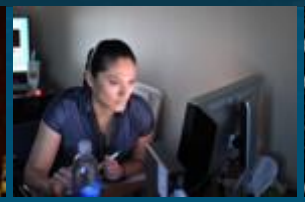
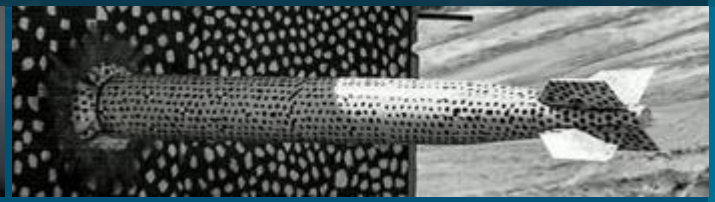
Securing Vehicle Charging Infrastructure





2021 DOE Vehicle Technologies Office Annual Merit Review

June 23, 2021

Ben Anderson, Sandia National Laboratories

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

Project ID: ELT198

SAND2021-5745 PE

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

Overview

$3M Project (Oct 2018–Sept 2021) (90% complete)

- Team: Sandia, PNNL, ANL
- Partners: DOT Volpe Center, NMFTA, 4 DCFC Vendors, 1 Utility, EPRI, NREL, Oxford, SAE PKI Working Group

Project Objective: Quantify cybersecurity risks to electric vehicle supply equipment (EVSE) and establish actionable recommendations to protect charging infrastructure so automotive, charging, and utility stakeholders can better protect customers, vehicles, and power systems in the face of new threats.

Technical Barriers/Gaps:

- Poorly implemented EVSE cybersecurity is a major barrier to electric vehicle (EV) adoption
- No comprehensive cybersecurity approach and limited best practices have been adopted by the EV industry
- Incomplete industry understanding of the attack surface, interconnected assets, and unsecured interfaces

Relevance

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

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

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

- Conducting adversary-based assessments of charging equipment
- Creating a threat model and attack graphs of EV charging
- Analyzing power system impact for different attack scenarios
- Providing a risk-based recommendations and hardening suggestions to the EVSE industry

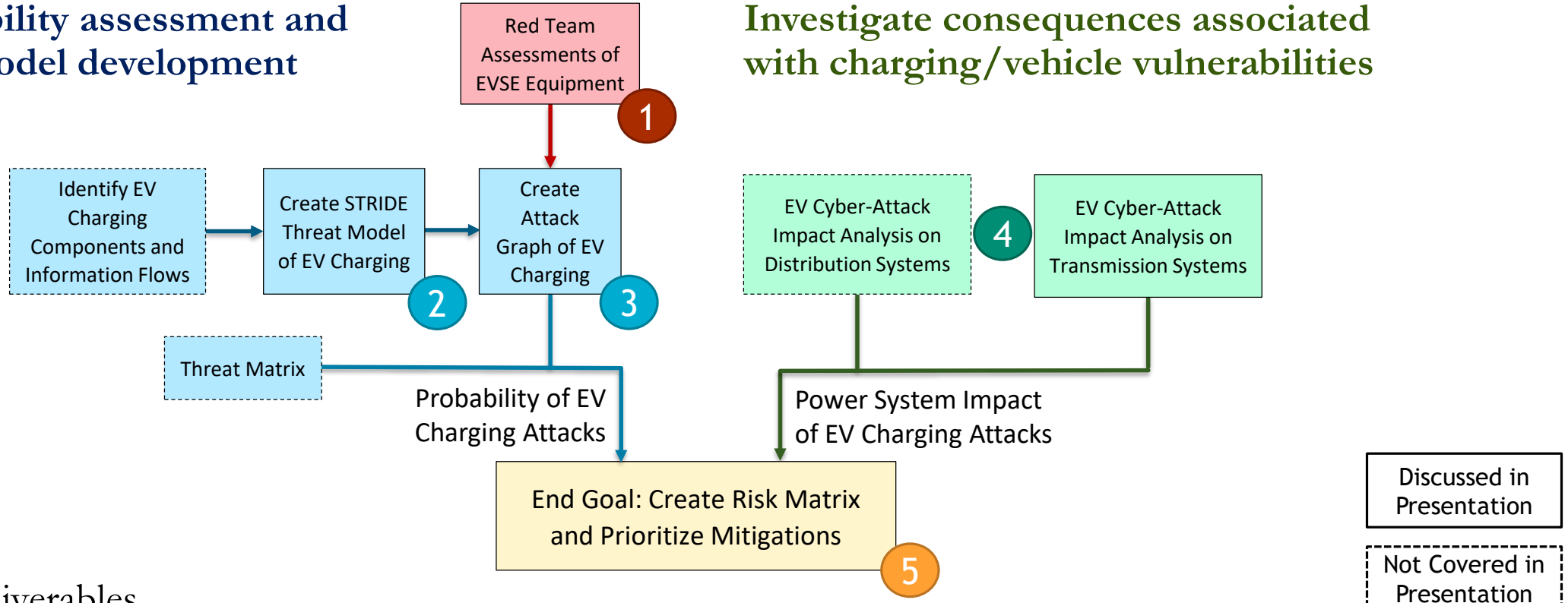
Goals and Milestones

- Publish attack graphs and present initial hardening recommendations
  - Presented at 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, Jan. 2020
  - Additional publication expected in 2021 – venue TBD
- Complete draft threat model for vehicles/charging infrastructure with prioritized vulnerabilities and enumerated communication entities/interfaces (FY21)
- Complete consequence study mapping EV/charging potential vulnerabilities to power system and other critical infrastructure impact (FY21)
- Draft hardening guide for EVSE vendors and networked associates
  - Generated EVSE Recommended Cybersecurity Practices Infographic
  - Shared with government and industry partners Oct 2020
- Complete PKI recommendations to standards development organizations
  - Worked with SAE PKI initiative to develop new standard for use of PKI in the EVSE ecosystem
  - Deployment of test system implementing the new standard planned for Q3 2021

Approach

Vulnerability assessment and threat model development

Investigate consequences associated with charging/vehicle vulnerabilities



Project Deliverables

1. Anonymized **red team results** with brownfield EVSE hardening guide, recommendations, and best practices
2. Report on the **threat model** with stakeholder entities, potential vulnerabilities, and risks to EV/EVSE infrastructure
3. Published **attack graph** indicating how different attack vectors could be exploited to enact impacts to critical infrastructure
4. Conference paper which quantifies cyber consequences associated with vehicle/charging vulnerabilities on the power system
5. Final report of EVSE **cyber risks assessment**, suggested **mitigations**, and approaches for EV charging **cyber-resilience**

