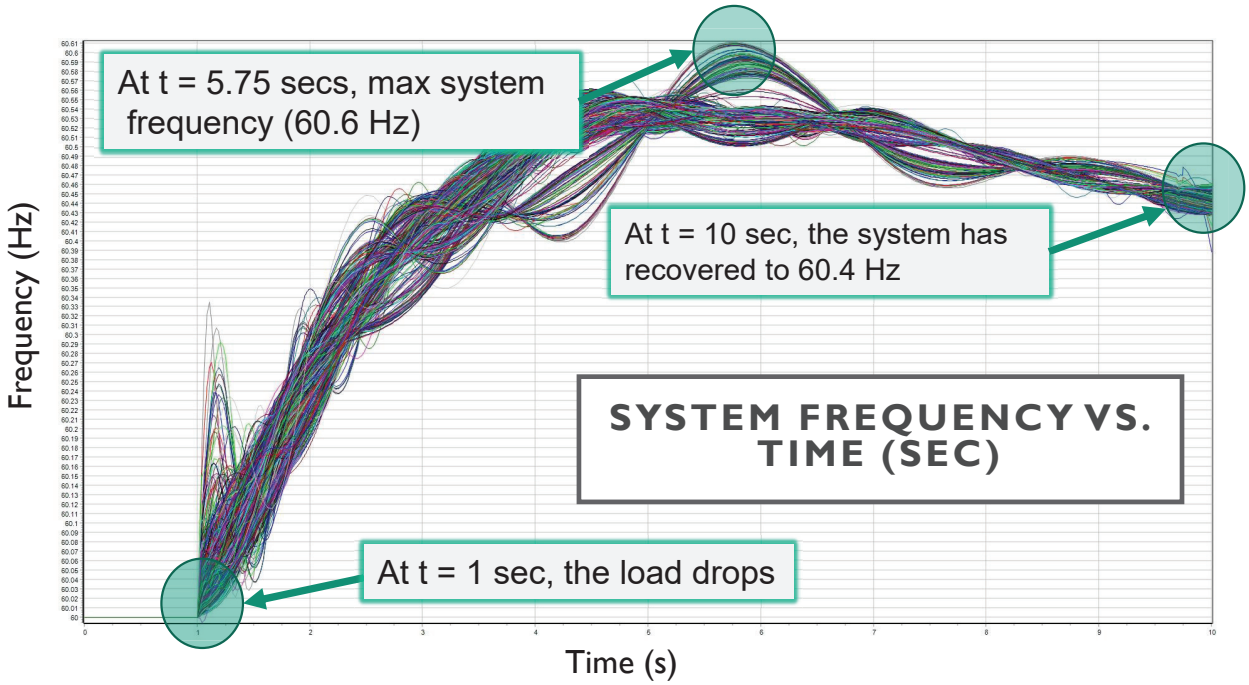
Transmission System Consequences

- Model: Full Western Electricity Coordinating Council (WECC)
  - British Columbia to Tijuana
  - All system protection (for generation and transmission) is modeled
  - Heavy summer usage case with 172 GW load
  - Software: GE's PSLF
- Load drop worst case scenarios
  - Simultaneous charging termination ("digital emergency stop")
  - The EVSE charging change impacted system voltage and frequency
- Results: frequency peak deviation was within NREC PRC-024-2 generator frequency protective relay settings (61.6 Hz for 30 sec)



Full WECC Model

Transmission System Full-WECC Response



System Response

- 10 GW simultaneous load drop throughout WECC (e.g., 22,000 EVSEs @ 450 kW)
- NO voltage or frequency limits were exceeded

Risk Matrix and Remediation Prioritization

- For each attack scenario, likelihood of success and potential power system impact will be used to estimate risk.
  - Risk = Probability * Impact
  - Probability: estimated from threat model and vulnerability assessments
  - Impact: determined from power system simulations
- Identifying highest risk scenarios will inform DOE and industry of mitigation priorities

Power System Consequence

Threat + Vulnerabilities

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Medium	Medium	Medium High	High	High
Likely	Low	Low Medium	Medium	Medium High	High
Possible	Low	Low Medium	Medium	Medium High	Medium High
Unlikely	Low	Low Medium	Low Medium	Medium	Medium High
Very Likely	Low	Low	Low Medium	Medium	Medium

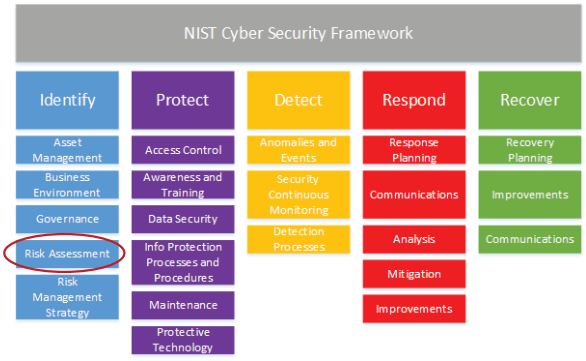
Remaining Challenges and Barriers / Future Research

This project is helping **identify potential EV charger vulnerabilities and quantify the risk to critical infrastructure** when vehicle charging infrastructure is maliciously controlled.

- First step in continuous process of hardening charging infrastructure against cyber-attacks.

Risk assessments are the beginning of a comprehensive approach to cybersecurity. Additional work must include:

- 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**.



15

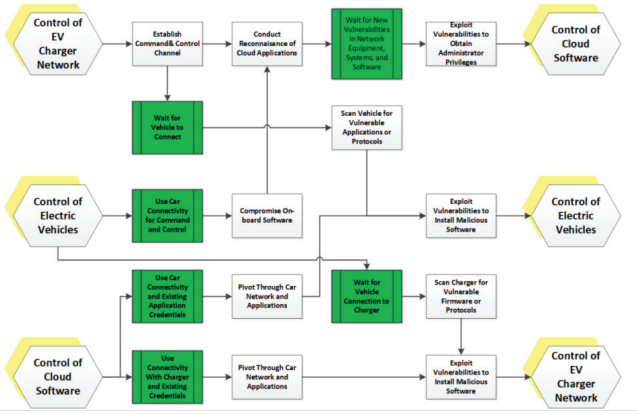
Summary

- **The goal of the project is to provide DOE and automotive, charging, and utility stakeholders with a strong technological basis for securing critical infrastructure**.
- By **collaborating closely with other government agencies and industry stakeholders**, we hope to generate a consensus threat model for EV charging and quantify the risk to the power system.
- To accomplish this, the team is:
  - Conducting adversary-based assessments of charging equipment
  - Enumerating EV/EVSE data flows and creating a STRIDE threat model of EV charging
  - Analyzing power system impact for different attack scenarios
- This is **only the beginning of a long process to secure charging infrastructure from cyber attacks**.

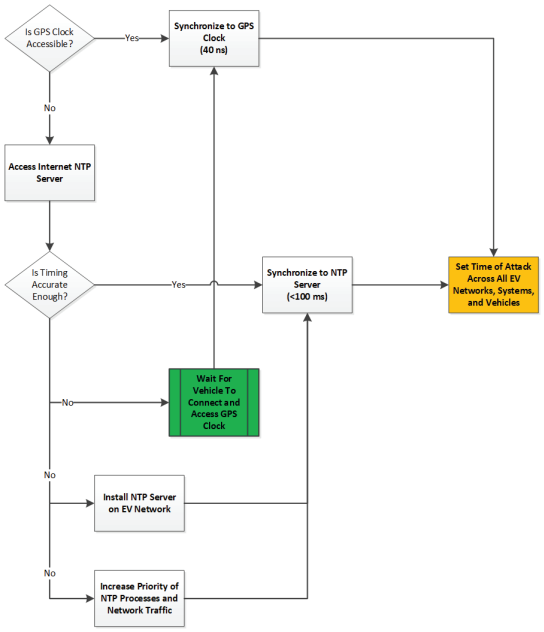
Backup Slides

Two Major Concerns in Large-Scale Attack

Pivoting Between Systems to Access Desired Data Flows



Synchronizing Attack Timing



Legend:

- Green hexagons are attacker access points
- Yellow hexagons are intermediate staging points
- Red ovals are the consequences of concern
- Rectangles are steps an attacker must take along the attack path
- Green rectangles are "No Ops" for the attacker (ex. Decrypt network traffic with compromised keys)
- Orange rectangles are "No Op Settings/Decisions" (ex. Selecting the time for an attack)

18

Threat Matrix

Threat Matrix is used as input to calculate the probability of a given attack.

- Some attacks require a high threat level (national state) and are, therefore, less likely.
- Other attacks could be conducted by a single, less-skilled "script kiddie"

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Federal Research in EVSE Cybersecurity:

Enabling Secure and Resilient XFC: A Software/Hardware-Security Co-Design Approach

Ryan M. Gerdes

Virginia Tech

September 12, 2019

Project ID elt207

This presentation does not contain any proprietary, confidential, or otherwise restricted information

Overview

Timeline

- 2018-10-01
- 2020-12-31

Barriers

- Compromise is difficult to detect, contain, and mitigate
- Remote remediation of compromise
- Maintaining operational capacity under compromise

Budget

- Total project funding
  - $2,500,000 DOE funding
  - $625,000 cost share

Partners

- Academic: *Virginia Tech*, Georgia Tech, Utah State University
- Industry: XFC Manufacturer, Commonwealth Edison Company, Ford Motor Co., Qualcomm (formerly OnBoard Security)

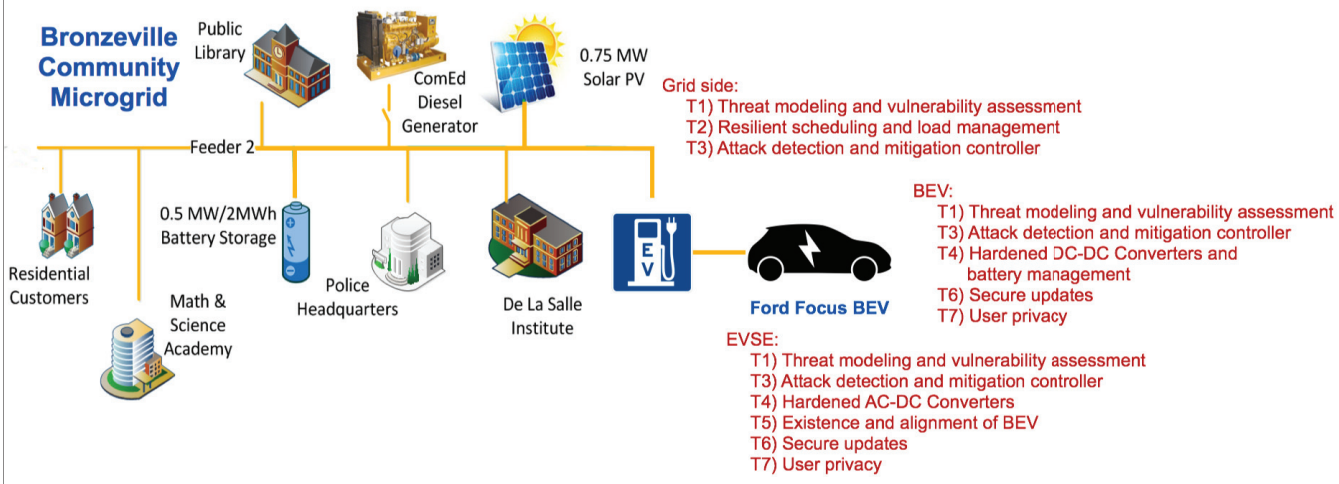
Relevance

- ***Enable the decrease in battery charge time in a secure and efficient manner***
  - coordination and cooperation between the grid, charging stations, and the vehicles
  - electric vehicle service equipment (EVSE) and the BEV themselves are untrustworthy
- **Resilient (and not just secure) system be put in place**
  - compromises of either BEV or EVSE are inevitable
  - maintain some operational capacity while guaranteeing safety
- **Motivating threats:**
  - A network of compromised EVSE could be used to simultaneously discharge the batteries of BEV
  - Compromised BEV, with possible collusion from compromised EVSE, drawing from the grid in a coordinated manner so as to cause instability
  - Malware being spread from a BEV to other BEV through the compromise of single or multiple EVSE

Approach

- **State-of-the-Art**
  - design process used for safety critical systems does not produce inherently more secure systems (e.g., automotive systems)
  - proprietary and/or high-level requirements
  - cyber-centric (best practices)
  - lack cyber-physical systems security perspective
- **Hardware/software-security (HW/SW-Sec) co-design approach**
  - security-hardened controllers, converters, and monitoring systems: secure sensing/actuation techniques, moving-target based detection and mitigation strategies
  - guarantee successful remediation of vulnerabilities in EVSE/BEV through remote updates
  - respecting end-user privacy
  - conductive and inductive charging at power levels of 200 kW to 400

Approach



Approach: Task 1

- **Cyber-physical threat and vulnerability assessment of EVSE/BEV/grid systems using a game-theoretic risk analysis and an automatic attack graph generator**
  - specify attacker characteristics, attack vectors, and assets
    - Traditional: Threat Analysis and Risk Assessment (TARA) for EVSE/BEV/grid
    - New: game theoretic approach (cost-vs-benefit analysis using structural non-equilibrium level-k thinking)
    - New: EVSE/BEV-specific automatic attack assessment tools for common interfaces and systems
  - first step in security co-design process: identify risks, failure states, and fail-safes
- **Novelty: differing rationalities and decision-making mechanisms; automatic generation of attack graphs of non-quasi-static and cyber-physical systems**
- **Need served: no clear threat model or trust model for the EVSE/BEV space; tools for automatic assessment; estimates of costs and capabilities of attackers under various threats**

Approach: Task 2

- **Performing experimentally-validated, grid-side modeling of XFC loading on a microgrid and using a reachability analysis to determine the safety of a given charge request**
  - detect and mitigate attacks under modeling uncertainty: determine if a sequence of charging events would result in grid instability
  - Bronzeville Community Microgrid testbed: empirical models developed in Opal-RT and RTDS and hardware-in-the-loop simulations (islanded and grid-connected)
    - non-attack: BEV charging profiles, baseline load, voltage and frequency profiles of the microgrid under different charging scenarios (non-attack)
    - attack scenarios: reachability analysis to define the unsafe states the system will not be allowed to enter
    - mitigation: moving-target defense for microgrid controller
- **Novelty: reinforcement learning to learn and refine system models so as to be robust against modeling uncertainty under attack**
- **Need served: how XFC chargers can be operated with minimal negative impact on the grid, even under attack**

Approach: Task 3

- **Development of a moving-target defense (MTD) for sensor and actuator attacks against EVSE/BEV/grid controllers**
  - adversarial agents may directly impact either via a corrupting actuator, sensor, or inter-agent (system) communication channels
  - goal: disruption of resources without detection
- **deep Q-learning structures (learn attacker and system over time) for model-free defense**
  - a framework to facilitate deception of potential attackers
  - switching of controllers for optimality and unpredictability
  - guarantee stability of the overall system for switched controllers
  - identify potentially corrupted sets of controllers/sensors/actuators
- **Novelty: model-free secure optimal feedback policies for EVSE/BEV systems**
- **Need served: resilient system (i.e., EVSE, BEV, and grid controllers individually and together) capable of learning and achieving its objective in the presence of adversarial agents**

