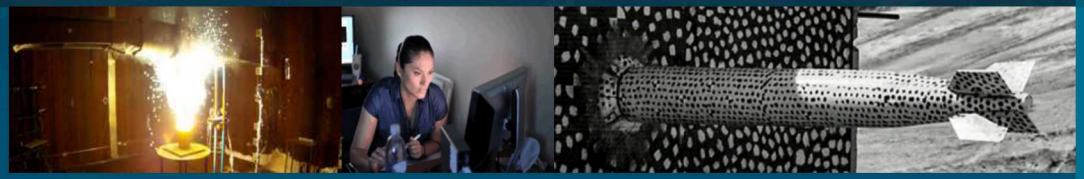
SAND2019-4145PE

Securing Vehicle Charging Infrastructure



2019 DOE Vehicle Technologies Office Annual Merit Review

Arlington, VA
June 10-13, 2019

PRESENTED BY

Jay Johnson, Sandia National Laboratories

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

Project ID: ELT198

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

$1M Project (Oct 2018–Sept 2019) (60% complete)

- Team: Sandia, PNNL, ANL
- Partners: DOT Volpe Center, NMFTA, BTCPower

Project objective: Create a cybersecurity threat model and perform a technical risk assessment of electric vehicle supply equipment (EVSE), so that automotive, charging, and utility stakeholders can better protect customers, vehicles, and power systems in the face of new cyber 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

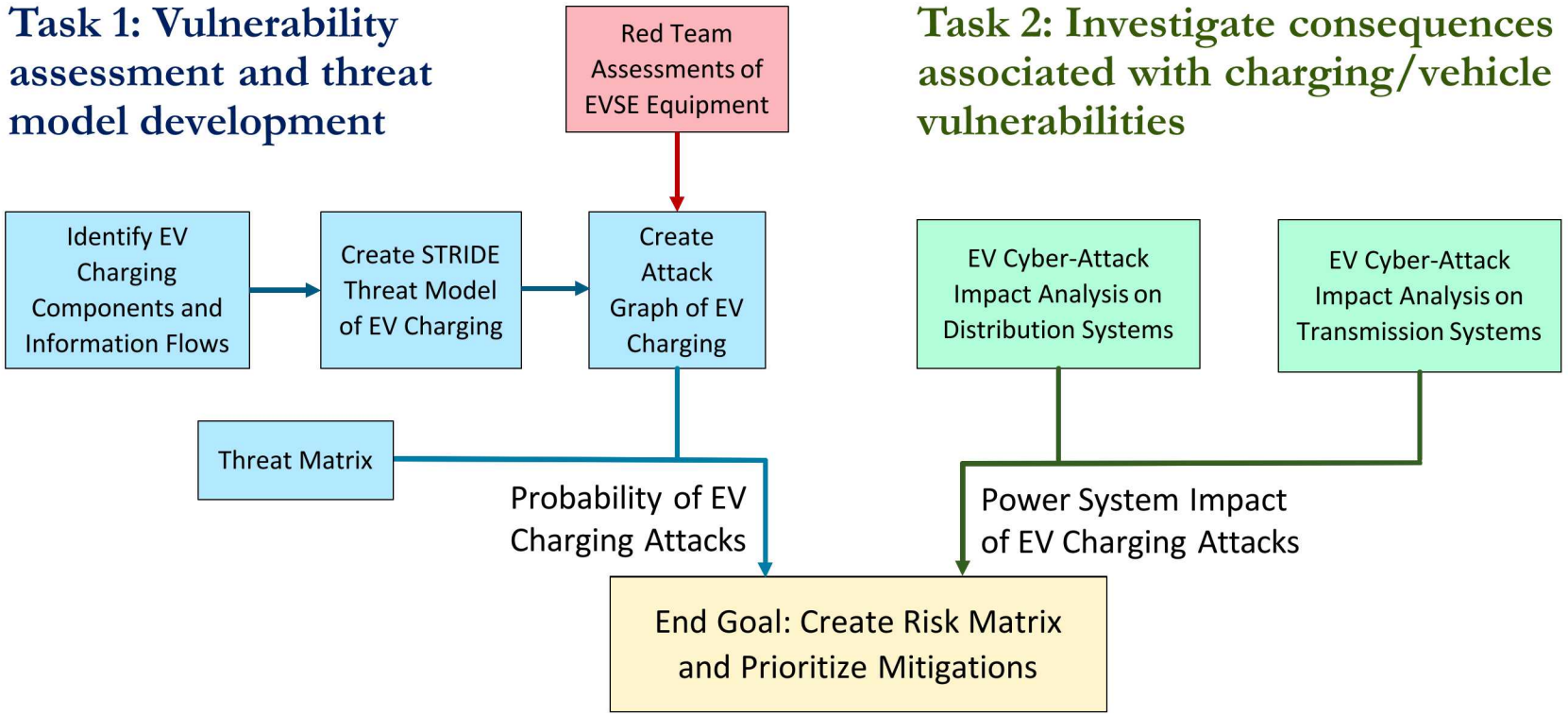
Primary goal: protect US critical infrastructure and improve energy security through technical analysis of the risk landscape presented by massive deployment of interoperable electric vehicle chargers.