PNNL Threat Model of EV Charging – Grid Impacts

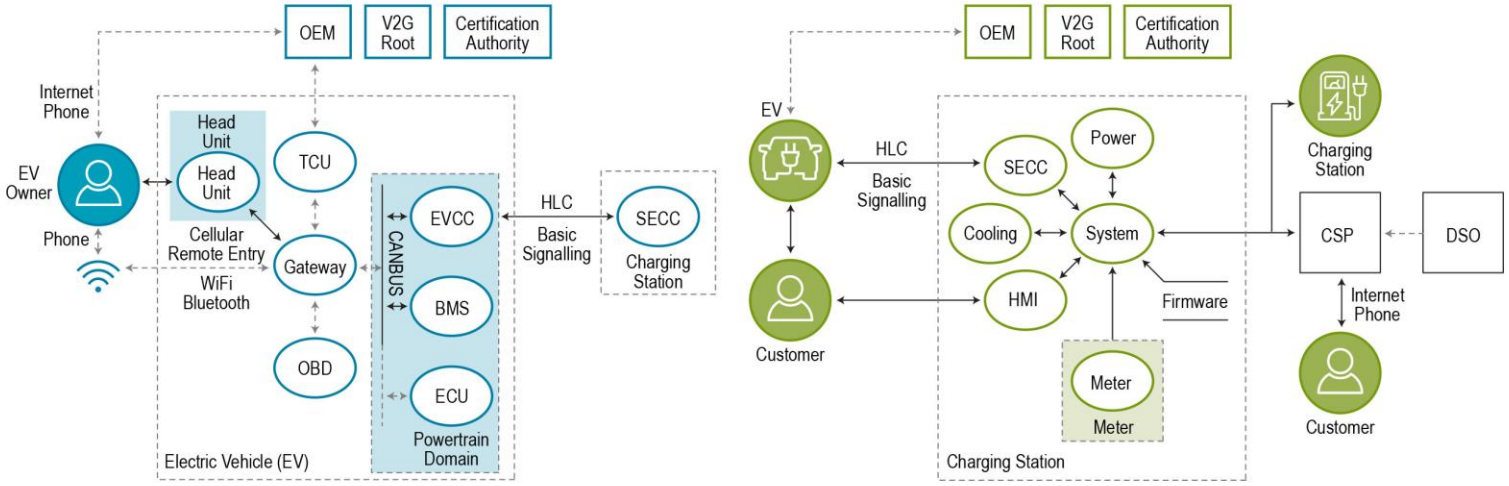


Figure 1: The vehicle system model (left) depicts the components of the vehicle and their relationship to the charger. The charger system model (right) illustrates component electric power and information relationships.

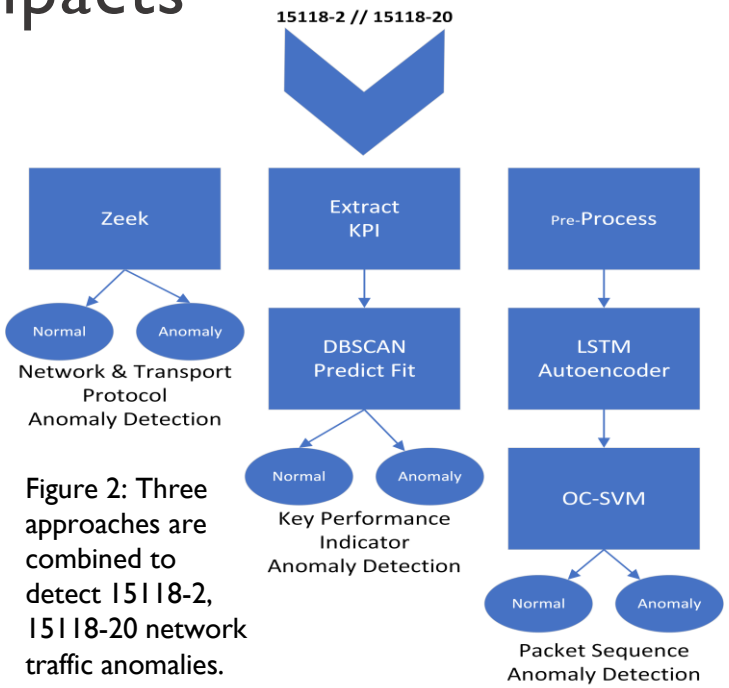


Figure 2: Three approaches are combined to detect 15118-2, 15118-20 network traffic anomalies.

Performed first of its kind EV Charging Infrastructure Threat Analysis (Figure 1):

1. Identify consequences to energy and transportation sectors
2. Define XFC security objectives: privacy, power system, transportation system, financial transactions, etc.
3. Model systems, identifying information and electric power flows
4. Examine flows for vulnerabilities
5. Identify controls and mitigations to address threats

Investigated cryptosystems and Public Key Infrastructure (PKI) as employed in ISO/IEC 15118-2//15118-20 ecosystems.

Findings:

- Consequences helped identify power/transportation threats.
- Energy sector cannot mitigate XFC alone; ecosystem parties need strong coordinated cyber practices.

Deliverable:

- Threat consequence report published 9/2020

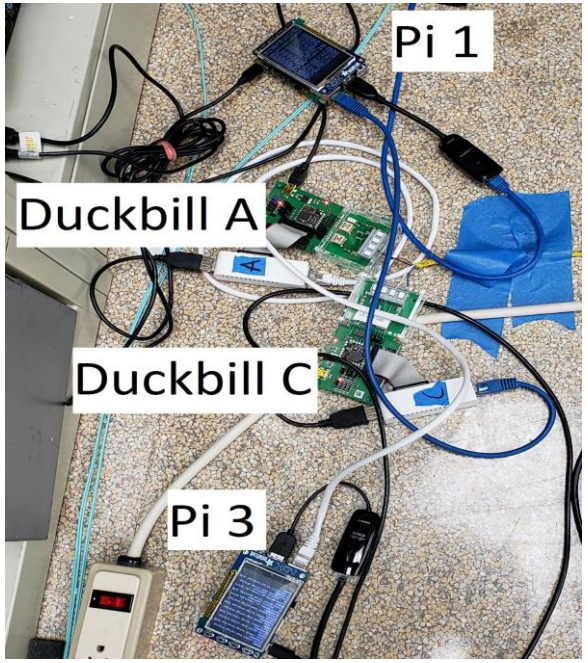
15118-20 anomaly detection (Figure 2):

- 15118-20 mandates TLS for all use cases
- Develop analysis techniques to detect anomalies patterns of encrypted network traffic.