Approach: Task 4

- **Designing AC-DC (for EVSE) and DC-DC (for BEV) converters and battery management systems (for BEV) capable of resisting false data and false actuation attacks by leveraging redundancy, diversity, and watermarking**
  - attacker: identify the fail-safes in converter and battery management systems (cyber and cyber-physical)
  - iterative design process for BMS and converters: identify fail-safes, attack, and then harden
    - determining which points of the systems are most vulnerable to a particular type of attack and determining whether redundancy can cost-effectively provide increased tolerance to attack (defense one)
    - devising models that relate diverse sensor measurements (defense two)
    - integrated MTD (defense three)
    - creating a two-way watermarking system that would allow a controller to know that an actuation signal was acted upon (detect)
- **Novelty: hardening approaches validated against attacks in a realistic full power system environment**
- **Need served: last line of defense at the vehicle to prevent damage; cyber-physical protection for EVSE/BEV**

Approach: Task 5

- **Using device fingerprinting to determine whether an actual EV is connected to the EVSE; building a secure ranging system with spoofing detection to ensure that a vehicle is properly and safely aligned with the charging pad**
  - attacker: compromised EVSE could coordinate charging into phantom vehicles to cause under-voltage on the grid; if a BEV is not properly aligned compromised could cause damage
  - EVSE can know vehicle is present:
    - charging characteristics can be used to classify BEV: robust to battery state of charge and ambient temperature
    - inductively charged BEV detected through changes of inductance of the charging pad
  - EVSE can know vehicle is aligned: secure ranging based on redundant semi-securing ranging systems (IR-UWB) and attack detectors
- **Novelty: secure ranging systems are rare and require specialized hardware; incorporate COTS components and still yield a high degree of security**
- **Need served: verify that an actual vehicle is being charged and vehicle is properly aligned (to reduce occurrence of A1,2)**

Approach: Task 6

- **Leveraging a trusted-computing base to guarantee that a formally verified, remote firmware update procedure takes place, even in the case of unreliable primary communications**
  - inevitable that vulnerabilities in EVSE will be discovered and exploited
  - light-weight crypto and a trusted computing base (TCB) for the embedded system running the EVSE firmware
  - update procedure will exist entirely in the TCB and be formally verified to ensure that it is free of vulnerabilities
  - secondary communication channels will be investigated to guard against denial of service
  - side-channel resistance: fuzzy extractor for key generation based on grid signals
- **Novelty: guarantee that firmware will be patched even when an adversary is allowed physical access to the system**
- **Need served: a resilient secure update procedure for EVSE/BEV integrated into existing frameworks (UPTANE)**

Approach: Task 7

- **Extending the ISO/IEC 15118 protocol to ensure user privacy even in the case of untrustworthy agents or when communication has been impaired**
  - charging infrastructure require protocols and standards that control authentication, authorization, and billing of BEV charging
  - Privacy Impact Assessment (PIA)
  - extended ISO/IEC 15118 protocol for privacy preservation:
    - untrustworthy agents at each of the transaction and
    - providing privacy guarantees even when connectivity between the charger and billing service is unavailable
- **Novelty: no significant mechanisms for privacy protection in place in existing protocols**
- **Need served: first open-source end-to-end solution for managing user credentials and data between differing network operators**

Approach: Milestones (FY2019-20)

Milestone	Type/Status	Description
Threat models (06/2019)	Technical (Complete)	TARA report that lists the main threats to focus on later in the project
Microgrid model (09/2019)	Technical (Ongoing)	The model of Bronzville microgrid is developed in real-time simulators
New designs for converter and BMS hardware (12/2019)	Technical (Ongoing)	Critical design review completed with team and program manager approval of hardened designs
MTD techniques with theoretical stability, optimality, and robustness guarantees (03/2020)	Go/No-Go (Ongoing)	A proactive and reactive defense framework for the EVSE/BEV/grid controllers

- **Hardware to be deployed:**
  - ChargePoint XFC charger (October 2019, Chicago, IL)
  - Ford Focus BEV (Blacksburg, VA & Boston, MA)

Approach: Milestones (FY2020)

Milestone	Type	Description
Privacy Impact Assessment of EVSE/BEV communication (06/2020)	Technical	Analyze data flows to identify personally identifiable information and ensure appropriate privacy controls
Vulnerability assessment of EVSE/BEV-grid interactions (09/2020)	Technical	Attack trees and attack graphs.
Trade-offs of grid-side resiliency approaches (12/2020)	Technical	Trade-offs for BEV-induced attacks are quantified
Install and demonstrate the technology within the Bronzeville Community Microgrid (03/2021)	Go/No-Go	Successful field demonstration given the minimum negative impact during the planning study

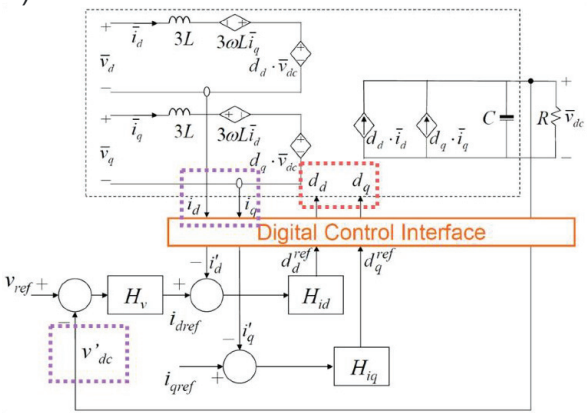
- **Hardware to be deployed:**
  - USU XFC (conductive & inductive) bus (Logan, UT)

Technical Accomplishments and Progress

- **Threat assessment of EVSE/BEV/grid using TARA methodology (T1, M1)**
  - BEV assessment (nearly) complete
  - EVSE/grid assessment to be completed upon integration of EVSE into research lab (Q4, 2019)
  - Participation in NMFTA XFC Cybersecurity Working Sub-Group A
- **Vulnerability assessment of a Ford BEV (T1, M2)**
  - Identify safety-critical faults, methods to detect, and fail-safes: induce, mask, and subvert
  - 18 attack vectors identified: Permanent disabling/degradation of vehicle and harm to occupants/persons nearby
  - Validation of four high-impact vectors
  - Ten undergraduate researchers
- **Gather electrical characteristics of the Bronzeville Community Microgrid (T2, M5)**
  - Anonymized data collected for construction of OPAL-RT and RTDS models

Technical Accomplishments and Progress

- **Trust Models of EVSE/BEV/grid (T1, M3)**
  - Attack vectors: delay, jamming, false-data injection, false-actuation injection
  - Initial system: AC/DC Converter (linearized)
  - Game theoretic formulation that allows for
    - Level-k hierarchy (differing rationalities and capabilities)
    - Goal: make system unstable, uncontrollable, or unobservable (eventually arbitrary unsafe states)
    - Expenditure of resources
      - Incorporation of costs
      - Attack points and number
      - Defensive strategies
        - » Redundancy
        - » Diversity
        - » Encryption



U.S. DEPARTMENT OF ENERGY OFFICE OF ENERGY EFFICIENCY & RENEWABLE ENERGY 16

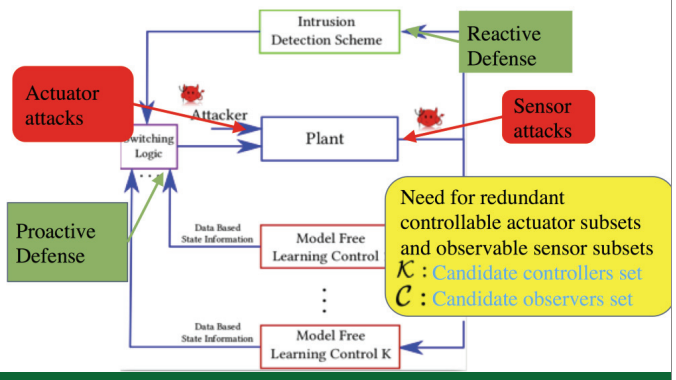
Technical Accomplishments and Progress

- **Trust Models of EVSE/BEV/grid (T1, M3)**
  - Attack vectors: delay, jamming, false-data injection, false-actuation injection
  - Initial system: AC/DC Converter (linearized)
  - Hybrid systems formulation that incorporates
    - Sensing, actuation, legitimate control, and communication
    - Manual specification of attacker objective(s)
    - Tractability: NP hard
      - Branch-and-bound
      - SAT solver to prune state space
    - Novel attack sequences discoverable

$$\min_{\mathbf{u}_a(t)} \quad ||\mathbf{x}(t) - \mathbf{x}_a(t)||_p$$
$$\text{s.t.} \quad \dot{\mathbf{x}}(t) = f\left(\mathbf{x}(t), \mathbf{u}(t), \mathbf{u}_a(t)\right)$$
$$\mathbf{u}_a(t) \in \{\text{delay, jamming, fdi, fda}\}$$

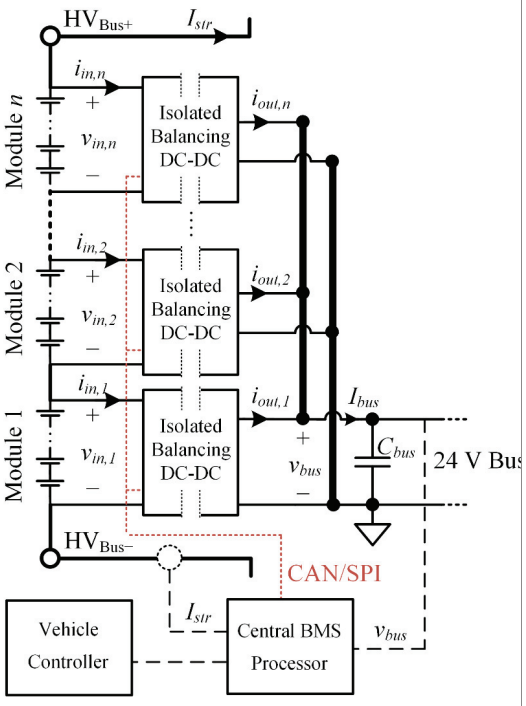
Technical Accomplishments and Progress

- **Proactive and reactive defense mechanism (T3, M8)**
  - Use of redundant sensor and actuators (generic CPS)
    - Switch active unit(s) in unpredictable and stochastic fashion
    - Increases cost to attacker with minimal cost to defender
  - System/environmental uncertainty: optimality achieved using non-equilibrium intermittent learning
  - Reactive defense necessary
    - Attacker goals realized under traditional MTD
    - Isolate the suspicious units
    - Continued safe operation



Technical Accomplishments and Progress

- **Iterative design of AC-DC converter and active BMS plus DC-DC converter (T4, M9)**
  - 480 V 3-phase ac input, 350 kW rated power XFC using 5 modules with 70 kW rated power each
  - Major power components for the AC/DC converter have been selected
  - Models for battery state-of-charge/health
  - Initial topology and control design of the BMS module (DC-DC converter and battery monitoring) with the consideration of cyber-physical security hardening
    - Analyzing the potential attack points of the system
    - Investigating the possible attack types for the potential attack points in the system
    - Determining which points of the systems are most vulnerable to a particular type of attack



Collaboration and Coordination

- **Academic Partners:**
  - Virginia Tech (Prime): cyber-physical systems security; micro and smart grid; sensor integration; intelligent transportation systems
  - Georgia Tech (Sub): optimal, adaptive control; game theory; reinforcement learning
  - Utah State University (Sub): Development and commercialization of electric vehicle fast charging equipment (inductive and conductive) and custom active battery management systems
- **Industry Partners:**
  - XFC Manufacturer (Sub): supplier of XFC unit(s)
  - Commonwealth Edison Company (Sub): one of the nation's largest electric utilities; evaluation and development of emerging grid technologies, including but not limited to energy storage and microgrid systems.
  - Ford Motor Company (Sub): expect to have 24 hybrid and 16 fully electric vehicles in their model lineup and $11 billion invested in BEV
  - OnBoard Security (Sub): cyber-physical systems security, CIA analysis, vulnerability assessment and design of embedded and intelligent transportation systems

Remaining Challenges and Barriers

- **Assessment and countermeasures**
  - Guarantees for linear time-invariant systems, only
  - Unsafe states for non-linear systems must be specified
  - Incorporation of cyber attacks into cyber-physical frameworks
- **Disparate knowledge/simulation domains across teams**
- **Physical realization of countermeasures**
  - Generic cyber-physical systems provably secure (against known attacks)
  - Implementations are flawed
    - Design of redundant /diverse sensing regimes not vulnerable to common (same) attacks
    - Cost-effective and resilient parallel actuation strategies
    - Redundancy/diversity leading to exponential gains in security (commonly only linear)

Proposed Future Research

Milestone #	Task	Milestone
3 (ongoing)	Trust Models (VT lead, GT, OBS, XFC, Ford, ComEd support) (M1-12)	Comprehensive list of attack points and the utility of attacking/defending them.
4	Vulnerability Assessment of EVSE (OBS lead, VT and XFC support) (M7-12)	Attack trees and attack graphs that indicate likely compromise points and the attack sequence necessary to achieve attacker goals.
6 (ongoing)	Develop a simulation circuit of the Bronzeville Community Microgrid (ComEd lead, VT support) (M7-9)	The model of Bronzville microgrid is developed in real-time simulators
7	Create BEV charging profiles using Monte Carlo simulation and insert BEV charging units with variation of charging profiles into the microgrid (VT lead, ComEd support) (M10-12)	Different BEV charge profiles are created based on real-world data
8 (ongoing)	Combined proactive and reactive defense mechanism (GT lead, VT support) (M1-12)	A proactive and reactive defense framework for the EVSE/BEV/grid controllers.
9 (ongoing)	Iterative design of 300 kW AC-DC converter and 5 kW integrated active BMS plus DC-DC converter (USU lead, VT, GT, OBS, and XFCsupport) (M1-6)	Critical design review completed with team and program manager approval of hardened designs.
10 (ongoing)	Hardware construction of BMS with integrated 5 kW DC-DC for vehicle LV loads (USU lead) (M7-12)	Hardware demonstration with functional operation of modified battery pack, BMS, and DC-DC and functional test of hardening features.
11 (ongoing)	Hardware construction of 60 kW module prototype for AC-DC converter (USU lead) (M7-12)	Hardware demonstration with functional operation of the 60 kW module with verified communications to a central AC/DC controller and verified hardening feature operation.

Proposed Future Research

Milestone #	Task	Milestone
12 (ongoing)	Devising device fingerprinting methodologies for conductive and inductive chargers (M7-12)	
13 (ongoing)	Creation of formally verified update procedure (OBS lead, VT and XFC support) (M1-12)	A TCB-based routine capable of initiating remote update procedure, authenticating firmware, and installing it.
14	Allowing updates to EVSE when primary communication channel is disabled (OBS lead, VT and XFC support) (M6-12)	Proof-of-concept demonstration that update routine can fall-back to secondary communication channel.
15	Privacy of EVSE-BEV, EVSE-Grid communication (OBS lead, VT support) (M7-12)	Privacy Impact Assessment of EVSE/BEV communication: The PIA analyzes the data flows to identify personally identifiable information. Data collection, retention, use, disclosure are then analyzed to ensure appropriate privacy controls.