- 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

Approach


Task 1: Vulnerability assessment and threat model development
Red Team Assessments of EVSE Equipment
Identify EV Charging Components and Information Flows
Create STRIDE Threat Model of EV Charging
Create Attack Graph of EV Charging
Threat Matrix
Probability of EV Charging Attacks
Task 2: Investigate consequences associated with charging/vehicle vulnerabilities
EV Cyber-Attack Impact Analysis on Distribution Systems
EV Cyber-Attack Impact Analysis on Transmission Systems
Power System Impact of EV Charging Attacks
End Goal: Create Risk Matrix and Prioritize Mitigations

STRIDE Threat Model of EV Charging

STRIDE Threat Modelling (by Microsoft)

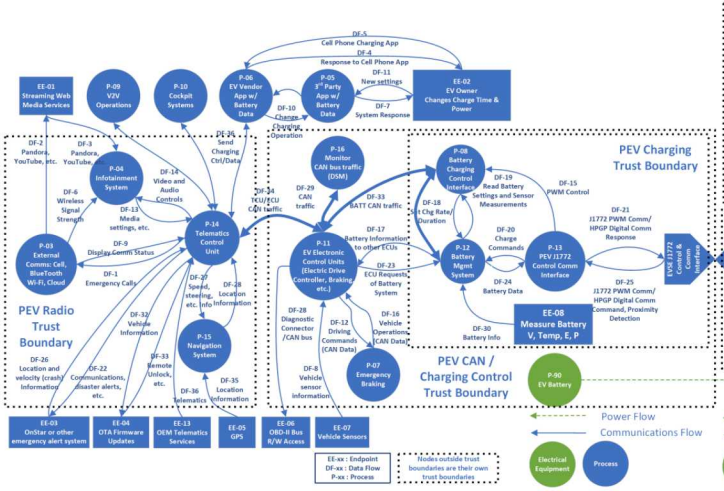
- Helps identify potential vulnerabilities in products/systems
- Step 1: Identify assets, access points, and information flows
- Step 2: List all potential STRIDE threats
- Step 3: Create mitigation plan

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

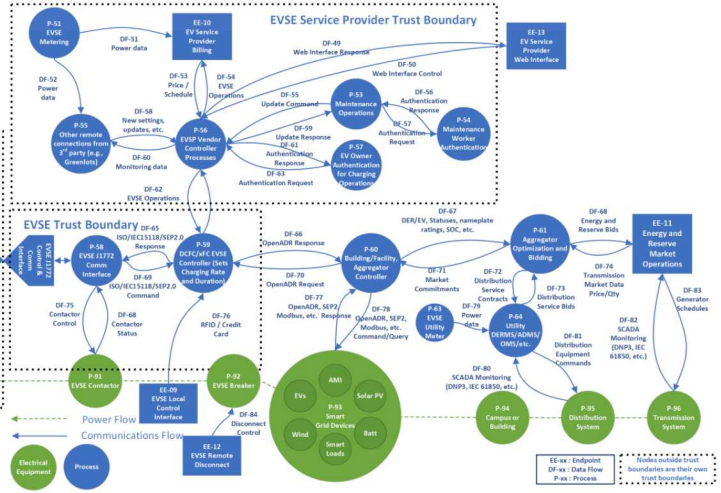
Model Inputs

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

STRIDE Threat Model for PEV Charging (Vehicle Side)



STRIDE Threat Model for PEV Charging (EVSE / Power Side)