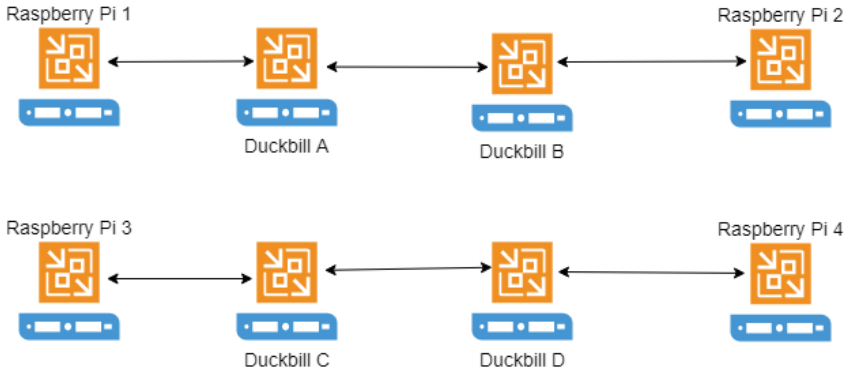
PNNL: Assessing Crosstalk and Signal Loss in Electric Vehicle Charging Communications

- Investigate the potential for HomePlug Green PHY (HPGP) crosstalk signal degradation
- On average, crosstalk resulted in 0.64 megabytes lost when cables were 1 millimeter apart
- The impacts were demonstrated to Daimler Truck NA on September 18, 2020 at PNNL

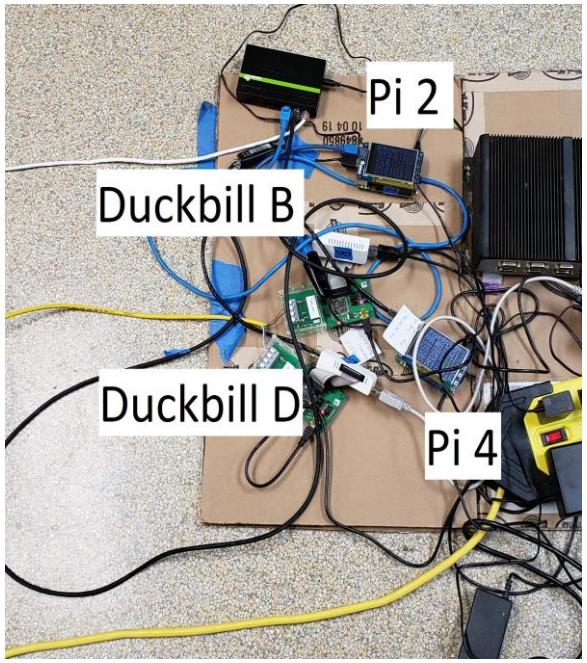
PNNL hosted Daimler Electric Heavy Vehicles



Signal Transmitter



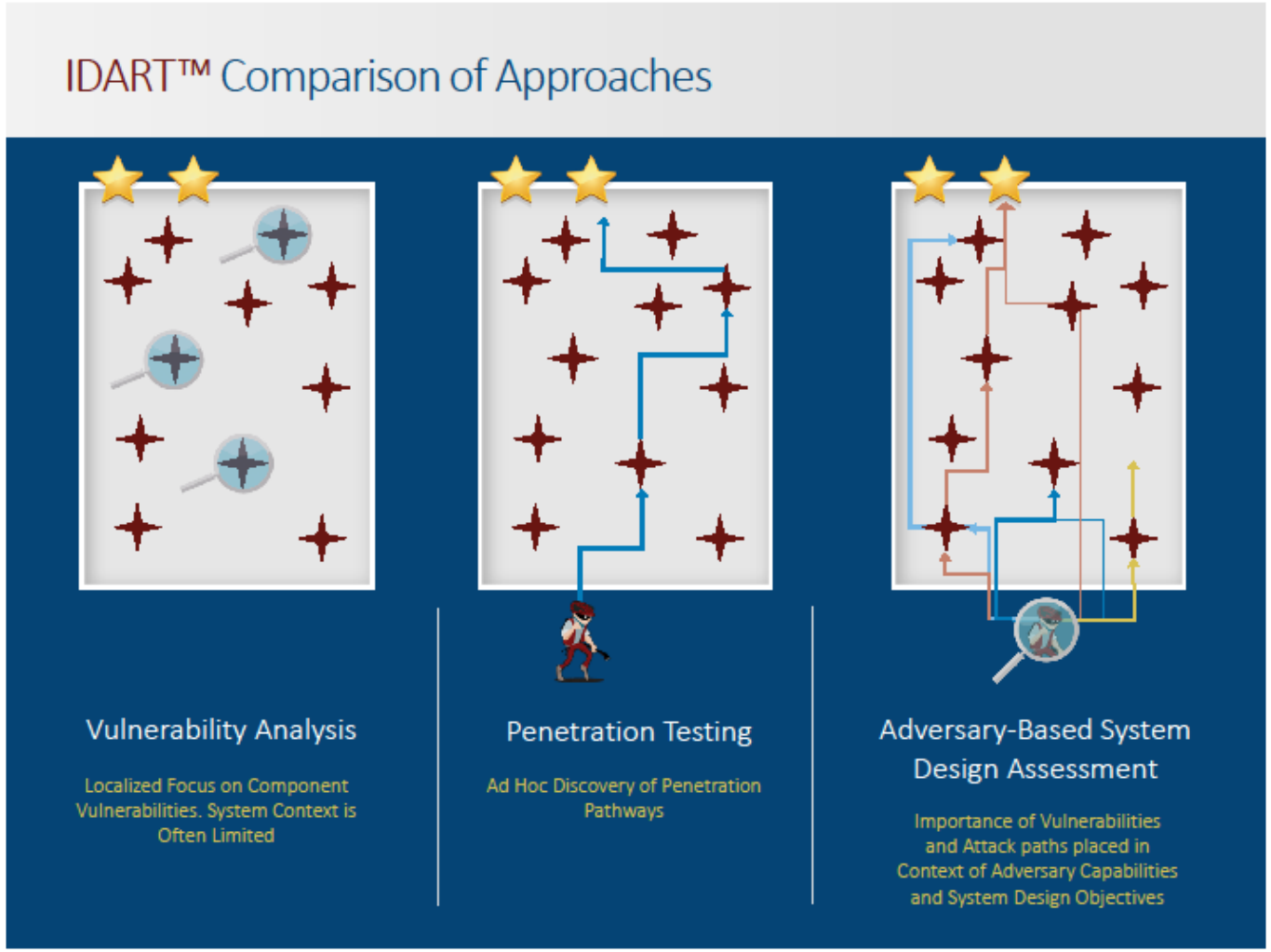
Logical Diagram



Signal Receiver

Red Team Assessments

- Can use the latest threat intelligence to appropriately model adversaries
  - More accurately reflects real-world threats
  - Evaluate systems against the latest adversary tactics, techniques, and procedures
- Ideal for situations where:
  - System is complex, or a system of systems
  - System is a target for dynamic, adaptable adversaries
  - Security trade-offs must be weighed
- The red team can build attack graphs that illustrate the various ways an adversary can attack a system
  - Identifies key components or vulnerabilities that can be exploited by an adversary
  - Central nodes can be identified and prioritized for mitigation efforts