Summary

- **Goal: secure and efficient charging**
- **Approach: hardware/software-security (HW/SW-Sec) co-design**
  - Develop security-hardened controllers, converters, and monitoring systems for XFC
    - maintain user privacy
    - secure sensing and actuation techniques
    - learning-enabled moving-target defense
    - remediation of vulnerabilities through remote updates
  - Benefits
    - Minimizing (secure) design time of future systems
    - Address findings of vulnerability assessments
    - Critical infrastructure that can resist (as a function of cost), and be resilient to, attack
  - The feasibility demonstrated on a real-world testbed that includes an XFC unit and BEV situated in a microgrid
  - Multi-disciplinary team and industry-academic partnership
    - Unique perspectives and expertise to examine threats and solutions

Consequence-driven Cybersecurity for High Power EV Charging Infrastructure

www.inl.gov

Idaho National Laboratory

Kenneth Rohde
Barney Carlson

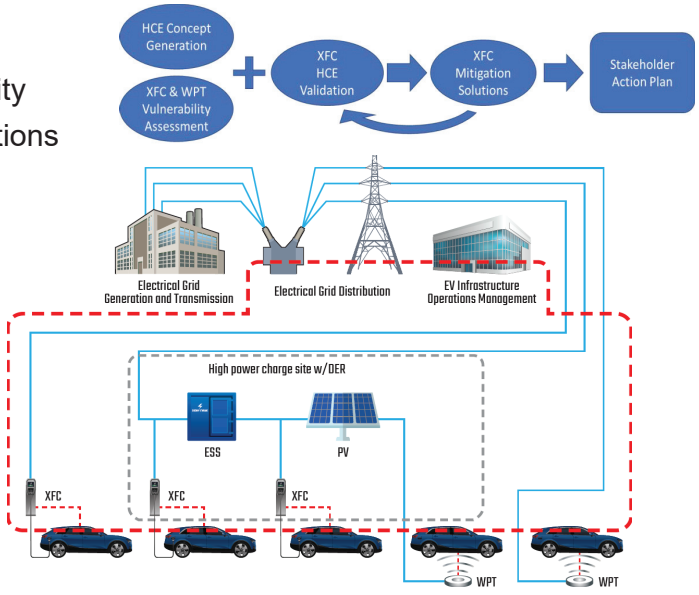
Sept. 12, 2019

INL/MIS-19-55540

Project Overview: Consequence-driven Cybersecurity for High Power EV Charging Infra.

Idaho National Laboratory

- ✓ Conceptualize high consequence events (HCE) caused by cyber manipulation for high power EV charging infrastructure
- ✓ Quantify and prioritize high consequence events
- Evaluate impact severity and cybersecurity complexity
- Develop and evaluate mitigation strategies and solutions
- Publish findings, solutions, and strategies



Idaho National Laboratory · NREL National Renewable Energy Laboratory · Oak Ridge National Laboratory · ABB · TRITIUM · electrify america

3 yr. Project Timeline

3

Categories: High Consequence Events for High Power EV Charging Infrastructure

- Grid Impacts
  - Disruption to the electrical distribution network(s) feeding the charger site(s)
    - Power outage, voltage instability, harmonics / distortion, etc.
- Hardware Damage
  - Damage to the charger(s), vehicle(s), or other equipment at the charger site
    - Not included: weather, accident, vandalism, etc.
- Safety
  - Public or occupational safety
    - EV driver, charger user / operator, public nearby, etc.
- Denial of Service
  - Unable to provide the necessary energy transfer to fulfill the EV charging requirements
    - Out of order, unable to charge, etc.
- Data Theft or Alteration
  - Personal, monetary, or business data / information
    - Account info, PII, cargo or route info, etc.

4

HCE Scoring & Prioritization

HCE Score = Impact ✖ Complexity

- Impact Severity
  - Severity based on 8 criteria
  - Weighting factor used for the 8 criteria
- Complexity Multiplier
  (ease of cyber-manipulation)
  - Number of attack vectors required to be concurrently manipulated
  - Expertise of attacker(s)

HCE Scoring

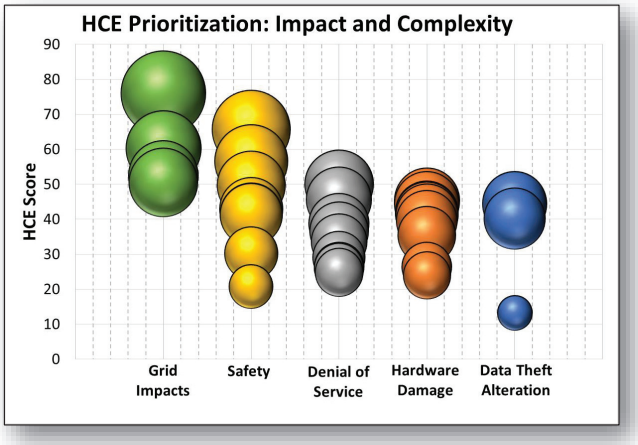
Complexity Multiplier	Impact Severity 1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Impact Severity Scoring

Criteria	N/A (0)	Low (1)	Medium (3)	High (5)
Level of Impact	N/A	Single unit affected (EV, XFC, or WPT)	Multiple units at a single site affected (EV, XFC and/or WPT)	Multiple unit at multiple sites affected (EV, XFC and/or WPT)
Magnitude (proprietary or standardized)	N/A	Manufacturer specific protocol implementation (EV or EVSE)	>1 manufacturers protocol implementation (supply chain) (EV or EVSE)	Across all standardized systems (both EVSE and EVs)
Duration	N/A	< 8 hours	> 8hr to < 5 days	> 5 days
Recovery Effort	Automated recovery without external intervention	Equipment can be returned to operating condition via reset or reboot (performed remotely or by on-site personnel)	Equipment can be returned to normal operating condition via reboot or servicing by off-site personnel (replace consumable part; travel to site)	Equipment can be returned to normal operating condition only via hardware replacement (replace components, requires special equipment, replace entire units)
Safety	No risk of injury	Risk of Minor injury (no hospitalization), NO risk of death	Risk of serious injury (hospitalization), but low risk of death	Significant risk of death
Costs	No Cost incurred	Cost of the event is significant, but well within the organization's ability to absorb	Cost of the event will require multiple years for financial (balance sheet) recovery	Cost of the event triggers a liquidity crisis that could result in bankruptcy of the organization
Effect Propagation Beyond EV or EVSE	No propagation	Localized to site	Within metro area; within single distribution feeder	Regional; impact to several distribution feeders
EV Industry Confidence, Reputation Damage	No impact to confidence or reputation	Minimal impact to EV adoption	Stagnant EV adoption	Negative EV adoption

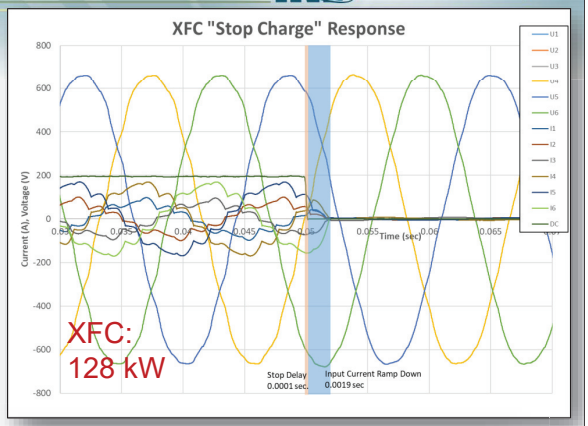
Prioritized HCE List

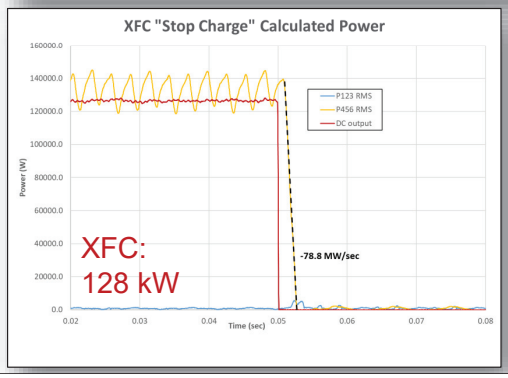
- Prioritized HCEs based on impact severity and cyber manipulation complexity:
  1. *Grid Impacts*: Utility power disruption due to sudden load shed or increase of XFC site
     - XFCs concurrently stop charging (load shed) or site ESS step load increase
  2. *Safety:* Shock / burn hazard from damaged cord set due to thermal cooling system manipulation
  3. *Safety:* EM-field public exposure near wireless charger
     - Especially people w/ a portable medical devices (pacemakers, insulin pumps, etc.)
  4. *Grid Impacts*: Charger site non-responsive to load management or aggregator commands
     - Curtailment requests, VAR support, load scheduling
  5. *Grid Impacts*: Feeder equipment damage
     - Overload, extended operation outside of nominal conditions, cycling resulting in reduced hardware life
  6. *Loss of Service*: No power transfer functionality
     - Error state in charger or site controls caused by cyber manipulation
  7. Approx. 45 more…….



1. Grid Impact: Sudden XFC Load Shed

- Concurrent “stop charging” of multiple XFC
  - Ramp down from full power to standby **in .0025 sec** (equivalent to ~128MW/sec for each XFC at 320kW)
    - Same “stop time” duration (.0025 ±.0006 sec)
      - normal “stop charge” request from EV or user
      - XFC error state resulting in stop charging
- Event:
  - Cyber manipulation resulting in the XFC to stop charging
  - Significant potential to coordinate multiple XFC to stop charging simultaneously
- Impact:
  - Sudden load shed can potential cause
    - Distribution feeder voltage instability
- Potential mitigation solution:
  - Use of local energy storage to isolate or dampen fast transients from distribution feeder network
  - TBD (future work)





Any future work is subject to change based on funding levels

2. Safety: XFC Cord Set Cooling System Manipulation

- XFC thermal system manipulation
  - Thermal sensors spoofed causing no cooling of cable and connector (insulation failure)
  - Unique vulnerability to XFC with a liquid cooled cable
- Event:
  - XFC cable failure / melting
- Impact:
  - Public safety & hardware damage
    - Burn or shock hazard (depending upon state of insulation)
    - Cable replacement required
- Potential mitigation solution:
  - Minimum coolant flow rate
  - Redundancy:
    - Flow rate based on current & thermal sensors used to trim flow rate
  - Vehicle-side inlet temperature measurement
    - IEC 61851-23
    - ISO/DIS 17409
  - TBD (future work)

Any future work is subject to change based on funding levels

3. Safety: WPT Operation with NO Vehicle Present

- WPT primary coil (ground-side) operating at full current
  - Wireless communications spoofed causing WPT operation with no EV present
  - Unique vulnerability to WPT
- Event:
  - Ground-side coil operation at full current with NO vehicle present
- Impact: potential public safety
  - EM-field exposure
  - Metallic object heating
  - Medical devices interaction
- Potential mitigation solution:
  - TBD (future work)

Any future work is subject to change based on funding levels

9

Initial Red Team assessment of ABB TerraHP - 350 kW (XFC)

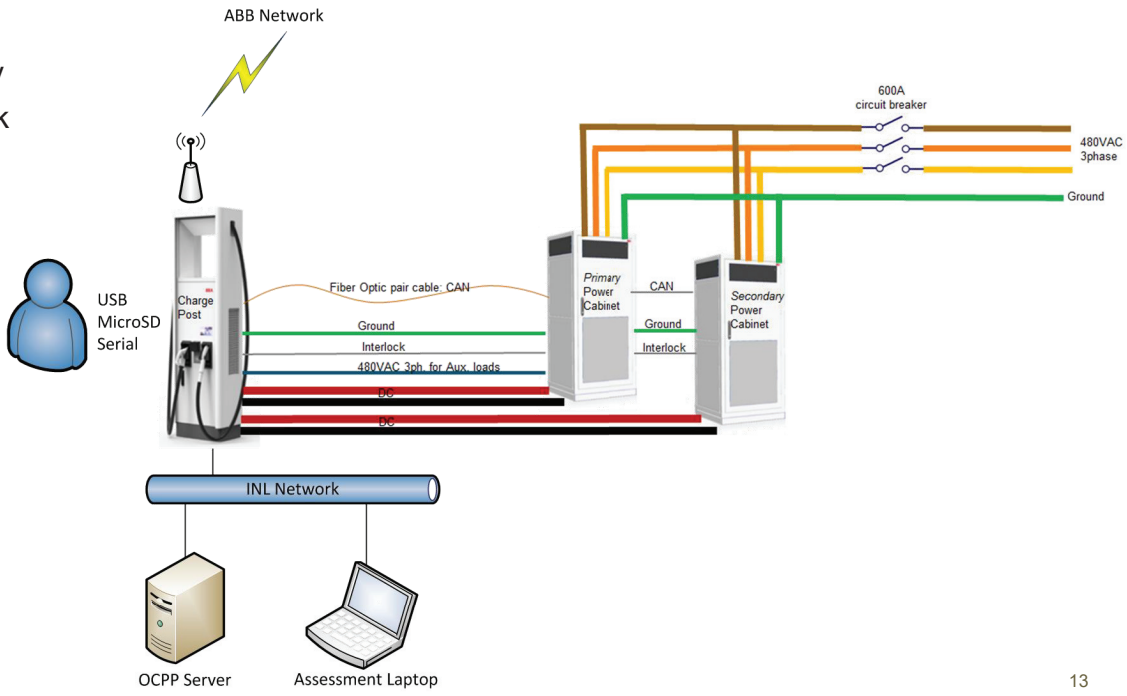
11

INL Red Team Assessment: ABB TerraHP (XFC)

1. **Identify Attack Pathways**
   - In what ways are this station reachable by the general public?
2. **Identify Vulnerabilities**
   - What vulnerable services and software are present on the station?
3. **Attempt System Compromise**
   - Can we gain unauthorized access to critical systems?
4. **Provide Mitigation Recommendations**
   - What can be done to harden the system?

1. Identify Attack Pathways

- Cellular Network
  - ABB Connectivity
- Local Ethernet Network
  - INL Connectivity
- Physical Access



1. Identify Attack Pathways

- **Cellular Network (ABB Connectivity)**
  - Remote access is only available if the attacker is located on the ABB network
  - System is relying upon the proper configuration and security settings provided by the Cellular carrier

- **Local Ethernet Network (INL Connectivity)**
  - Connected to an isolated network switch
  - Requires typical network services for access (e.g. DHCP)
  - OCPP functionality is provided

- **Physical Access**
  - The HMI screen has very limited connectivity
  - Requires physical access to the station (charge post)
  - Cabinet is typically locked (doors have proximity switches)
  - Extremely dangerous when the system is powered on due to high voltage / arc flash hazard

14

2. Identify Vulnerabilities

- **Cellular Network (ABB Connectivity)**
  - INL does not have a CRADA or NDA in place with ABB
    - We cannot connect to or test from the ABB network
    - Limited to the web portal to our XFC
  - Parallel efforts by ABB R&D will hopefully address this connection
  - Direct communication with the cellular hardware to attempt compromise is still possible

- **Local Ethernet Network (INL Connectivity)**
  - Vulnerable to basic networking attacks
    - ARP poisoning
    - DNS injection
    - Router manipulation
  - Provides remote access via OpenSSH version 7.5
    - There are no current “high” or “critical” known vulnerabilities for this version
  - OCPP server is located on this network
    - Connections are outbound from the station to the server
    - Manipulation of these communications require man-in-the-middle attack techniques
    - INL OCPP server is still in development

15

2. Identify Vulnerabilities *(continued)*

- **Physical Access**
  - The Charge Post is most at risk of intrusion
    - The HMI screen provides all connectivity
  - The Power Cabinets are usually located behind a high fence
  - HMI physical access protections are very strong
    - Several attempts at breaking into the system have so far failed
      - USB, bootloader, MicroSD, keyboard, etc.