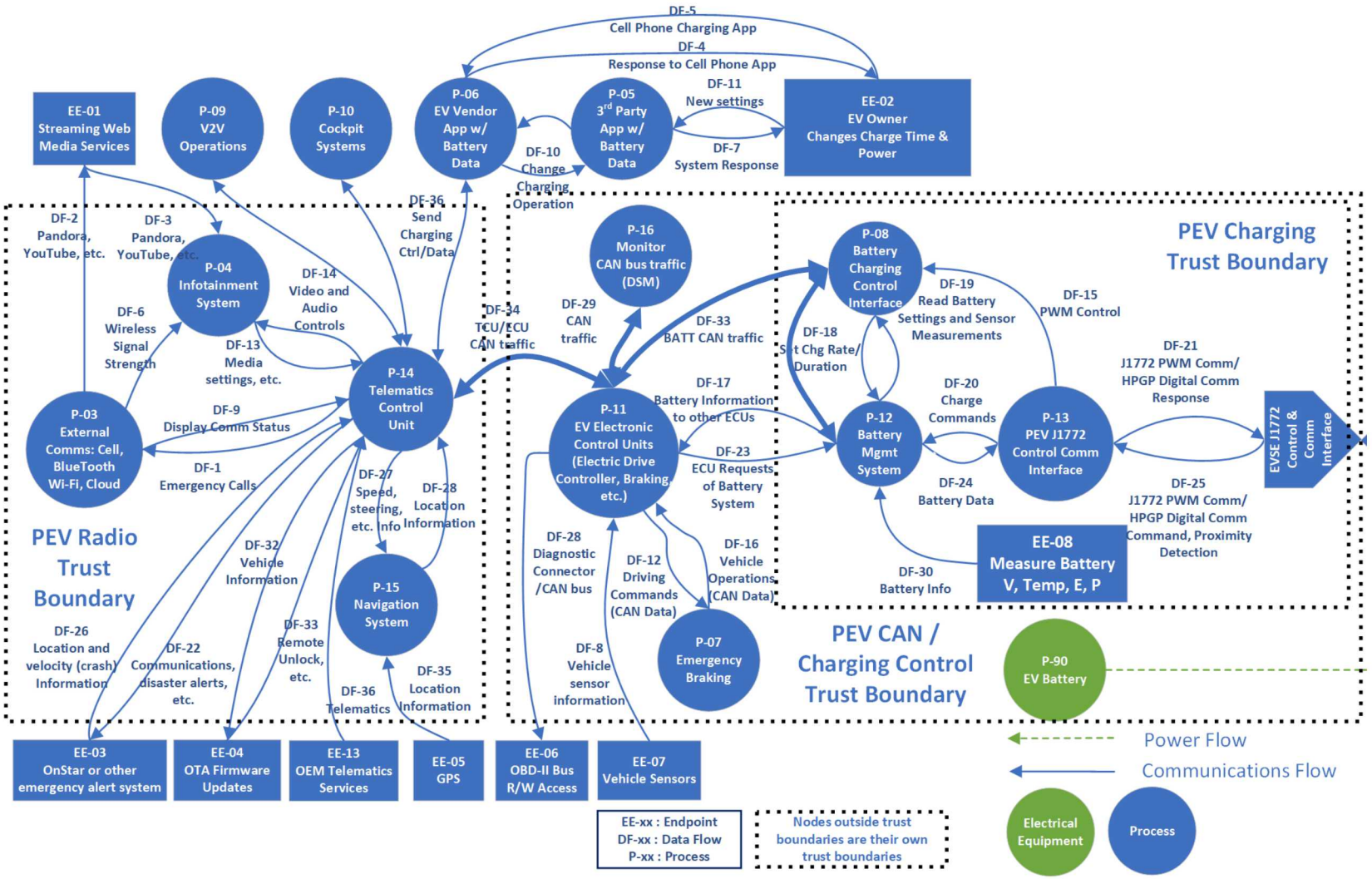


Threat model includes:

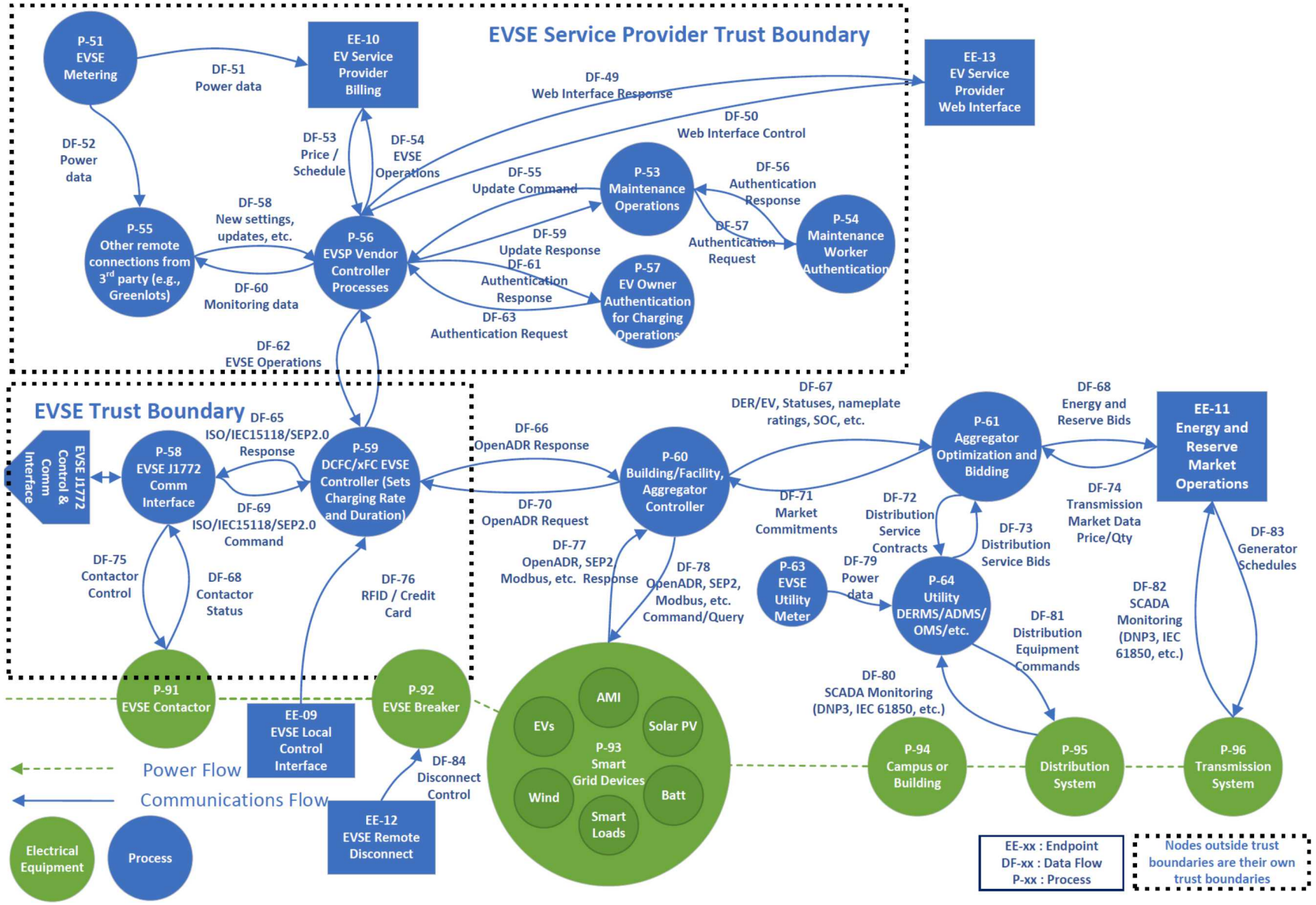
- Processes (P)
- Data Flows (DFs)
- Endpoint (EE)
- Trust Boundaries (dashed)
- Electrical Equipment (green)

Milestone 1: Complete draft threat model for vehicles/charging infrastructure with prioritized vulnerabilities and enumerated communication entities/interfaces.