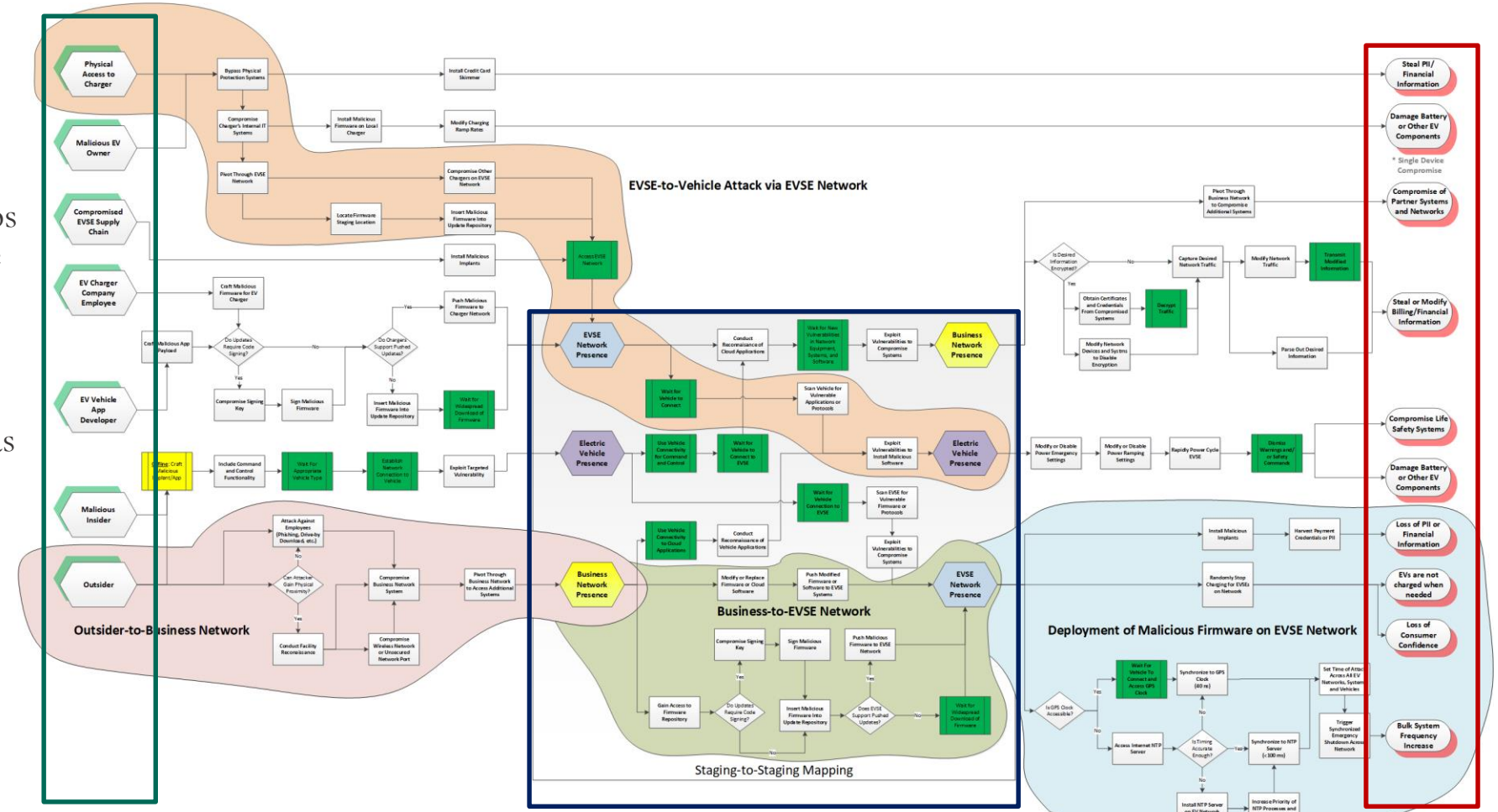
Red Team Assessments

- Gaining access to equipment required:
  - Extensive collaboration with EVSE vendors/owners
  - Building trust and cooperation with these organizations
  - Non-disclosure agreements
  - Use of non-production cloud resources for testing
  - Concurrence on rules of engagement
- To date, the red team has investigated:
  - 8 DCFCs and 4 Level 2 chargers (from 10 companies)
  - 2 backend networks
  - OCPP 1.6 and ISO 15118-2 PKI requirements
- Findings have been incorporated into best practices infographic
  - Specific vulnerability information has been provided to industry partners
  - Partners have already addressed many of the findings, or incorporated changes/mitigations into product roadmaps
  - Specific details have been abstracted out of public recommendations

EV Charging Attack Graphs

An Attack graph shows 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 advise attack graph