3. Attempt System Compromise

- Unauthorized access will likely only succeed with physical access
- The potential for remote compromise is very low
  - The OpenSSH server needs to be continually updated as vulnerabilities are discovered
- The OCPP client on the station might have vulnerabilities

4. Provide Mitigation Recommendations

- Mitigation solutions developed during this project will be provided in later stages of this project

16

Summary: INL Red Team Assessment of ABB TerraHP (XFC)

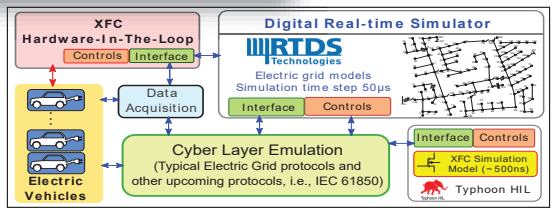
- Assessment is ~50% complete
- This 350 kW XFC station is significantly more secure than the 50 kW DCFC (predecessor)
- Compromise of this system, in actual deployment, will be difficult

17

Future Research: Laboratory Evaluation & Mitigation Development

Assess the *highest* prioritized HCEs:

- Validation of cyber manipulation complexity:
  - Laboratory evaluation with high power EV charging hardware and hardware-in-the-loop capabilities
- Evaluation of :
  - HCE Impact Severity
  - Vulnerability manipulation complexity
- Guidance and recommended solutions
  - Solutions to hardened attack surfaces and close vulnerabilities
  - Methodology to safeguard personal information & data
  - Methods to identify occurrence of cybersecurity malicious event
  - Response during and after cybersecurity malicious event



Any future work is subject to change based on funding levels

Summary:

- List of High Consequence Events for high power EV Charging infrastructure
  - Completion of scoring and prioritization based on:
    - Impact Severity
    - Complexity Multiplier
- Red Team assessment of XFC is in progress
  - Initial findings: very secure, difficult to compromise
- Prioritized HCE list will guide / prioritize the next steps in the project
  - Laboratory evaluation and verification of
    - Impact severity
    - Cyber complexity multiplier
  - Refine HCE prioritization list based on evaluation findings
- Develop mitigation strategies and solutions for highest prioritized HCEs
- Publish results and findings

DOE Vehicle Technologies Office
Cyber-Security of On-Road Transportation:

Cybersecurity for Grid Connected eXtreme Fast Charging (XFC) Station (CyberX)

PI: David Coats (Previously Junho Hong)

ABB Inc.

9/12/2019

This presentation does not contain any proprietary, confidential, or otherwise restricted information

Overview

Timeline

- Project start date: 01/2019
- Project end date: 12/2020
- Percent complete: 30%

Barriers

- Barriers addressed
  - Designing XFC station considering future extensions and security needs
  - Identify/detect anomalies in the XFC station
  - Integrate the prototype result into HIL testbed

Budget

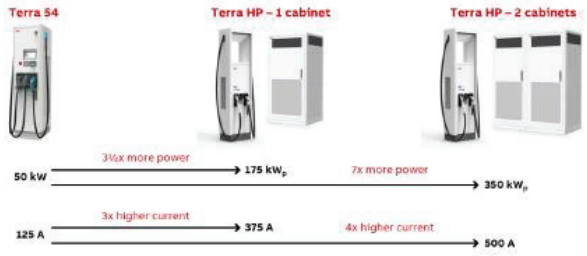
- Total project funding
  - Total: $2.1 M
  - DOE share: $1.68 M
  - Cost share: $0.42 M (20%)

Partners

- **INL**: Power hardware-in-the-loop simulator for demonstration, Don R Scoffield(lead)
- **APS Global**: Electric distribution system model and threat analysis, Karl Heimer (lead)
- **XOS Trucks**: Electric vehicle for demonstration testing, Austin Benzinger (lead)

Objectives

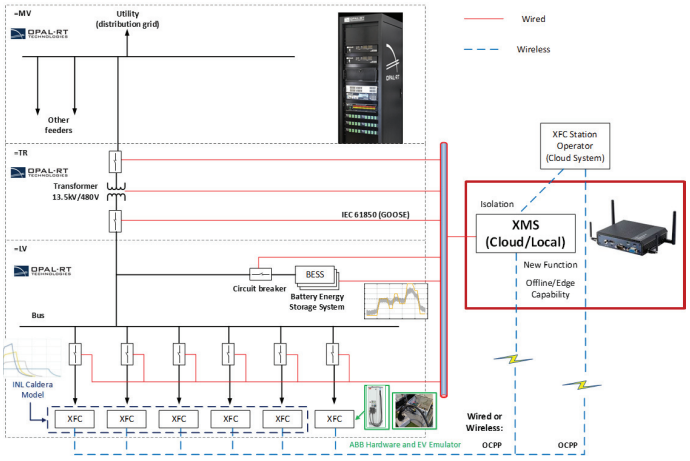
- **Research, develop and demonstrate a resilient AC input XFC (>350kW) station that reduces the risk and impact of cyber intrusions**
  - Reduce the false positive/negative ratio of anomaly detection
  - Prototype integration with commercial products in HIL testbed
- **Design a resilient XFC station management system to safeguard EVs, EVCI (electric-vehicle charging infrastructure), customers and station operators**



Approach

Overall approach for CyberX

- Tasks for CyberX Project
  - Task 1.1: XFC station and control system
  - Task 1.2: Threat analysis
  - Task 1.3: Secure XFC station control methodology development
  - Task 2.1 ~ 2.2: Methodology validation
  - Task 2.3: Performance analysis
  - Task 3: Knowledge dissemination

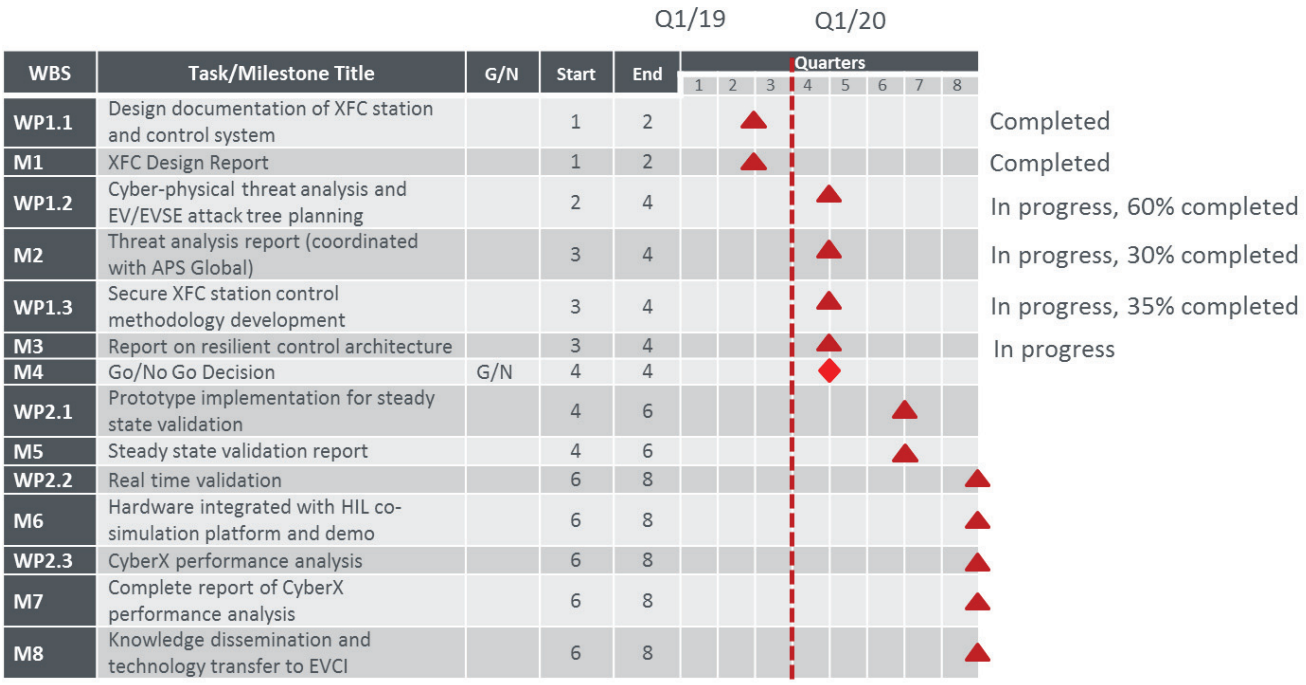


- Unique aspects
  - XFC station management system (XMS) with cybersecurity features
  - Prototype implementation using HIL testbed
- Use knowledge from previous/on-going DOE (CEDS) funded cybersecurity projects
  - Substation, microgrids, HVDC, FACTS and IEEE 1547and etc.

U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

Approach (cont.)

Planned milestones and go/no-go decisions for FY 2019 and FY 2020



WBS	Task/Milestone Title	G/N	Start	End	
WP1.1	Design documentation of XFC station and control system		1	2	Completed
M1	XFC Design Report		1	2	Completed
WP1.2	Cyber-physical threat analysis and EV/EVSE attack tree planning		2	4	In progress, 60% completed
M2	Threat analysis report (coordinated with APS Global)		3	4	In progress, 30% completed
WP1.3	Secure XFC station control methodology development		3	4	In progress, 35% completed
M3	Report on resilient control architecture		3	4	In progress
M4	Go/No Go Decision	G/N	4	4	
WP2.1	Prototype implementation for steady state validation		4	6	
M5	Steady state validation report		4	6	
WP2.2	Real time validation		6	8	
M6	Hardware integrated with HIL co-simulation platform and demo		6	8	
WP2.3	CyberX performance analysis		6	8	
M7	Complete report of CyberX performance analysis		6	8	
M8	Knowledge dissemination and technology transfer to EVCI		6	8	

Collaboration and Coordination

Expertise

– ABB: Cyber attack detection and mitigation architecture and practices, algorithm development and validation with HIL testbed

- Anomaly detection, communications and system modeling, HIL testbed and power systems

– INL: Power hardware-in-the-loop simulator for demonstration

- EV/EVSE communication, HIL testbed and power systems

– APS Global: Electric distribution system model and threat analysis

- EV/EVSE cybersecurity and threat analysis

– Thor Trucks: Electric vehicle for testing of demonstration

- EV engineer

Overall Impact

Impacts

- A cyber secure extreme fast charging (XFC) station that reduces the risk and impact of cyber intrusions
- Prototype implementation with commercial products in HIL
- Implement the solutions into existing and future products

Innovations

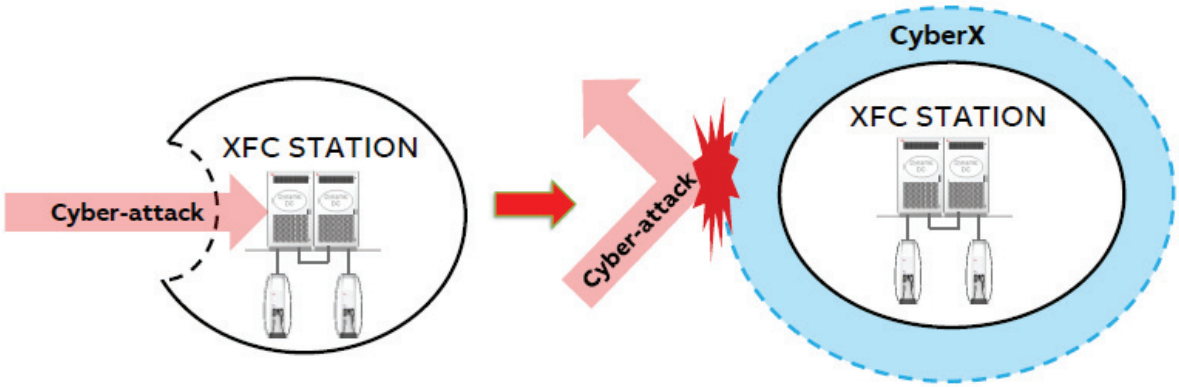
- XFC station management system with first principle based cybersecurity features
- A state-of-the-art anomaly detection system that can identify the abnormal cyber behaviors within the XFC station

Overall Impact (cont.)

- Project plans (2019 ~ 2020)
- 2019
  - System modeling
  - Threat analysis
  - Detection and mitigation algorithms
- 2020
  - Prototype implementation
  - HIL testing
  - Performance analysis
  - Dissemination

Summary

- Secure XFC (>350kW) station
- CyberX layer for detection and mitigation of cyber events
- Prototype implementation with existing technology
- Power HIL testbed focusing on potential grid impact



Project Coordination

Resources and Capabilities

Existing capabilities
In development

- What charging equipment or facility capabilities does your project have available?
  - **ABB EV charger (350 kW)**
  - XFC station management system (XMS)

- INL has installed and commissioned the ABB Terra HP Fast charger in its lab
- XFC charging models will be based on and validated against this charger

U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

Resources and Capabilities (cont.)

- What charging equipment or facility capabilities does your project have available?
  - ABB EV charger(s)
  - XFC station management system (XMS)
- What software/hardware tools will your team be using during the project?
  - MATLAB/Simulink (system modeling), Python, Scikit-learn (ADS), Docker, Javascript, C/C++ (XMS)
  - Embedded system for prototype XMS
  - Local HIL threat testbed (Opal-RT, EV emulator, grid simulator)
  - High Power HIL testbed (Opal-RT, Chroma grid simulator)
  - High fidelity XFC charging models (INL)

Existing capabilities **In development**

U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

Assessment Activities

- **What are your project cyber security assessment needs?**
  - Vulnerability assessment for XFC station including local generation (different size and number of XFCs, different type of generations and communications, emerging standards)
- **What information do you need on threat vectors, vulnerabilities, etc. to complete your project?**
  - Emerging or use case types for EVSEs
  - Communication diagram for EV charging station
- **What outcomes or information could your project provide to other teams around the year 1 timeframe?**
  - Some aspects of threat analysis for XFC station

Proposed Future Works

- **Ongoing FY-19**
  - Finish the real-time system conversion of existing model to power HIL testbed
  - Perform functional testing and use case scenarios
  - Additional testing and verification for High fidelity XFC charging models (INL)
  - Complete a threat analysis report of the grid connected XFC station
  - Develop cyber attack detection and mitigation algorithms

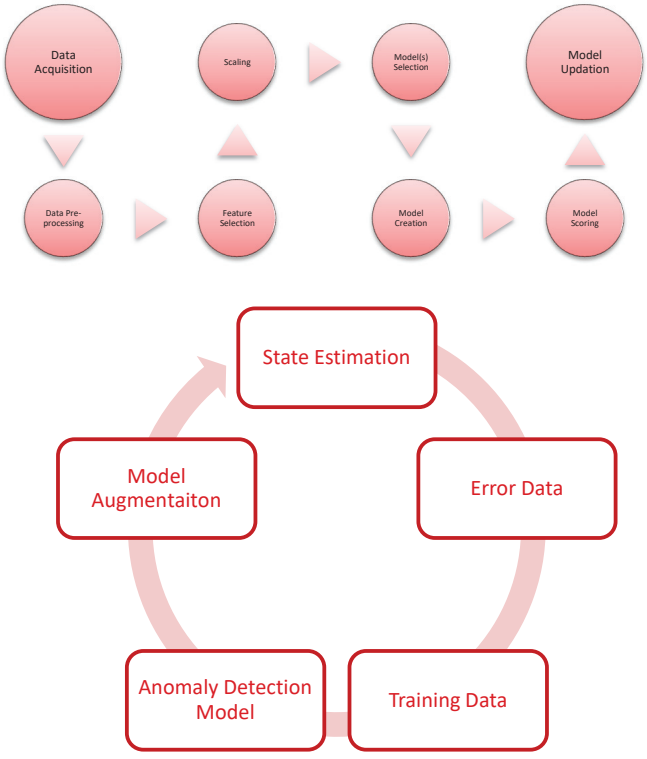
- **FY-20**
  - Prototype implementation of XMS system and control
  - Power HIL testing using EV truck
  - Performance analysis
  - Dissemination

Technical Backup Slides

Approach (cont.)