PEV STRIDE Threat Model

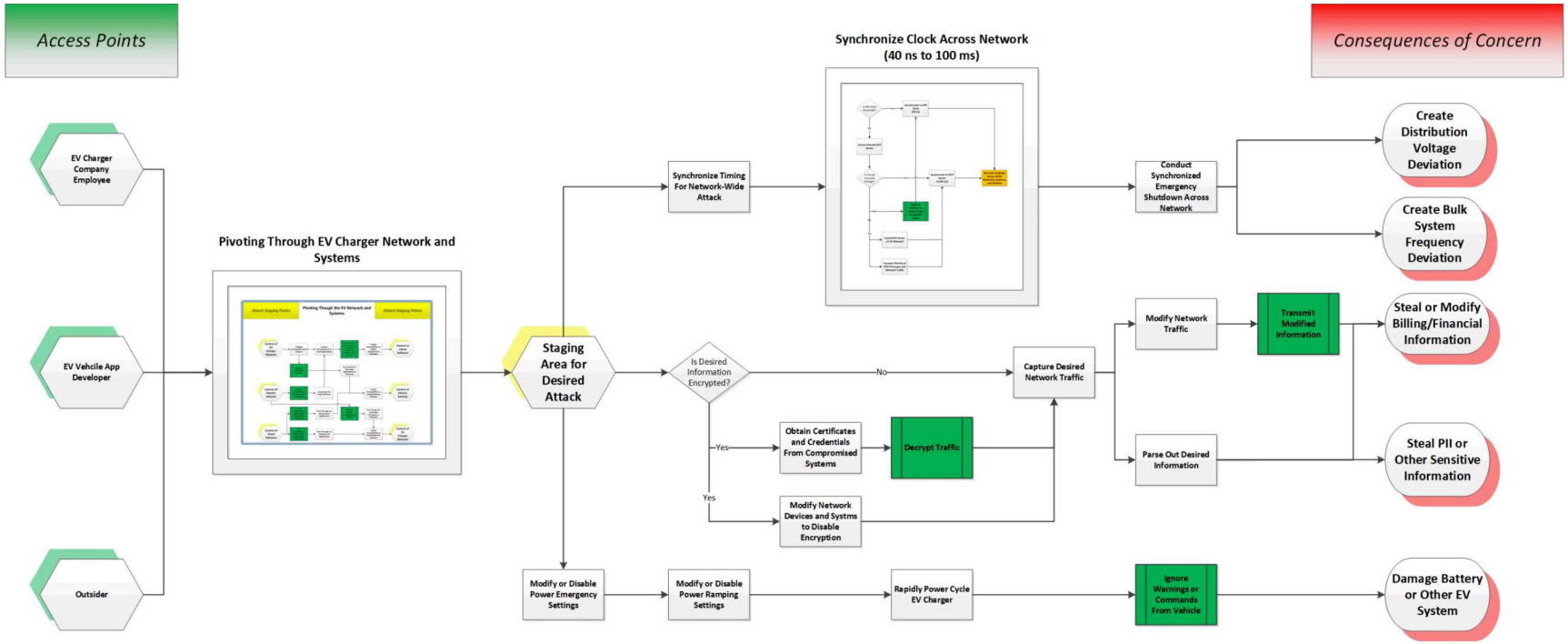


EVSE STRIDE Threat Model



EV Charging Attack Graph

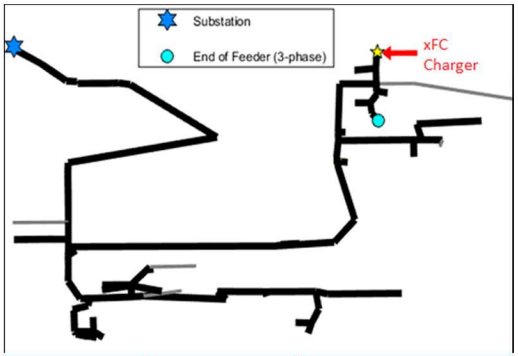
- Attack graphs show attacker actions to achieve an objective
  - Illustrates access points, staging areas, and consequences of concern
  - Graphically illustrates the steps an attacker must take to move from system/network access to the consequences of concern
  - Complex steps are displayed as images
  - 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?



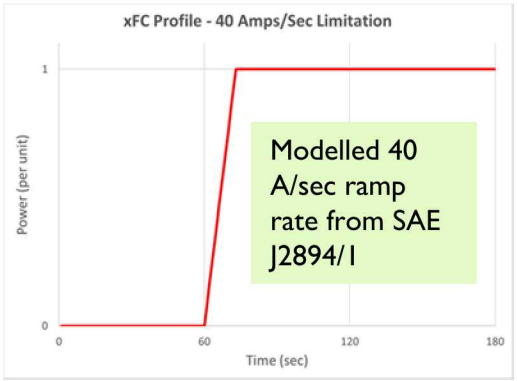
Distribution system impact analysis

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).