Access Points:
attacker starting locations

Staging Points:
network presence/pivoting

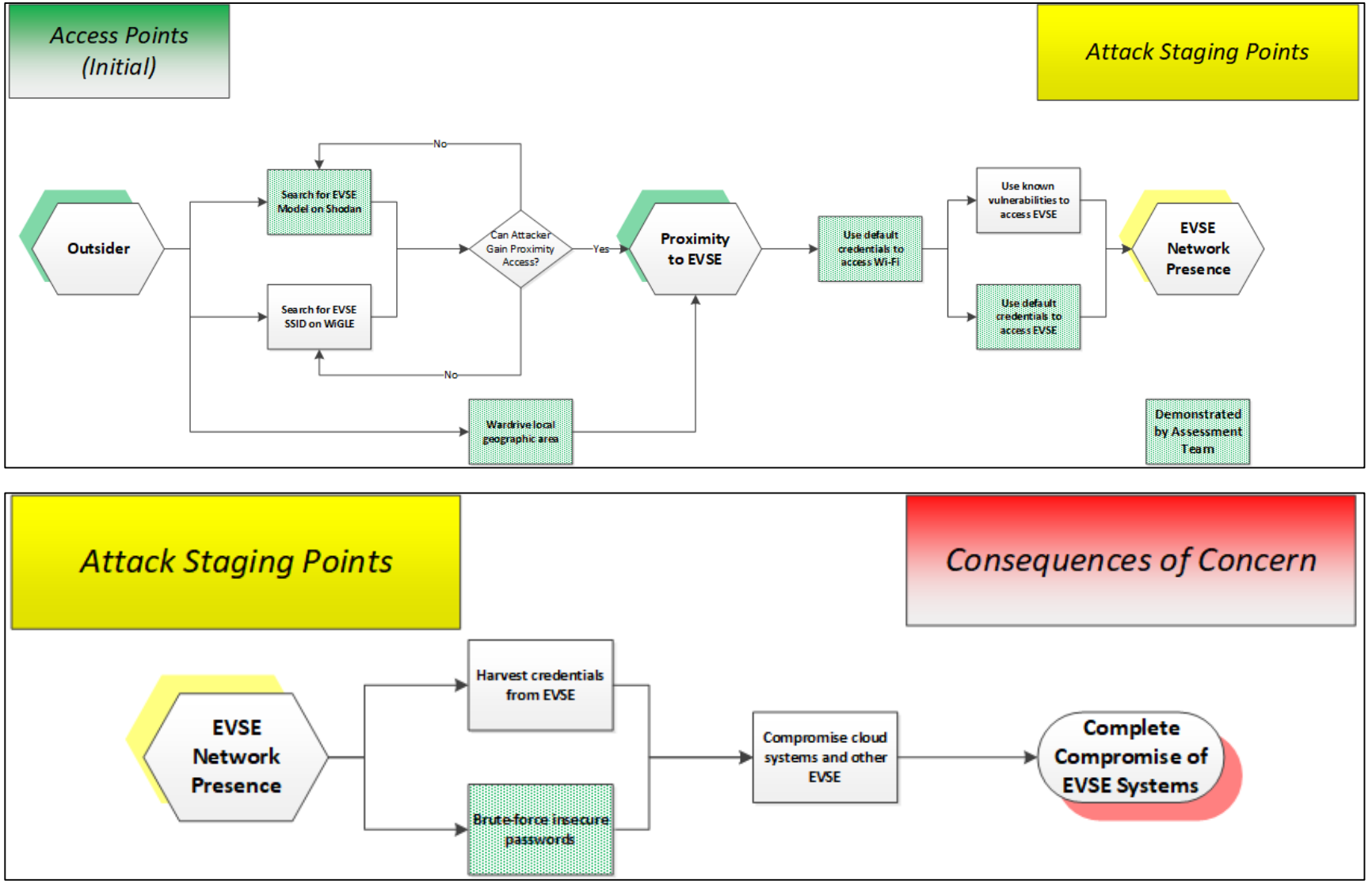
Consequences of Concern:
impacts

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

EV Charging Attack Graphs

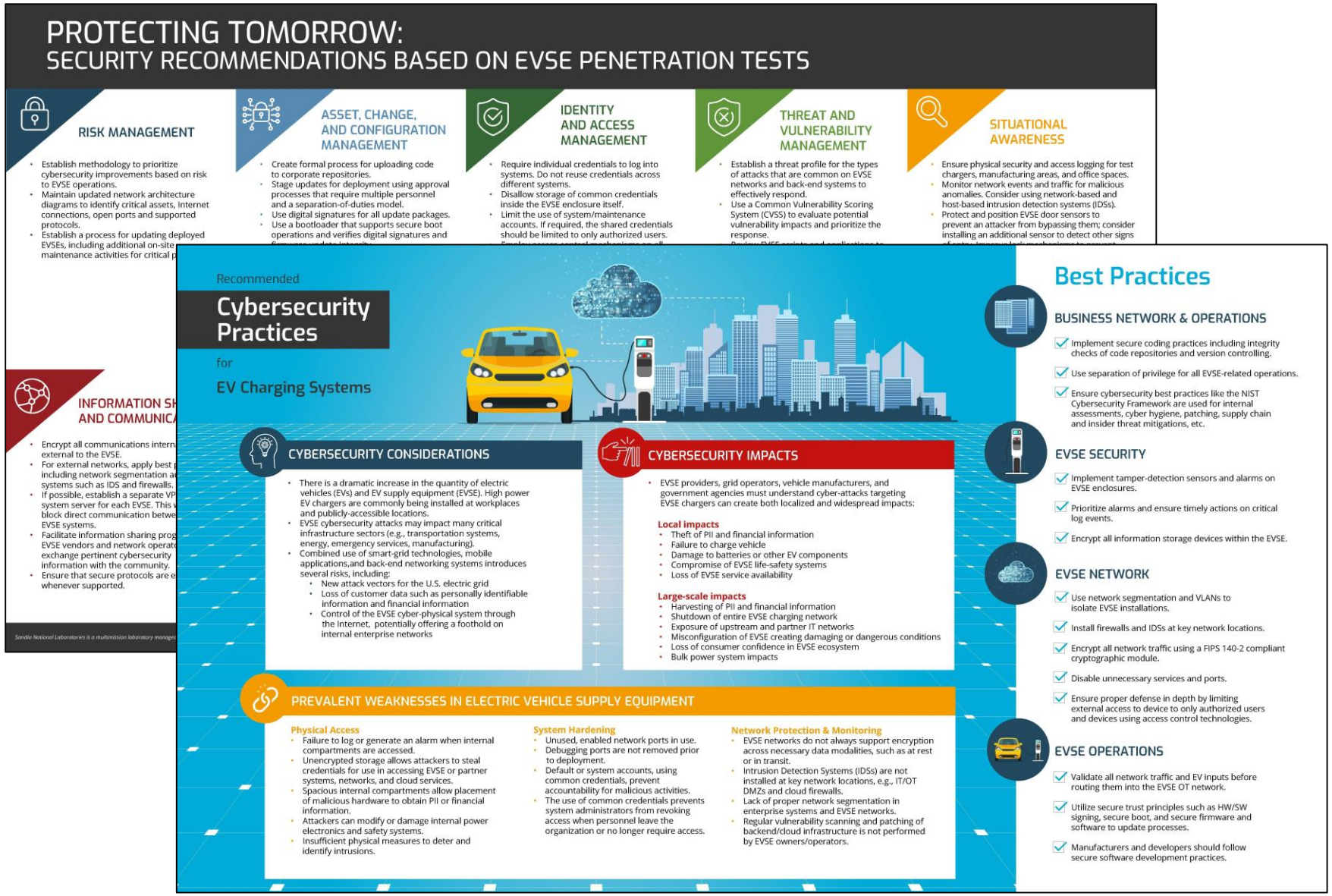
These specific graphs show the current attack path being investigated by the red team

- The green nodes have been successfully demonstrated on various EVSE models.
- Current testing is being done in partnership with an EVSE vendor.
- EVSE vendor is providing a replica of their cloud infrastructure for the assessment efforts.
- **Major Risk:** One EVSE owner was ***not aware*** of the Wi-Fi Access Point installed in the equipment.