Coordinated Anomaly Detection System

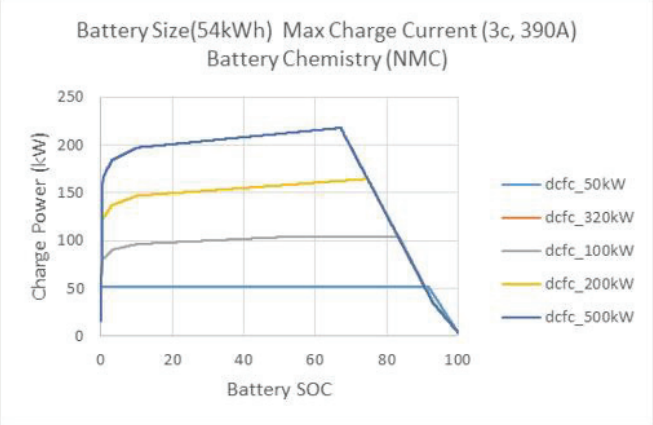
- The objective is to develop an anomaly detection system to assist the existing State estimation (primary method) to detect bad data
- Looking for anomalous patterns in the data which might suggest abnormal operation including, but not limited to, cyber attacks.
- Given the scarcity anomalies in real data, entries obtained from State Estimation can be used to train Anomaly Detection models to learn patterns
- These can be fit into various models including k-NN, One class SVM, neural networks, etc.
- Knowledge gained from First Principles forms part of a model to help identify anomalies in real-time or archival data.

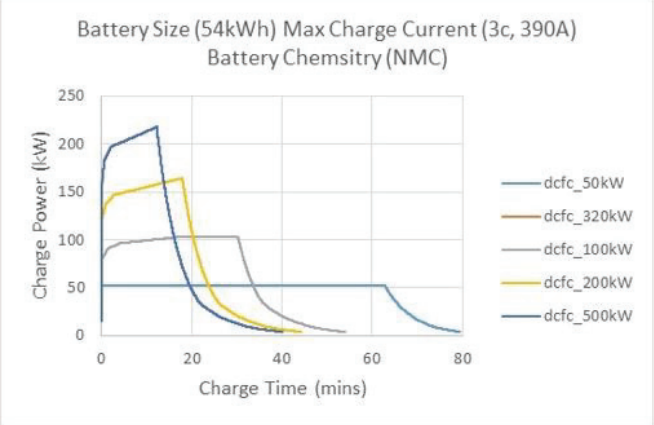


Resources and Capabilities (cont.)

High fidelity XFC charging models (INL)

- INL has done extensive battery testing for various battery chemistries
- Using test data able to generate high-fidelity charge profiles for PEVs that are not commercially available

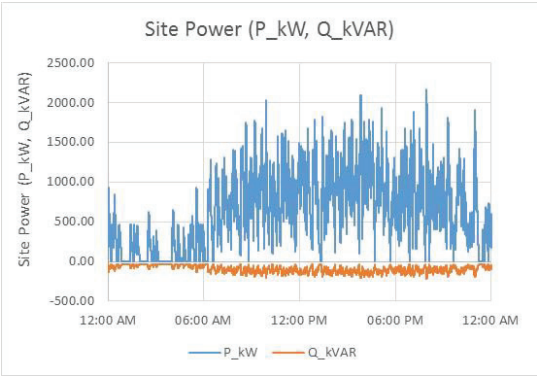




Resources and Capabilities (cont.)

High fidelity XFC charging models (INL)

- XFC site load profiles can be very volatile
- Volatile behavior may cause False Positives in anomaly detection systems
- Accurate charging models needed when designing system to avoid False Positives



- XFC site charge profile generated from charging models
- XFC site with 6 chargers
- All PEVs charged at site able to charge at 350 kW

NMFTA Medium Duty and Heavy Duty Electric Vehicle (MD/HDEV) Extreme Fast Charging (XFC) Cybersecurity Working Group

Advanced Vehicle Technology Division

September 12, 2019

NMFTA National Motor Freight Traffic Association, Inc.

U.S. Department of Transportation Volpe Center

Advancing transportation innovation for the public good

Agenda

- **DOT/Volpe Center Overview**
- **NMFTA Extreme Fast Charging Cybersecurity Project**
  - Background
  - Cybersecurity Concerns
  - XFC Cybersecurity Working Group
  - XFC Cybersecurity Requirements and Procurement Language Report

DOT/Volpe Center Overview

U.S. Department of Transportation Volpe Center

History in Brief

- The Transportation Systems Center was created in 1970, drawing on the legacy of the former NASA Electronics Research Center.
- In 1990, the Center was renamed in honor of the second Secretary of Transportation and former Governor of Massachusetts, John A. Volpe.
- The Volpe Center has proudly and professionally served 17 Secretaries of Transportation, their deputies and assistant secretaries, and over 300 modal administrators.

U.S. Department of Transportation Volpe Center

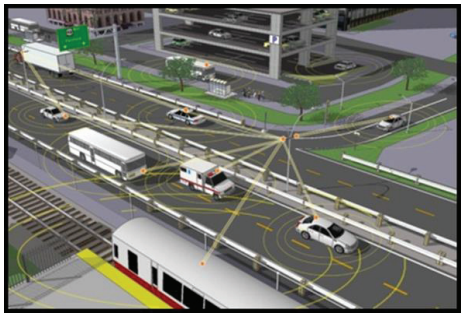
Key Features of the U.S. DOT Volpe Center

- Federal partner
- Track record of exceptional products and impact
- World-class talent and resources
- Multimodal and cross-disciplinary expertise
- Flexible, adaptable, and responsive to sponsors
- Historical perspective, institutional memory
- Entrepreneurial and efficient
- Strong, collaborative working relationships across U.S. DOT, other Federal agencies, and the broader transportation community
- Values-driven honest broker
- Cost reimbursable

Infrastructure Systems and Technology

Focus

- ❑ Transportation infrastructure evaluation and engineering
- ❑ Crash avoidance and electronic systems safety and resilience
- ❑ Cybersecurity of the transportation enterprise
- ❑ Logistics and supply chain analysis



Example projects

- ❑ Cybersecurity for government vehicles (DHS)
- ❑ Heavy vehicle cybersecurity (NMFTA, Inc.)
- ❑ Analysis of automotive cybersecurity incidents and response (NHTSA)
- ❑ Connected vehicles evaluation and safety assessment (FHWA)
- ❑ Improving grade crossing safety (FRA)
- ❑ Intelligent transportation systems policy and planning (ITS JPO)

Extreme Fast Charging (XFC) Cybersecurity Requirements Report

U.S. Department of Transportation Volpe Center

Extreme Fast Charging

- **What can you power with 1 Megawatt?**
- Run a refrigerator for 3 months
- Download 133,320 songs
- Brew 2,400 pots of coffee
- Charge 5,556 iPhones
- Power a Traffic Signal for three months
- Host 600 World Series final game parties

U.S. Department of Transportation Volpe Center

Volpe's Role in the development of the NMFTA XFC Cybersecurity Requirements Report

- Volpe was responsible for creating and hosting the NMFTA XFC cybersecurity working group and collecting the requirements derived from the working group but not writing the requirements themselves

Extreme Fast Charging Cybersecurity Concerns

- **Cybersecurity Concerns for Extreme Fast Charging**
  - Damage to chargers/vehicles through cyber attacks
  - Disruption to electrical grid via "whipsaw" cyber attacks on networked extreme fast chargers
  - Networking of multiple chargers increases cybersecurity risk and potential damage
  - Business and commerce disruptions due to Medium and Heavy Duty Electric Vehicles (MD/HDEV) becoming non-operational
  - Currently there are No world-wide cybersecurity standards for charging units

NMFTA MD/HDEV XFC Cybersecurity Working Group - Background

Background

- Department of Energy/DOT-Volpe Center
  - November 29-30, 2017 DOE held the first ever EV/EVSE cybersecurity workshop with many stakeholders in the Electric Vehicle environment
    - At the end of the workshop, it became clear that EVSEs have critical and major vulnerabilities
    - *DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report** was produced detailing the findings of the workshop

*https://rosap.ntl.bts.gov/view/dot/34991/dot_34991_DS1.pdf?download-document-submit=Download

XFC Cybersecurity Project Objectives

U.S. Department of Transportation Volpe Center

NMFTA MD/HDEVXFC Cybersecurity Working Group - Objectives

- *NMFTA/Volpe MD/HDEV and Charging Infrastructure Cyber Security Baseline Reference Document*
  - Provided a baseline reference document for understanding the issues surrounding MD/HDEV cybersecurity

- XFC Cybersecurity Working Group
  - Coordination and harmonization among stakeholders is essential
    - Reduces parallel research efforts
    - Defines clear roles and responsibilities
    - Maximizes return on investment for the greater research community
    - Bridges two critical infrastructure groups: energy and transportation

13

U.S. Department of Transportation Volpe Center

NMFTA MD/HDEVXFC Cybersecurity Working Group – Objectives (Cont'd)

Volpe's role in the Working Group:

Volpe conducted the working group meetings, collected requirements derived from the meetings and produced the output of the group in a report format

Objectives

- Cybersecurity best practices and requirements for a MD/HDEV XFC document
- Procurement language and technical cybersecurity requirements for carriers and OEMs
- Assurance language for cybersecurity requirements
- Cybersecurity requirements that are commercially feasible

14

U.S. Department of Transportation Volpe Center

NMFTA MD/HDEVXFC Cybersecurity Working Group – Objectives (Cont'd)

Objectives

- Provide the *XFC Cybersecurity Best Practices and Requirements for MD/HDEV* document to various standards organizations such as:
  - National Institute of Standards and Technology (NIST)
  - Charging Interface Initiative (CHarIN e.v.)
  - International Electrotechnical Commission Technical Committee 69-Electric Road Vehicles and Electric Industrial Trucks (Contact: Craig Rodine, ChargePoint)
- And others for adoption by the MD/HDEV sector and NMFTA stakeholders/members

NMFTA MD/HDEV XFC Cybersecurity Working Group - Members

- **XFC Cybersecurity Working Group Members**
  - **Federal Agencies** - DOE, National Institute of Standards and Technology, DOT (i.e., the Volpe Center, FMCSA, Federal Transit Administration, and the DOE National Laboratories
  - **Electric Trucking Industry Stakeholders** - Electric truck OEM/suppliers, electric truck charging vendors, utilities, network aggregators, trade associations, standards bodies and others
  - **International Govt. Agencies** - National Research Council-Canada, Office for Low Emission Vehicles-UK
  - **ISACs**: Automotive Information Sharing and Analysis Center (Auto-ISAC) and Electricity Information Sharing and Analysis Center (E-ISAC)

NMFTA MD/HDEV XFC Cybersecurity Working Group – Progress to Date

- **Cyber Security Sub-Working Groups**
  - Sub-Working Group A – Technical
    - Currently meeting on a bi-weekly basis
    - Contributes to identifying and defining MD/HDEV XFC cyber security requirements
    - Does the writing and drafting of the requirements to ensure that the proper language is used with regard to applicable industry, procurement and guidance standards
  - Sub-Working Group B – Review
    - Reviews, comments, and gathers consensus among working group members on Sub-Working Group A's Documents

XFC Cybersecurity WG Example Products

U.S. Department of Transportation Volpe Center

NMFTA MD/HDEV XFC Cybersecurity Working Group Report – Functions/Security Controls

- Design
  - Defines future-proofing, secure remote updates, secure versioning, etc.
- Cryptography
  - Defines crypto algorithms, key lengths, key management, crypto versioning
- Communications
  - Defines message/firmware confidentiality, integrity, authenticity, replay detection, etc.
- Hardening
  - Defines least functionality, device hardening, interface minimization, physical manipulation protections, etc.
- Resiliency
  - Defines message integrity verification, fail-secure operation

NMFTA MD/HDEV XFC Cybersecurity Working Group Report – Functions/Security Controls

- Secure Operation
  - Defines access controls, key management, secure data storage, pen testing, etc.
- Logging
  - Defines aspects of IDS/IPS, and the logging of cybersecurity events that occur
- Lifecycle and Governance
  - Defines vulnerability disclosure program, configuration management, security awareness, incident response plan, etc.
- Assurance
  - Defines design evidence, security testing, secure coding practices, etc.
- EVSE Operator/Utility Communications
  - Defines aspects of EVSE Operator and Utility communications authentication and integrity

U.S. Department of Transportation Volpe Center

NMFTA MD/HDEV XFC Cybersecurity Working Group Report – Section 3 Example

EVSE System Specification Section: Cryptography

Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols			
Ref #	Requirement Type	Devices	Requirements
SSCR-02	Cryptographic Random Number Generation	Local Controllers, Authentication Terminals	The Device SHALL use a dedicated cryptographic pseudo- random number generator, as defined in FIPS 186-4 [9], FIPS 140-2 (Annex C)[10] to generate random numbers used for security functions such as secret key generation and generation of nonces. The Device SHALL use the algorithms implemented exactly as they are described in reviewed literature without any modifications.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Proof of the implementation could be the reports of a standardized test procedure such as the NIST Cryptographic Algorithm Validation Program (CAVP). • NIST SP 800-22 provides a standardized test suite to look for biases found in non-cryptographic random number generator during a black-box test.			
System Threat Reference			
Spoofing	**3.2.1,.2,.3,.4**		
Tampering	**3.2.1,.2,.3,.4**		
Repudiation	**3.2.1,.2,.3,.4**		
Information Disclosure	**3.2.1,.2,.3,.4**		
Denial of Service	**3.2.1,.2,.3,.4**		
Elevation of Privilege	**3.2.1,.2,.3,.4**		

U.S. Department of Transportation Volpe Center

NMFTA MD/HDEV XFC Cybersecurity Working Group – Final Report

- Purpose of Final Report
  - Provide an industry overview of MD/HDEV XFC systems
  - Define Cyber Security best practices and requirements for a MD/HDEV XFC based on feedback and concurrence from working group efforts
  - Provide procurement language and technical requirements for Carriers and Electric Truck OEMs
  - The report was delivered to the NMFTA and is posted on the NMFTA'S GitHub site: https://github.com/nmfta-repo/nmfta-hvcs-xfc, where it can be downloaded and commented on. (If appropriate, the NMFTA will coordinate future revision efforts)
  - The NMFTA-DOT/Volpe technical support contract ended on July 1, 2019

U.S. Department of Transportation Volpe Center

Questions

Contact Information

Kevin Harnett
IT Specialist (Information Systems Security) & Program Manager
DOT, OST-R, Volpe Center
Advanced Vehicle Technology Division
kevin.harnett@dot.gov
617-699-7086

Urban Jonson
Chief Technology Officer
NMFTA, Inc.
urban.Jonson@nmfta.org
(703) 838-1828

Graham Watson
Sr. Engineer
KBRwyle/Stinger Ghaffarian Technologies
assigned to: DOT/Volpe Center
graham.watson.ctr@dot.gov
508-378-7167

Brendan Harris
IT Specialist (Information Systems Security) & Program Manager
DOT, OST-R, Volpe Center
Advanced Vehicle Technology Division
brendan.harris@dot.gov
617-494-2833

NAVFAC Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report

Advanced Vehicle Technology Division

Sept 12, 2019

U.S. Department of Transportation
Volpe Center
Advancing transportation innovation for the public good

Agenda

- **NAVFAC Transportation Alt Fuel Vehicle Initiative Overview**
- **NAVFAC EVSE Cybersecurity Best Practices and Procurement Language Report**
  - Background & Objective
  - Navy & U.S. Government EVSE Overview
  - Cybersecurity Concerns
  - EVSE Cybersecurity Requirements and Procurement Language Report

NAVFAC Transportation Alt Fuel Vehicle Initiative

- Integrates alternative fuel vehicles across the Navy non-tactical vehicle (NTV) fleet to meet federal fleet requirements:
  - Energy Independence and Security Act (EISA)
  - Energy Policy Act (EPAct)
  - Executive Order 13834
- Mission impact of increased AFV utilization are:
  - Decreased reliance on petroleum
  - Increased base resiliency
  - Increased energy security

Focused on increasing availability of Electric Vehicle Supply Equipment (EVSE) to support further NTV fleet electrification

3

U.S. Department of Transportation Volpe Center

NAVFAC EVSE Cybersecurity Best Practices and Procurement Language Report

U.S. Department of Transportation Volpe Center

Background

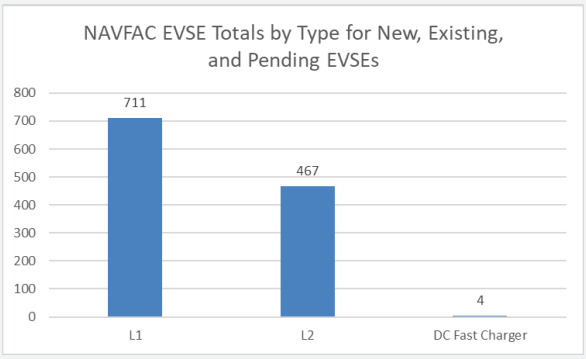
- **November 2017** - DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report
  - Identified EVSE as a major vulnerability point in the electric vehicle environment.
- Follow on studies by various entities such as the Volpe Center, National Motor Freight Transportation Administration (NMFTA), Idaho and Sandia National Labs, to name a few, have identified and documented specific vulnerabilities as well as cybersecurity recommendations.
- **Executive Order (EO) 13834**, Efficient Federal Operations, Section 1 instructs agencies to meet statutory requirements related to energy and environmental performance of vehicles in a manner that increases efficiency, optimizes performance, and reduces waste and costs
- Other Guidance:
  - Energy Independence and Security Act (EISA)
  - Energy Policy Act (EPAct)

Objectives

- **TASK**
  - **Conduct interviews** with SMEs in Navy EV and EVSE purchasing, deployment, maintenance and operations
  - **Identify threats** and vulnerabilities to Navy EVSE and create a threat model
  - **Define** cybersecurity controls/requirements based on threat model
- **DELIVERABLE**
  - Document that defines baseline EVSE cybersecurity requirements and procurement language for Level 2, DCFC, and XFC's
- **AUDIENCE**
  - Asset owners, operators, integrators, and suppliers during the EVSE procurement process and engineers for EVSE deployment /operations

NAVFAC (Navy) EVSE Overview

- 1,182 EVSE across U.S. Naval Installations:
  - 711 Level 1 Chargers
  - 467 Level 2 Chargers
  - 4 DC Fast Chargers
- Supporting 211 Electric Vehicles Across the Navy



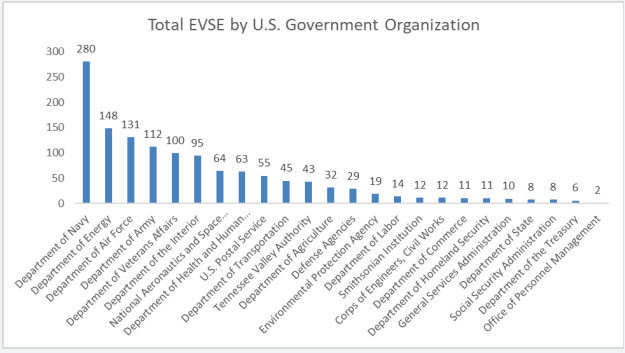
7

U.S. Department of Transportation Volpe Center

U.S. Government EVSE Overview

- 1,310 EVSE across U.S. Government
  - 1,484 Level 1 EVSE
  - 17 DC Fast Chargers

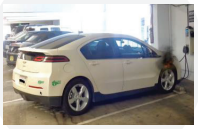
    *includes Navy EVSE
- Combined 367 Electric Vehicles across U.S. Government as of 2018
- Navy is the largest U.S. Government user of EV/EVSE



8

U.S. Department of Transportation Volpe Center

Navy EVSE Cybersecurity Concerns

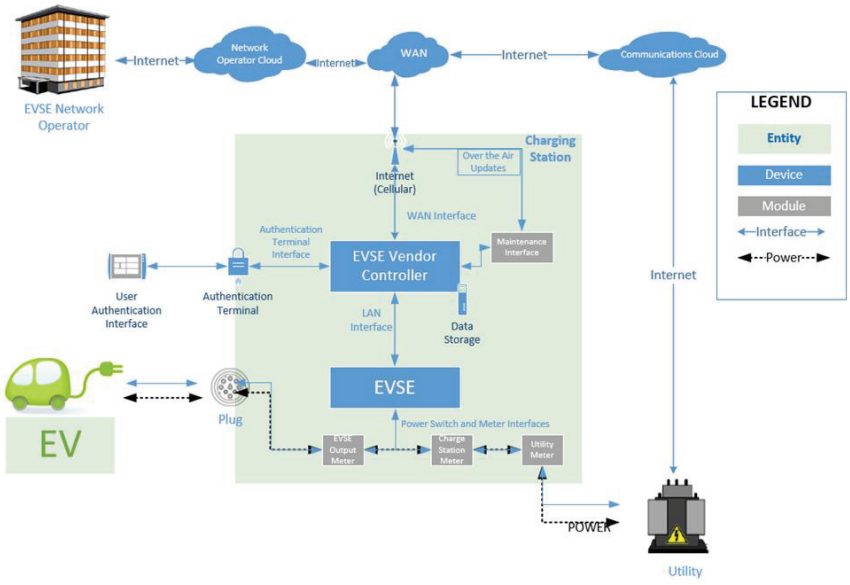


- Damage to chargers/vehicles through cyber attacks.
- Damage to critical military resources or infrastructure through EVSE cyber attacks.
- Disruption to electrical grid via cyber attacks on networked EVSE.
- Networking of multiple chargers increases cybersecurity risk and potential damage.
- Business and financial impacts as a result of compromised metering/billing components.
- Lack of/ current DoD or Federal cybersecurity standards for charging unit deployment, maintenance or acquisitions.

EVSE Cybersecurity Requirements and Procurement Language Report

- Provides detailed overview of the current Navy and U.S. Government EV and EVSE landscapes.
  - Derived from analysis of Federal Automotive Statistical Tool (FAST) program data
  - Supported by interview responses from NAVFAC EV and EVSE Subject Matter Experts
- Defines EVSE types and system components
  - Critical in understanding the EVSE Threat Analysis
- Provides notional EVSE Architecture diagram
  - Intended to be an example of how an EVSE installation may connect with other critical Navy systems

Notional EVSE Architecture Diagram



U.S. Department of Transportation Volpe Center

EVSE Cybersecurity Requirements and Procurement Language Report

Continued..

- Identifies cybersecurity considerations for U.S. Government EVSE and provides a detailed threat model.

- Defines cybersecurity requirements and best practices for use in the acquisition and installation/integration of EVSE to U.S. Government installations.

U.S. Department of Transportation Volpe Center

EVSE Cybersecurity Requirements Matrix - Example

No.	Requirement Type	Devices	Requirements	Assurances
EVSE System Specification Section: Design				
Source: ElaadNL-Chapter 2 Section 2.1 Future-Proof Design				
SSD-01	Design future-proofing	Local Controllers, Authentication Terminals	The Device SHALL have sufficient reserves in memory and computing power to allow updates to security functions that security experts anticipate are necessary during the Device's lifecycle.	• Analysis of the design documentation provided by the Vendor. • Testing the performance of the Device for algorithms and protocols anticipated for future use.

Current Status of Effort

- Report currently undergoing internal reviews
- Finalizing data and information for U.S. Government EV and EVSE projected growth.
- Final due to NAVFAC 30 Sept 2019

Questions

Contact Information

Kevin Harnett
IT Specialist (Information Systems Security) & Program Manager
DOT, OST-R, Volpe Center
Advanced Vehicle Technology Division
kevin.harnett@dot.gov
617-699-7086

Brendan Casey
Alternative Fuel Vehicle Program Manager
NAVFAC Atlantic, PW7
Brendan.Casey@navy.mil
202.685.8248

Graham Watson
Sr. Engineer
KBR
assigned to: DOT/Volpe Center
graham.watson.ctr@dot.gov
508-378-7167

Gus Brown
Lead IT Security Analyst
KBR
assigned to: DOT/Volpe Center
gus.brown@us.kbr.com
843-300-4792

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Reference Architecture for Securing XFC-Integrated Charging Infrastructure

Tobias Whitney
Technical Executive
EPRI

www.epri.com

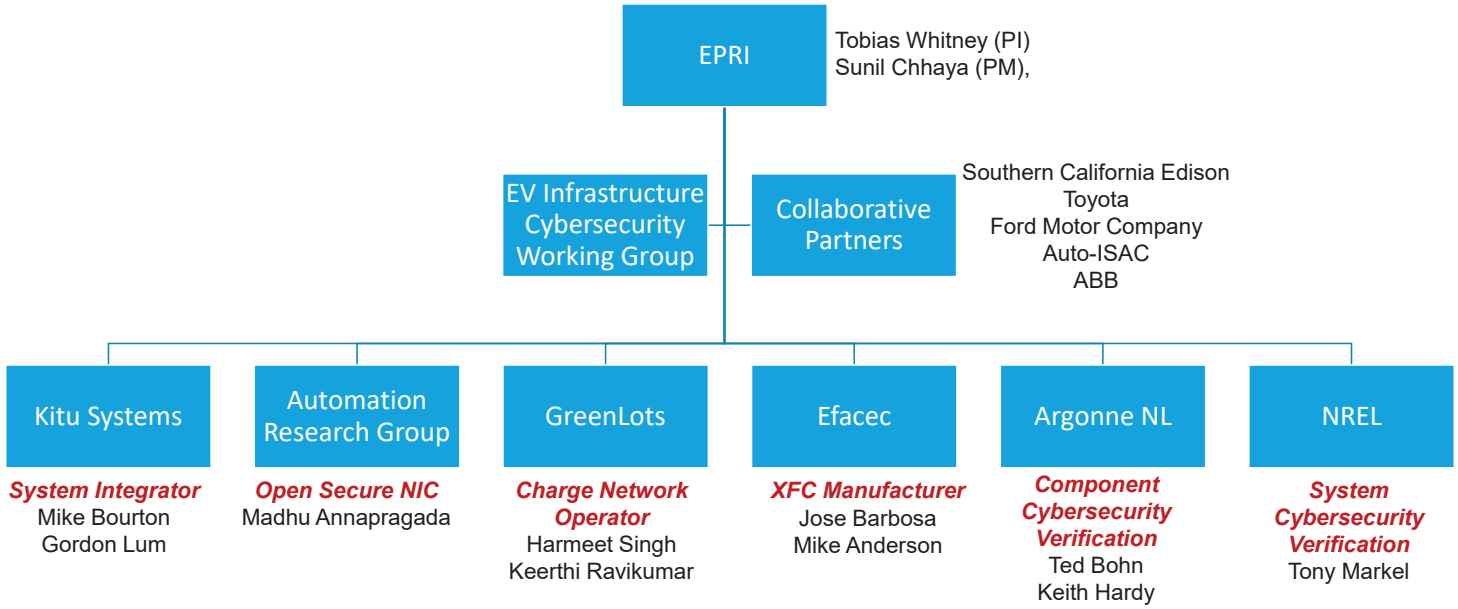
XFC Security Project Summary

- EPRI's model focuses on hardware components and connectivity between systems (leveraging Technical Assessment Methodology)
- Security Controls identified to address 4 risk categories:
  - Reliability
  - Financial
  - Safety
  - Privacy
- Key challenge: the role of the utility with regard to XFC infrastructure given high charge rates.

XFC Charging Rates in Comparison

	Level 1 (110V, 1.4 kW)	Level 2 (220V, 7.2 kW)	DC Fast Charger (480V, 50 kW)	Tesla SuperCharger (480V, 140 kW)	XFC (800+V, 400 kW)
Range Per Minute of Charge (miles)	0.082	0.42	2.92	8.17	23.3
Time to Charge for 200 Miles (minutes)	2,143	417	60	21,	7.5

EPRI Team Organizational Chart



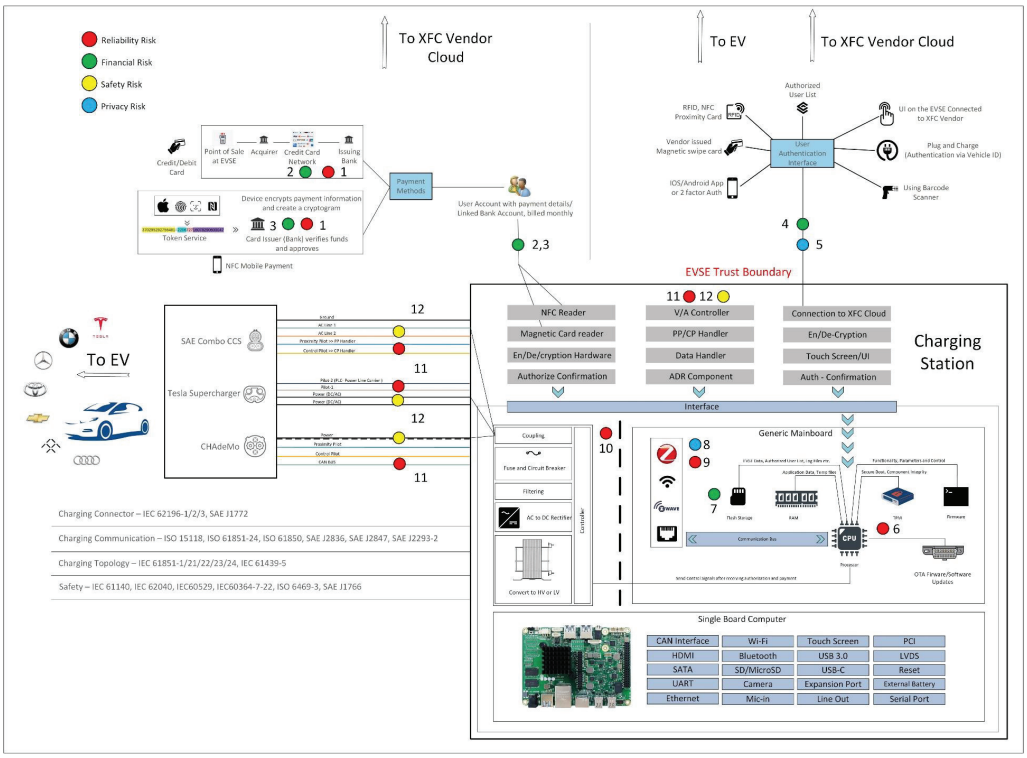
SOPO Timeline and Key Milestones – 2018-19

Milestone	Type	Description	Delivery Date
Risk Matrix Completed	Technical	Risk Matrix for Each Ecosystem Subfunction completed.	Q1 2019 → 3/29/19
Working Group Created	Technical	EV Infrastructure Cybersecurity WG created.	Q1 2019 → 3/29/19
Vulnerabilities and Threats Identified	Technical	Security vulnerabilities and threats for each subsystem identified.	Q2 2019 → 6/28/19
Secure Network Interface Card	Technical	Network interface card open source retrofit	Q2 2019 → 6/28/19
Subsystem Security Requirement Complete	Technical	Subsystem Security Requirement Complete.	Q3 2019 → 9/30/19
Draft Reference Cybersecurity Architecture Completed	Go/No Go	Draft Reference Cybersecurity Architecture Completed.	Q4 2019 → 12/20/19