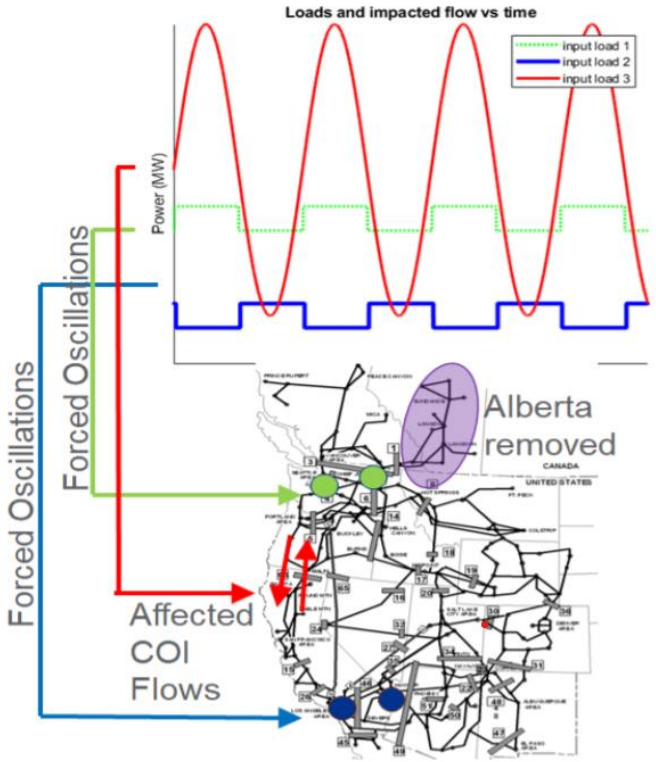
Best Practices Infographic

- Guide is based on findings from hands-on assessments of systems
  - EVSE
  - Cloud systems
  - EVSE vendor and provider:
    - Business networks
    - Processes and procedures
    - Supply chain
- Covers all critical areas of the EVSE ecosystem in a single, concise document
- Provides the high-level view of the entire ecosystem ensuring critical security aspects are not overlooked



PNNL's Update on Power System Consequences

- **Purpose**: Explore impact of load manipulation on power grid
- **Motivation**: As EV loads are linked to power grid through modern communications systems, we need to understand potential consequences malicious manipulation
- **Final Deliverable**: Electric Vehicle Infrastructure Consequence Assessment paper under internal review for submission to Electric Power Systems Research Journal.

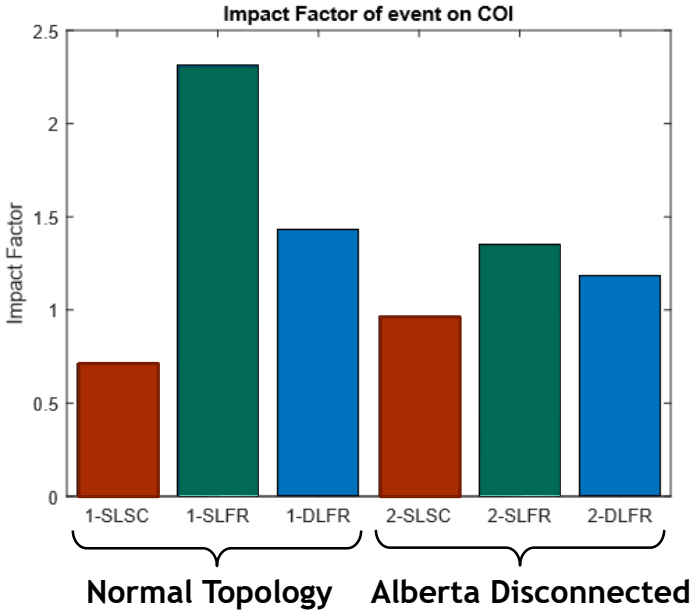


Modulate loads (red/green) north/south of COI 180 degrees out of phase to cause inter-area oscillations on COI.

- **Impact factors** for 500 MW of modulated load
  - up to ~1.4 for distributed load
  - up to ~2.4 for single well-placed load.

$$IF = \frac{Peak\ to\ peak\ path\ flow}{Controllable\ load}$$

- Inter-area oscillations put grid in elevated state of risk during system events.
- Did not find significant adverse effects caused by the events and scenarios studied.



- Single 500 MW load modulated in southern California
- Single 500 MW load with modulated at bus with largest frequency response
- 20 loads distributed around WECC (each of 25 MW) modulated. Locations chosen with large frequency responses.

Modulated loads on 20,000 bus WECC planning model to excite grid resonant frequencies.

Impact factors (IF) on California Oregon Intertie (COI) due to load modulation.

Risk Matrix and Remediation Prioritization

- PNNL's analysis on power system consequences indicates "Major" and "Severe" consequences were not attainable
- Red team assessments did not identify a full attack path that could be exploited by "Script Kiddie" attackers
- Identifying highest risk scenarios will inform DOE and industry of mitigation priorities
- Nation states can also field "Moderately Skilled Teams" which are captured in the "Possible" row
- **Future Consequence**:
  - As vehicle fleets convert to electric, loss of local charging could impact delivery of critical supplies (ex. COVID vaccines)

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

Responses to Reviewers' Comments (FY20)

Incorporating DoD and commercial red team would add value.

- Given the specialized nature of the systems, using the same team allows the team to increase its knowledge in the domain area as they conduct multiple assessments. It also improves the consistency and repeatability of the assessment activities.
- In addition, the team can apply new insights retroactively by reviewing their information on previous assessments. For example, if the team discovers a weakness in a system configuration, it can review information from previous assessments to see if that weakness also exists in those systems.

Please provide equipment lists (including software) and also spend rates versus estimated spend rates so the reviewer can understand progress against schedule and cost goals as well as "tool" sufficiency.

- This detailed information could reveal industry partners and allow the identification of specific vulnerabilities in their systems.
- For example, if an Acme Coyote 1000 EV charger was purchased, an adversary reviewing this information could assume some of the identified vulnerabilities exist in that product and attempt to exploit them.

This is a small sampling of the products for AC and DC charging.

- Agreed. The team worked with multiple organizations to investigate additional EVSE located at their sites.
- This included setting up virtual walkthroughs and remote access to systems since COVID restrictions prevented on-site assessments to be conducted.

STRIDE should be used in conjunction with Common Vulnerability Scoring System or Security Cards.

- Threat modeling was undertaken to investigate the structural vulnerabilities of EV charging infrastructure and ecosystem. The threat analysis occurred over an abstract charging infrastructure system model and was scoped to identify consequences that could impact electric grid and transportation sections. If the threat modeling occurred on a real-world system, application of CVSS is feasible as we have the system and environment information to score the metric. As the employed abstract model did not have this fidelity, CVSS was not applicable.
- While we started the endeavor using Stride, we derived a consequence-centric extension to (i) discover adverse consequences related to electricity, transportation, or both; and (ii) focus subsequent modeling and analysis on threats that may precipitate the consequence. The extension enhanced the analysis, allowing us to understand how the system may impact the environment.