SOPO Timeline and Key Milestones – 2020

Milestone	Type	Description	Delivery Date
End-to-End Security Test Plan Complete	Technical	Test plan finalized.	Q1 2020 → 3/31/20
Security Testing Complete	Technical	Testing complete with results documented.	Q2 2020 → 6/30/20
Integrated Grid Security Risk Management Tool Finalized	Technical	Tool developed and updated based on testing results.	Q3 2020 → 9/30/20
Integrated Grid Security Risk Management Tool Published	Technical	Reference architecture is market-ready for implementation through industry deployments and regulatory framework.	Q4 2020 → 12/18/20

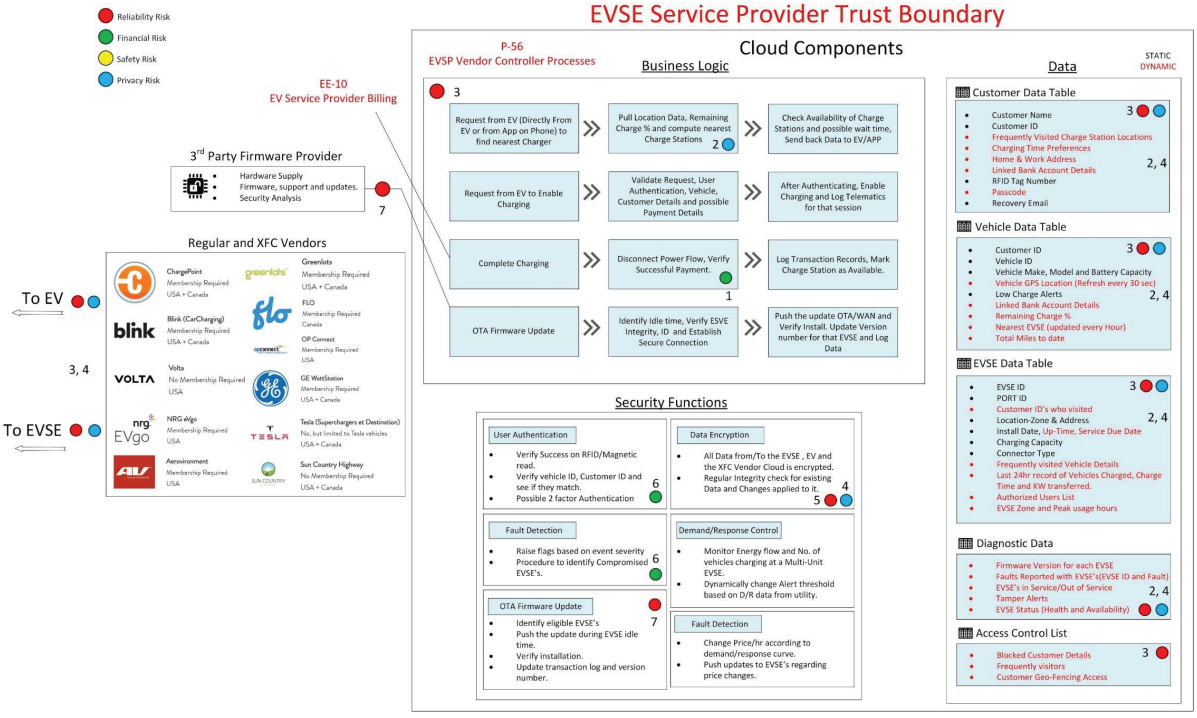
EVSE



RISK TYPE	SUB-SYSTEM	COMPONENTS INVOLVED	RISK DESCRIPTION	Consequences/Notes
Reliability Risk	EVSE	Payment interface, Magnetic Card Reader, NFC Reader.	The card reader might go through different gateways to finalize payment and authorize. These communications are subject to attacks. The locally available cell modem is a primary target.	Payment services can be unreliable if the cellular modem is tampered/jammed.
Financial Risk	EVSE	Payment interface, Magnetic Card Reader.	Theft of payment information using a skimmer or getting into the communications to authorize payment elsewhere.	This can allow attacker to get payment details, charge a vehicle elsewhere at a similar EVSE.
Financial Risk	EVSE	Payment interface, NFC Reader.	Theft of payment information using a skimmer or getting into the communications to authorize payment elsewhere.	This can allow attacker to get payment details, charge a vehicle elsewhere at a similar EVSE.
Privacy Risk	EVSE	Authentication Interface, EV, RFID, NFC, Mobile App, UI and Barcode Scanner.	Compromise in any of these methods can reveal sensitive authentication details of the EV & User.	Once the authentication details are procured, attacker can impersonate the user, get into his account and know variety of PII including frequent locations etc.
Financial Risk	EVSE	Authentication Interface, EV, RFID, NFC, Mobile App, UI and Barcode Scanner.	Access into authentication interface by one of the means will give the attacker payment information/account details.	This could be a basic payment details theft. Likely to happen if the EVSE is located in a remote place.
Reliability Risk	EVSE	Authentication Interface, EV, RFID, NFC, Mobile App, UI and Barcode Scanner.	All the mentioned methods are subject to spoofing, replay attacks and jamming. Unavailability of authentication would cause service disruption.	An EVSE could be temporarily out of service/unusable.
Financial Risk	EVSE	Main board, Flash Storage	Any on-board storage is going to contain EVSE data, Firmware Data, User Data. Attacker can modify as per his/her need	This could mean the attacker adding himself to the authorized list, or getting crucial details about how the EVSE functions.
Privacy Risk	EVSE	EVSE, Communication Mainboard/Module	All the methods of communication (Wi-Fi, ZigBee, RF, Z-wave, BT or Ethernet) are subject to attacks. Risk of theft of Data in Motion exists. (MIM)	Attacker can target selected interfaces which EVSE is using to talk to master/EV's.
Reliability Risk	EVSE	EVSE, Communication Mainboard/Module	Jamming/Disabling the communication adapter by creating severe interference/noise will pose a reliability risk for the EVSE or the Master itself in a fleet environment.	This would put the EVSE or the fleet out of service momentarily or until the jamming/disabling is in effect.
Reliability Risk	EVSE	Charge Controller	Modifications to the EVSE hardware, specially power electronics can question the reliability of the EVSE provider. (Ex: substituting with a high A rated fuse)	This will bring in undesired behavior of EVSE and can also pose a Safety Risk.
Reliability Risk	EVSE	Pilot Interface, CAN, PLC	The Pilot interface controls the current and voltage. Modification of the charging plug can disable/change behavior of data flowing on Pilot pins.	Now bad data on Pilot pins would mean wrong current levels and possibly start/stop charging at will.
Safety Risk	EVSE	Pilot Interface, CAN, PLC	The Pilot interface controls the current and voltage. Modification of the charging plug can disable/change behavior of data flowing on Pilot pins.	This can possibly damage the charge controllers on either side.

Sub System	Components	Assets	Vulnerability
EVSE	Payment Interface – Magnetic Card Reader/NFC Reader	Payment process, Trust and the hardware modules for processing payment	The payment processing hardware is stacked on the EVSE and is routed through a separate connection to the payment gateway or goes directly through EVSE's network. The key vulnerabilities here are the cellular modem and hops made by the payment information to get the authorize confirmation back to EVSE.
EVSE	Payment Interface – Magnetic Card Reader	Payment details, Payment process, Magnetic Card Reader	A magnetic stripe with encoded data is swiped on the reader, transferring all the bits during the swipe. The reader is vulnerable to modifications such as adding a skimmer on top of the read head.
EVSE	Payment Interface – NFC Card Reader	Payment details, Payment process, NFC Card Reader	Being wireless, NFC is more vulnerable to spoofing and data modifications. Just like magnetic readers, NFC readers can be modified or added with an extra layer which eavesdrops the payment information before it reaches the reader.
EVSE	EV Charging controller, EVSE, wired comms. and RF/Wi-Fi	Authentication Interface – Barcode, UI Login, RFID tag.	The RFID tag is subject to duplication; the UI-login is subject to phishing attacks where the user is tricked with a similar UI but setup by the attacker purely to capture credentials. Some insight from different EVSE manufacturers showed the usage of SBC's (Single Board Computer) running Windows-10 to run their UI and custom software. This brings in lot of vulnerabilities within the operating system and the hardware it is running on.
EVSE	Authentication Interface – Barcode, UI Login, RFID tag.	Financial details, PII, User accounts.	Referring to #4, there are vulnerabilities associated with the authentication methods like QRcode, Login, RFID tag etc. Each of these methods can be attacked by phishing, spoofing or sniffing the data/credentials while in-transit. These vulnerabilities not only attract threats which will affect the reliability of the system but can pose severe financial loss depending on how the systems store/process payment information.
EVSE	Mainboard, On-board Flash Storage, attached/connected local storage.	EVSE, Access List, Sensitive Files	If the XFC EVSE is available in a remote location with little or no surveillance, it is easy for the attacker to have an inside look by damaging the cabin or forced entry. If it is a fleet environment, entire fleet along with site-controller is open to the attacker to examine, trace, capture and analyze the information.
EVSE	Wireless/Wired communications – adapters (Wi-Fi, Bluetooth, Z-wave etc.)	PII/User data – data in motion/at rest.	Any wireless communication between the charging stations, Site controller and the cellular modem are vulnerable to attacks like spoofing, replay, jamming, DOS etc. These wireless links could be end to end encrypted but that cannot prevent a jamming attack.
EVSE	Mainboard, Wireless/Wired communications – adapters (Wi-Fi, Bluetooth, Z-wave etc.)	Communications, Data transfers, EVSE Operations	Similar to #7. In a fleet situation, the individual EVSE's are connected to a local Site Controller. There are dependencies the EVSE has with the controller like setting the price, operational parameters, load balancing and emergency shutoff.
EVSE	Charge Controller	Communications, Charging Profile, V/A adjustments	The charge parameters are communicated in a series of messages between EV and EVSE which happen over the pilot pins/CAN/PLC depending on type of connector. RF signals can be manipulated with equipment like an oscilloscope, generator and amplifier. The PLC operating at 2-30MHz makes it possible for the signal to interfere with nearby EVSE's.
EVSE	Charge Controller, Pilot Pins and signals.	Charging Profile, V/A adjustments, Power requirements.	The pilot pins are available physically conducting at the end of connector while they are active with power and signal during a charge session. It is possible to modify an unlocked charging connector. This vulnerability exists for EVSE's whose charging connector is unlocked and available all times irrespective of an active charge session.

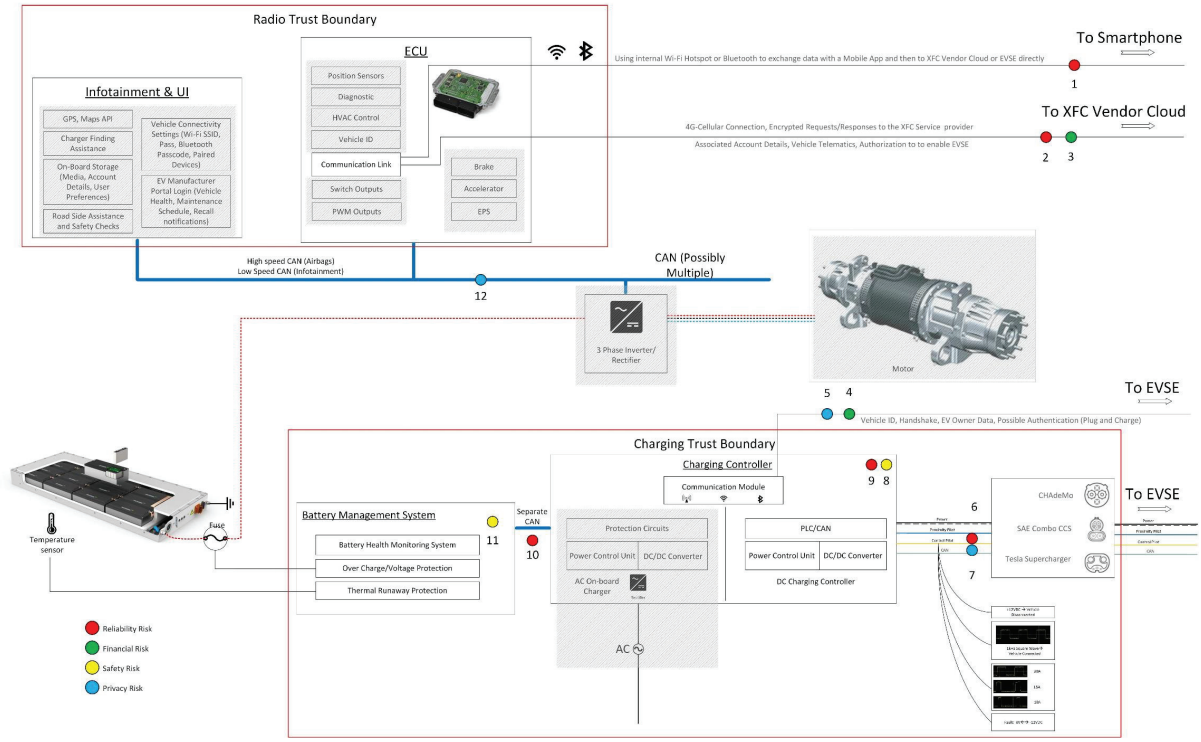
XFC Vendor/EVSE Cloud



RISK TYPE	SUB-SYSTEM	COMPONENTS INVOLVED	RISK DESCRIPTION	Consequences/Notes
1. Financial Risk	XFC/EVSE Vendor Cloud	Business Logic verifying payment authorization	Gaining root access to the cloud can expose payment details of all consumers who have Auto-Pay setup.	Financial loss due to stolen payment details.
1. Privacy Risk	XFC/EVSE Vendor Cloud	Vehicle Data Table, Customer Data Table	Compromise in security can reveal dynamic location of 100's of EV's	Attacker can track EV's with whatever precision the cloud application gets to know.
1. Reliability Risk	XFC/EVSE Vendor Cloud	EVSE and XFC Vendor Cloud	Modifying/interrupting data between EVSE and cloud to mark a particular EVSE as unavailable or corrupting Data on EVSE Cloud or adding bogus data.	This can trick EV's and the cloud such that all EVSE's appear to be occupied and unavailable; resulting in chaos and loss of business until attack in effect.
1. Privacy Risk	XFC/EVSE Vendor Cloud	Data Blob/Tables/Clusters or any format data is stored.	Once access is achieved, all the dynamic data is now available to spy on thousands of users resulting in massive breach of data and privacy.	Attacker can get all the PII of Users and vehicles like location, address, miles remaining, possible time when user will arrive at the EVSE and other vehicle telematics.
1. Reliability Risk	XFC/EVSE Vendor Cloud	Security Functions	Post unauthorized access to cloud, the security functions are subject to modifications or disabling as per attackers need.	One way is to disable encryption or get the keys so that attacker can later steal all the data without being noticed.
1. Financial Risk	XFC/EVSE Vendor Cloud	Security Functions	Tampering with the security functions creates a huge financial risk, allowing many users to exploit the changes made to the cloud application.	Possibility of getting free charging, theft of payment details, bank account details etc.
1. Reliability Risk	XFC/EVSE Vendor Cloud	OTA/Wired Firmware Update. In-House firmware or outsourced to 3rd party vendor.	The more steps a firmware will take to reach to the final device, the more chances of it being tampered/modified.	Modified firmware can effect entire behavior of the system until fixed.