Partnerships/Collaborations

National Lab Team: SNL, PNNL, ANL
Government Partners: DOT Volpe Center, NREL
Industry Partners:

- National Motor Freight Traffic Association, Inc. (NMFTA)
- Multiple leading DC Fast Charging (DCFC) vendors
  - Additional equipment access from several more
- Electric Power Research Institute (EPRI)
- Society of Automotive Engineers (SAE) PKI consortium
- Large utility partner

External Collaborators: The team continues to work closely with DOE VTO-funded cybersecurity projects and government agencies, including:

- DHS
- DOT
- Navy
- Army
- DOE FEMP
- DOE CESER

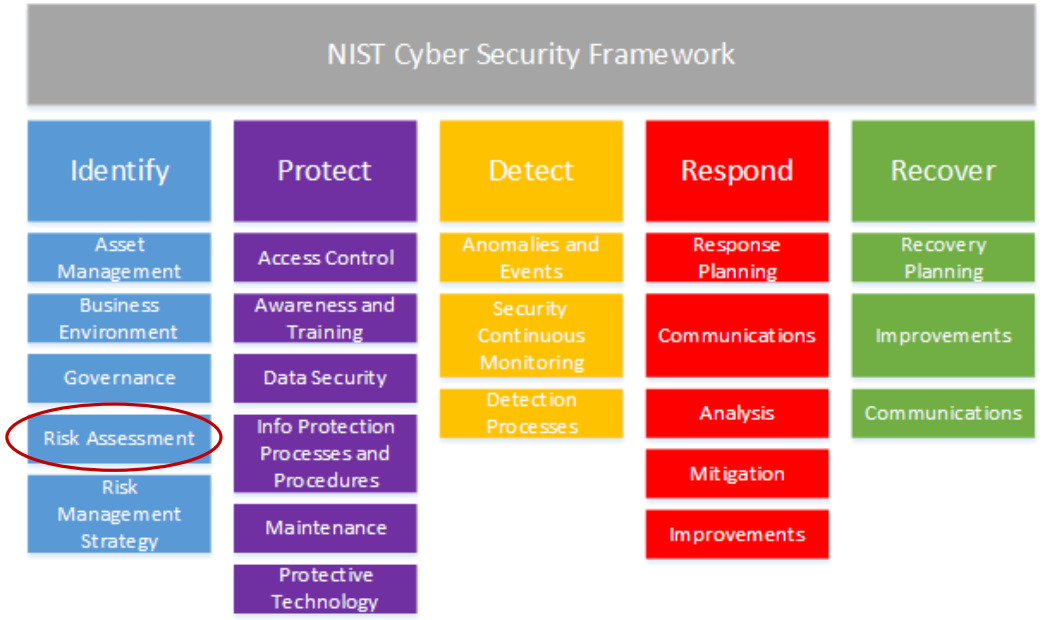
Remaining Challenges and Barriers / Future Research

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/prevention systems**, and anomaly detection.
- Researching **response mechanisms** to prevent further adversary actions on the system, nonrepudiation technologies, and dynamic responses.
- Creating hardware- and software-based fallback and **contingency operating modes.**



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.

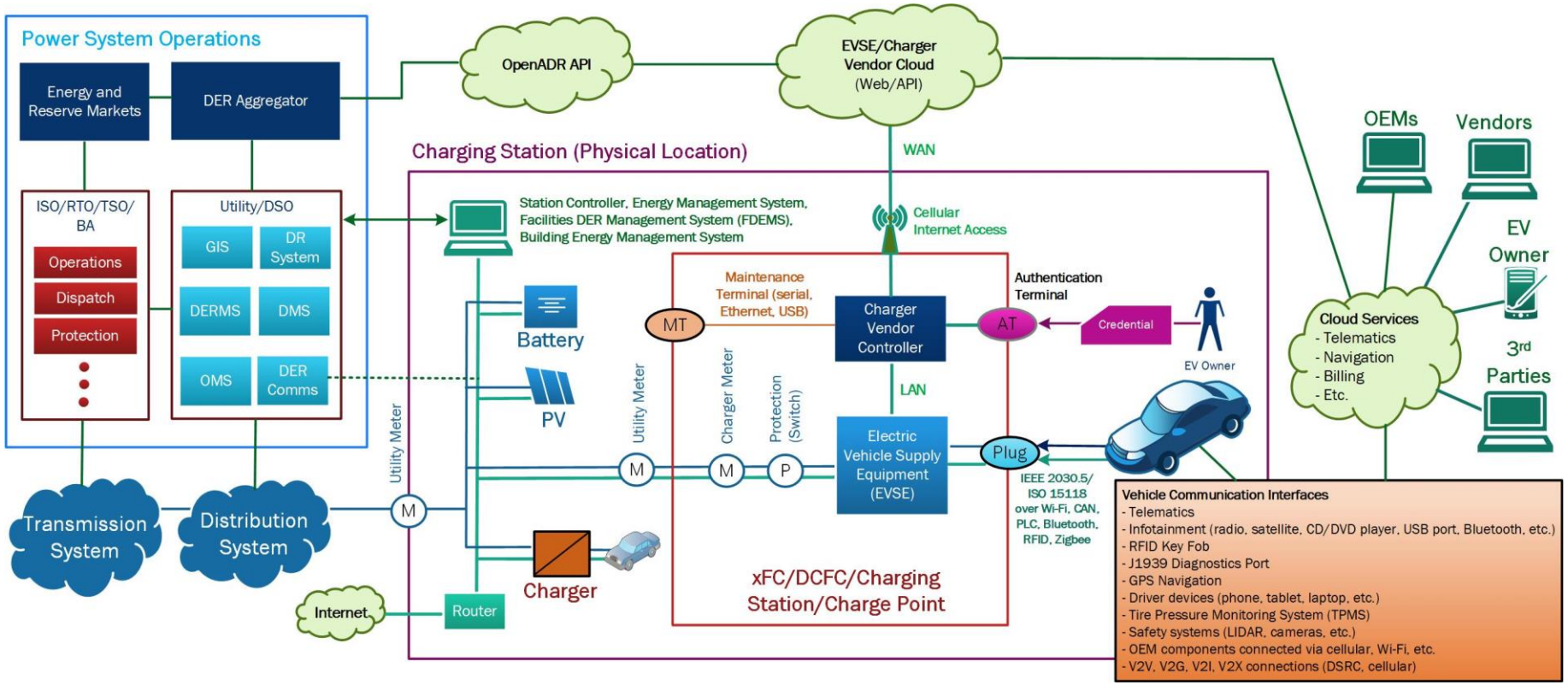
- To accomplish this, the team is:
  - Conducting adversary-based assessments of charging equipment
  - Creating threat models and attack graphs of the EV ecosystem to estimate the probability of different attacks
  - Analyzing power system impact for different attack scenarios

- This is **only the beginning of a long process to secure charging infrastructure from cyber attacks**.