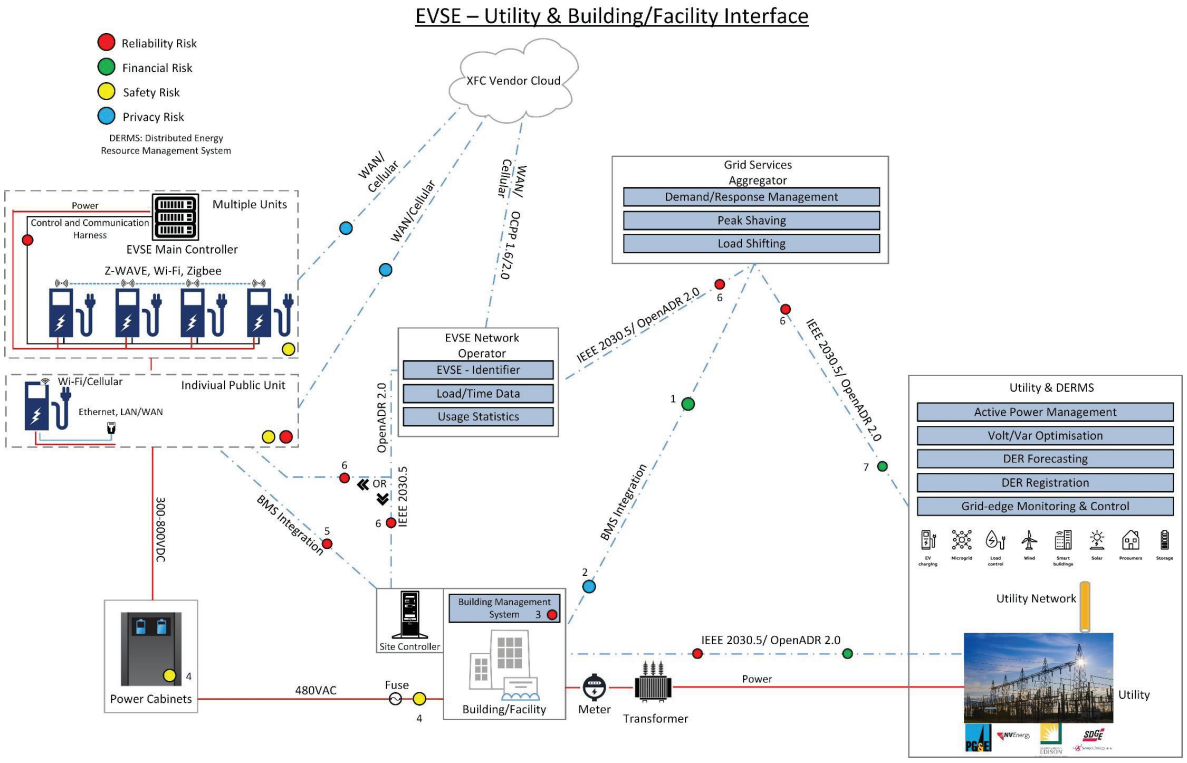
Sub System	Components	Assets	Vulnerability
XFC Vendor Cloud/Service Provider	Business logic and payment authorization	Financial details, Payment information	XFC charging service provider hosts data from various charge stations on a cloud. The user details table consists of payment information of the users who might have enabled auto-pay. This data is vulnerable and can be exposed to the attacker/on the network if not secured well.
XFC Vendor Cloud/Service Provider	EV data, Customer data	User PII, Vehicle PII and Preferences.	As discussed in #1, same set of vulnerabilities exist for assets like user PII, vehicle PII and other sensitive information.
XFC Vendor Cloud/Service Provider	EVSE data	Charge Station details, inventory list, Identifiable information	Referring to data table in the risk assessment section which contains all the details relevant to EVSE like the EVSE location, ID number, Maintenance Date, firmware version, Active Status, Up-Time, Down-Time etc. Getting access to this data is possible by exploiting vulnerabilities/backdoors in the EVSE service provider application or monitoring the network.
XFC Vendor Cloud/Service Provider	Security functions	data and parameters controlling security functions	The functions listed in the architecture diagram are Data Encryption, User Authentication, Fault Detection, Demand/Response Control, Firmware Updates and a function to handle pricing data. These functions are critical and ensure smooth operation. Weak implementation of these, and inadequate access control can allow an attacker to misuse or disable these.
XFC Vendor Cloud/Service Provider	Firmware update, OTA communications/Updates	Firmware, updating medium, involved machines.	The firmware delivery process itself can consist of attack surfaces and weak points where the firmware is subject to modification or getting corrupted.

Electric Vehicle



RISK TYPE	SUB-SYSTEM	COMPONENTS INVOLVED	RISK DESCRIPTION	Consequences/Notes
Reliability Risk	EV	Communication between Smartphone and EV. Wi-Fi	Data/Control Flowing between the Mobile application and EV is through cellular/Wi-Fi or Bluetooth which can be intercepted.	This can bring in reliability issues for the user and his interaction with the EV.
Reliability Risk	EV	Communication between EV and XFC Vendor Cloud	Possible modification of data/request being sent to XFC Vendor Cloud to trigger/stop charging when not desired.	Attack on this pathway can allow the attacker to control/see what is being sent to the cloud.
Financial Risk	EV	EV, smartphone and XFC Vendor Cloud, 4g-Cellular communication	Account credentials, Vehicle Telematics and payment information are vulnerable to theft during exchange between cloud, EV and smartphone.	Payment details/Account Details breach can pose heavy financial risk to the users and cloud service providers.
Financial Risk	EV	EV Charging Controller, EVSE, Wired comm., RF/Wi-Fi	Data theft when EV is directly communicating with the EVSE to handshake, authenticate, authorize. This could be over the wire (Connector) or Wireless.	The bad actor can get lot of details, probably impersonate/replicate the actual vehicle's presence to get free charge.
Privacy Risk	EV	EV Charging Controller, EVSE, Wired comm., RF/Wi-Fi	If the EVSE and EV talk on Wi-Fi or RF, there is a risk of anyone intercepting/capturing packets and spy on sensitive information	Lot of PII regarding the user/EV can be captured.
Reliability Risk	EV	EV and EVSE charging connector plug	Modification of the connector plug or replacing with a 3rd party plug can cause reliability issues.	Possibly irregular current flowing through the harness, power directed elsewhere.
Privacy Risk	EV	EV and EVSE charging connector plug	Risk of identifying charging patterns, vehicle data, protocols etc. by modifying the charging connector/adding a spy chip/hardware to it.	Tiny wireless chips when planted can provide valuable insights to the attacker.
Safety Risk	EV	Charging Controller	Risk of firmware/Hardware modification. Protection envelopes being disabled, wrong charge parameters being communicated etc.	This can pose a safety risk because now the vehicles charge controller is being tricked. Over charge, discharge, missing alerts etc.
Reliability Risk	EV	Charging Controller, Communication Module	Modified firmware of charging controller can refuse to charge a battery, over charge or discharge at the attacker's will.	Possible DOS, the user will be uncertain about the charging behavior of the EV; unless firmware is fixed
Reliability Risk	EV	CAN Bus for Charging Controller, Communications	Manipulation of vehicle's CAN bus specific to charge controller can hand complete control of charge system to attacker	This would be dangerous since vehicles integrity is still intact, yet the bad packets on CAN pretend to be authentic.
Safety Risk	EV	Battery Management System, CAN connected to it and Charging Controller.	Gaining access on the CAN bus specific to Charging and BMS can potentially disable safety systems in place for the battery packs.	Possible thermal runaway, undesired behavior of the EV anywhere within the charging cycle/process.
Privacy Risk	EV	CAN, OBD-II and PLC	Setting up a clone EVSE can allow Sensitive Data going out of these ports to be captured.	Sensitive data related to vehicle is captured by malicious EVSE.

Sub System	Components	Assets	Vulnerability
Electric Vehicle	Smartphone, Android/IOS application, Bluetooth, Wi-Fi Hotspot, Smartphone Memory (internal/External)	Customer PII, Payment Information and user credentials	Weakly designed smartphone application, un-encrypted communication with vehicle, Vuln. Associated with Bluetooth version.
Electric Vehicle	Vehicle cell modem, XFC vendor cloud, vehicle telematics	Vehicle PII, Service provider functions	The communications between vehicle cell modem and the XFC/Charging service provider carry vehicle telematics and other vehicle PII depending on the operation. Security on this link determines the scope of vulnerability here.
Electric Vehicle	EV, Smartphone application, vehicle Infotainment	User contacts, PII, Payment information and user creds.	A compromised smartphone application can be used as a portal into vehicle's infotainment. Both #1 and #2 are applicable
Electric Vehicle	EV Charging controller, EVSE, wired comms. and RF/Wi-Fi	Identity of vehicle/user, payment details	The sequence of handshakes and data between the EVSE and the EV during a charge session is vulnerable to attacks. In certain cases, the vehicle ID is transmitted wirelessly or through the charging connector along with the charging profile to the EVSE.
Electric Vehicle	EV Charging Controller, EVSE, Wired Communication, RF/Wi-Fi.	User and EV privacy, EV-Charging profile	Data exchanges made at the charging station from the EV to EVSE and the user providing input to the EVSE using HMI/Interface are sensitive and vulnerable.
Electric Vehicle	EV Charging connector-female, EVSE	EV side controller, Charging connector and the charging service	In remote locations the charge stations are often unmonitored. The EV charging connector is vulnerable to modifications both physically and electronically.
Electric Vehicle	EV Charging connector-female, EVSE	Handshake details, charging protocol, detailed signal data	Similar to #6, the connector on the EV or the EVSE is subject to modification for data sniffing and pattern identification.
Electric Vehicle	EV Charging controller, Firmware	Charging service, EV controller, EV charging functionality	The charging controller inside of EV contains components and firmware which orchestrate the charging process when connected to an EVSE. This firmware is vulnerable to many things like modification, remote control, disabled functions etc.
Electric Vehicle	CAN bus/OBD Port, EV Charging Controller and communications	Charging service, EV controller, EV charging functionality	Majority of vehicles/EV's use CAN as their control bus which loops through all the components of vehicle that talk to or get controlled by. It is vulnerable and can be hacked/controlled once attacker has access to it.



RISK TYPE	SUB-SYSTEM	COMPONENTS INVOLVED	RISK DESCRIPTION	Consequences/Notes
1. Financial Risk	Grid Services Aggregator and Building Management System	APIs for BMS and the Grid Services Aggregator	Modification/Attacks on data in motion can set power consumption levels differently, causing high usage during peak hours.	Compromised communications between BMS and aggregator can lead to several issues on how the EVSEs are controlled during peak demand period.
2. Privacy Risk	Grid Services Aggregator and Building Management System	APIs for BMS and the Grid Services Aggregator	Possible risk of private data being exposed if the aggregator-BMS communications are intercepted. BMS could contain lot of PII.	The BMS can consist of RFID details of all users entering the building and access codes to secure rooms. This data can be compromised if the mentioned comm. Is attacked.
3. Reliability Risk	EVSE and Building Management System, EVSE Network Operator (Direct Connection)	EVSE, BMS and EVSE-network Operator	An insider or anyone with access to BMS can pose a risk of changing the behavior of BMS and EVSE integration.	This can lead to an EVSE not being billed for the power used or use too much power when not needed.
4. Safety Risk	EVSE & Building Interface	Power Cabinets and BMS	XFC based EVSEs may contain high power cabinets. Any access to components in between poses a safety risk.	Shutting off a single power-cabinet can affect multiple EVSEs in a fleet situation.
5. Reliability Risk	Building and EVSE Integration	BMS	Communication between BMS and EVSE are needed to implement DR commands. This communication link can be attacked and cause reliability issues.	Even accidental changes to BMS can cause reliability issues for the EVSEs/Fleet based EVSE.
6. Reliability Risk	EVSE – Utility &Building Interface	EVSE, DERMS, Grid Services Aggregator, EVSE Network Operator	Communication between the mentioned components happens over OpenADR/IEEE2030.5. Security of these interlinks is dependent on how they are implemented.	Attacks/Compromise of these protocols can lead to improper load shifting, EVSE network not responding during Peak demand session etc.
7. Financial Risk	Grid Services Aggregator, Utility and DERMS	Grid Services Aggregator, Utility and DERMS	Communication between Grid Services Aggregator and Utility-DERMS includes pricing data, D/R levels, Locations and Zip codes for D/R etc. The integrity of this data is crucial and any attacks on this interlink can pose a Financial Risk.	Modified pricing or D/R data can lead to a cascading effect and change how much the user pays at the end. Also wrong D/R data can cause grid instability.

Sub System	Components	Assets	Vulnerability
EVSE-Utility/Grid Services Aggregator/DERMS	APIs for BMS and the Grid Services Aggregator	Power, EVSE and BMS Data	The EVSEs are connected to the Building Management System (BMS) and the BMS is integrated with Grid Services Aggregator (GSA). BMS is an application provided by the vendor who also provides controllers for HVAC & Lighting for the building. Access to the BMS application provides control over the building as well as EVSE, assuming the EVSEs are integrated with BMS. The D/R commands are sent by the GSA to the BMS which requests the EVSEs to reduce the power output. The communication link between GSA and the BMS is vulnerable to attacks depending on implementation and security. In other case where the GSA is sending D/R commands to the EVSE via the EVSE Network Operator the OpenADR link is vulnerable to attacks. OpenADR has requirements regarding certificates and encryption techniques and an entity like GSA can communicate to Utility/DERMS on OpenADR only if it meets all the requirements.
EVSE-Utility/Grid Services Aggregator/DERMS	APIs for BMS and the Grid Services Aggregator	Building and its users PII	
EVSE-Utility/Grid Services Aggregator/DERMS	BMS	EVSE Reliability, EVSE Up-time	Referring to #1, the BMS is an application to provide a visual representation of the building state and its controls. The machine hosting BMS application is usually windows/Linux that is connected to BMS server on the building network. The machine itself is a point of entry into the BMS and the EVSE controls.
EVSE-Utility/Grid Services Aggregator/DERMS	Power Cabinets and emergency disconnect	EVSE	The power cabinets are connected to the Site-Controller to facilitate operations like shutdown, detect any faults in the cabinets, temperature etc. This connection could be over Modbus or any proprietary protocol and makes the power cabinets vulnerable to attacks.
EVSE-Utility/Grid Services Aggregator/DERMS	EVSE, Site Controller and the BMS	EVSE reliability and communications between EVSE and Site Controller.	Refer #1 & #2
EVSE-Utility/Grid Services Aggregator/DERMS	Grid Services Aggregator, DERMS & Utility, EVSE Network Operator	Pricing Information, D/R Data, Location/Zip Data and Customer IDs	The communication between Grid Services Aggregator (GSA) and the utility/DERMS happens over OpenADR2.0/IEEE2030.5. Part of DERMS & Utility conducts analysis and send out D/R commands to GSA. These D/R commands include information like pricing data per kilowatt, how much D/R is needed in terms of power, Location/Zipcode of zones where the D/R command will effect and possibly customer ID. This information is subject to attacks/modifications.

Key Findings…so far. We still have work to do.

- Authenticating Charging Stations: Implementing a PKI-based solution given the diversity of system and network owners
- Physical Security: Tamper alarm monitoring and accessing physical access logs
- Extreme Fast Charging Station Visibility: Require XFC have two-way communication for greater visibility
- Network Architecture: Using gateway devices and network access controls to minimize exposure from lower trust charging stations
- Commissioning of XFC: Utility company coordination in to provision XFC and integration into DR and Direct Load Control programs.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Thank You!

Coordination meeting to provide knowledge share and resource collaboration between XFC-Security Projects

July 11, 2019
Hosted by: EPRI