Technical Backup Slides

EV Charging Components and Information Flows

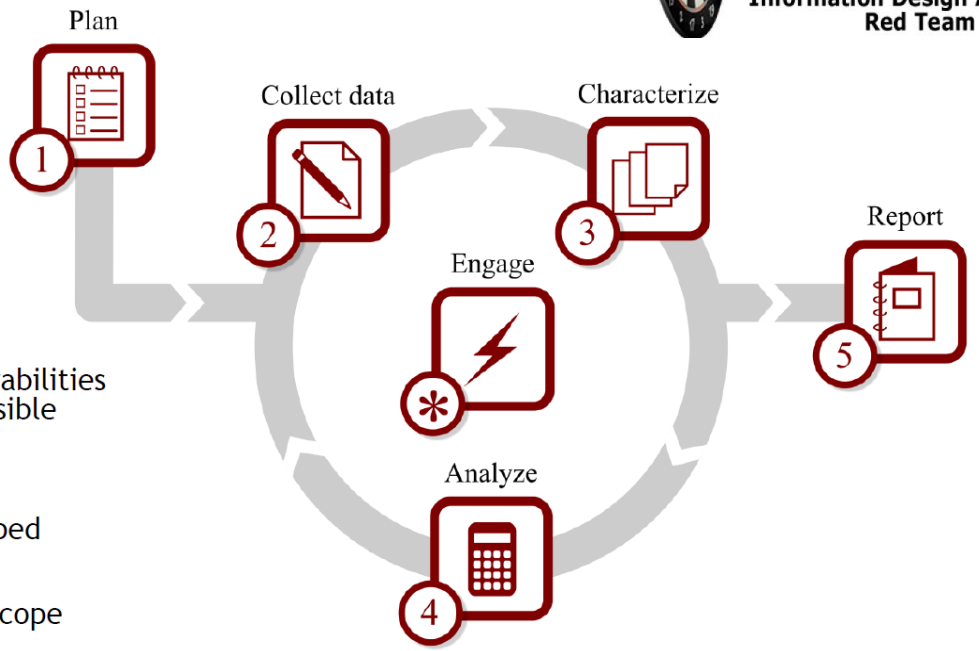
Created common nomenclature and enumerate assets and interfaces.



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



Risk Matrix and Remediation Prioritization

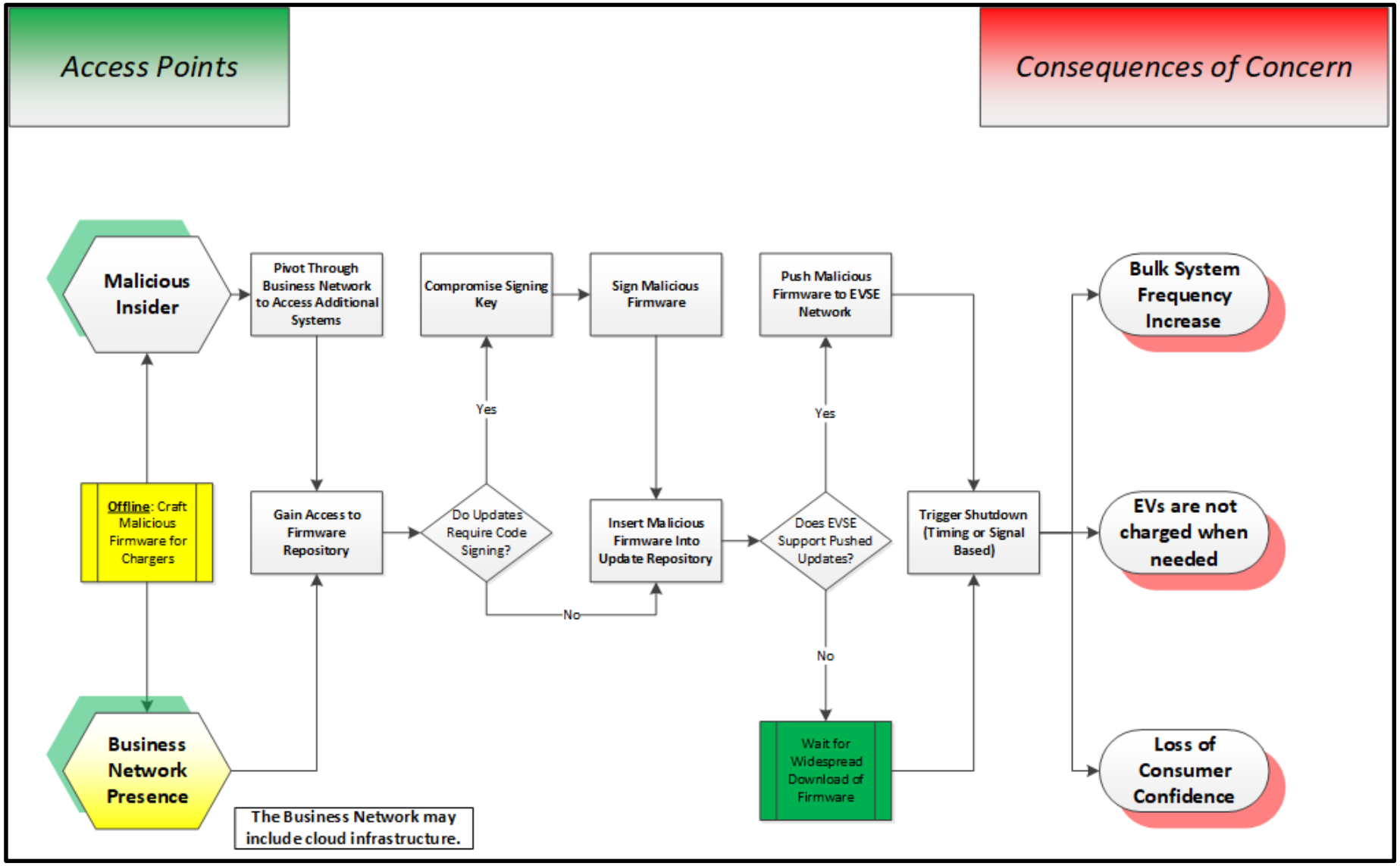
- For each attack scenario, likelihood of success and potential power system impact will be used to estimate risk.
  - Risk = Probability * Impact
  - Probability: estimated from threat model and vulnerability assessments
  - Impact: determined from power system simulations
- Identifying highest risk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

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

Likelihood axis advised by:
[1] M. Mateski, et al. “Cyber Threat Metrics” SAND2012-2427.
[2] D.P. Duggan, S.R. Thomas, C.K.K. Veitch, L. Woodard. “Categorizing Threat: Building and Using a Generic Threat Matrix.” SAND2007-5791.

Consequence axis advised by:
[3] J. Johnson, et al., “Power System Effects and Mitigation Recommendations for DER Cyber Attacks,” IET Cyber-Physical Systems: Theory & Applications, Jan 2019.

Deployment of Malicious Firmware



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

Initial EVSE Hardening Recommendations

Implementation of industry best practices across all networks

- Critical business systems should be well protected and accessible only to essential personnel
- Limit connections between different networks
- Log and monitor events within the various networks
- Require digital signatures for all software and firmware
- Utilize multi-factor authentication and separation of duty principles for critical activities

Physically secure EVSE to prevent tampering

- Ensure the supply chain is secure and spot check hardware before deployment
- Monitor EVSE systems for unscheduled physical access