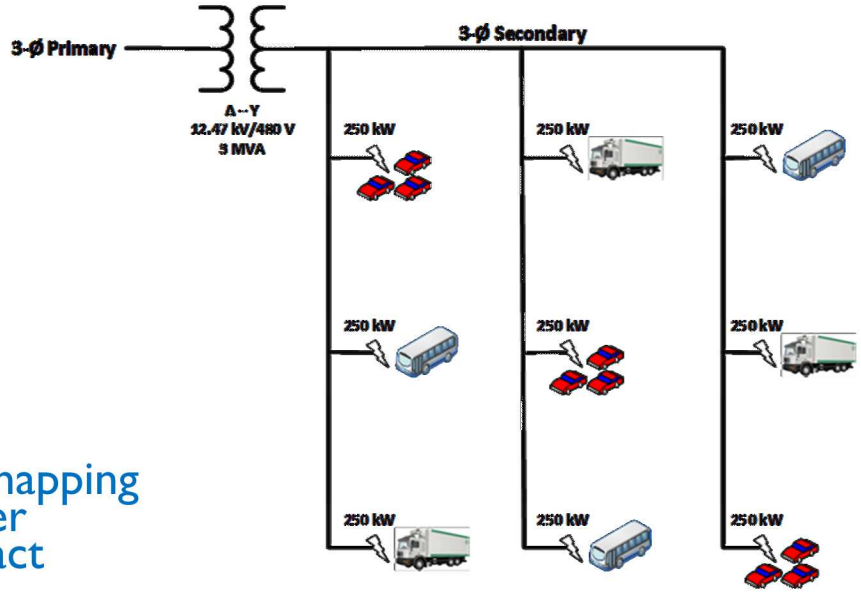


Load Period	Date/Time	Feeder Demand (kW)
Peak	7/22 @ 13:00	3946
Minimum	3/22 @ 23:00	1483



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.

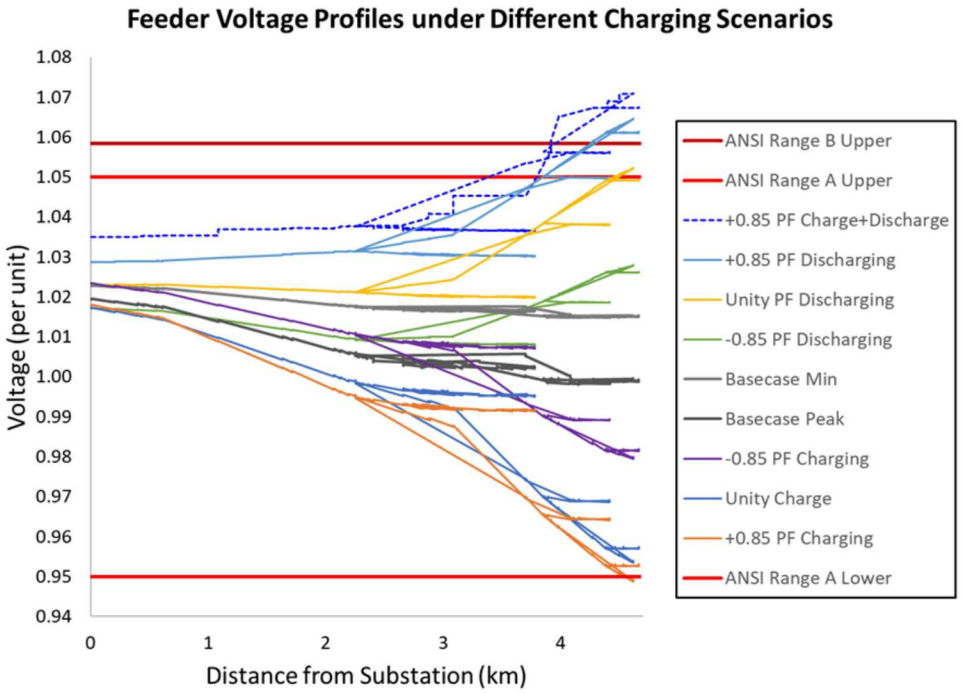


Milestone 2: Complete consequence study mapping EV/charging potential vulnerabilities to power system and other critical infrastructure impact

Distribution System Impact Analysis

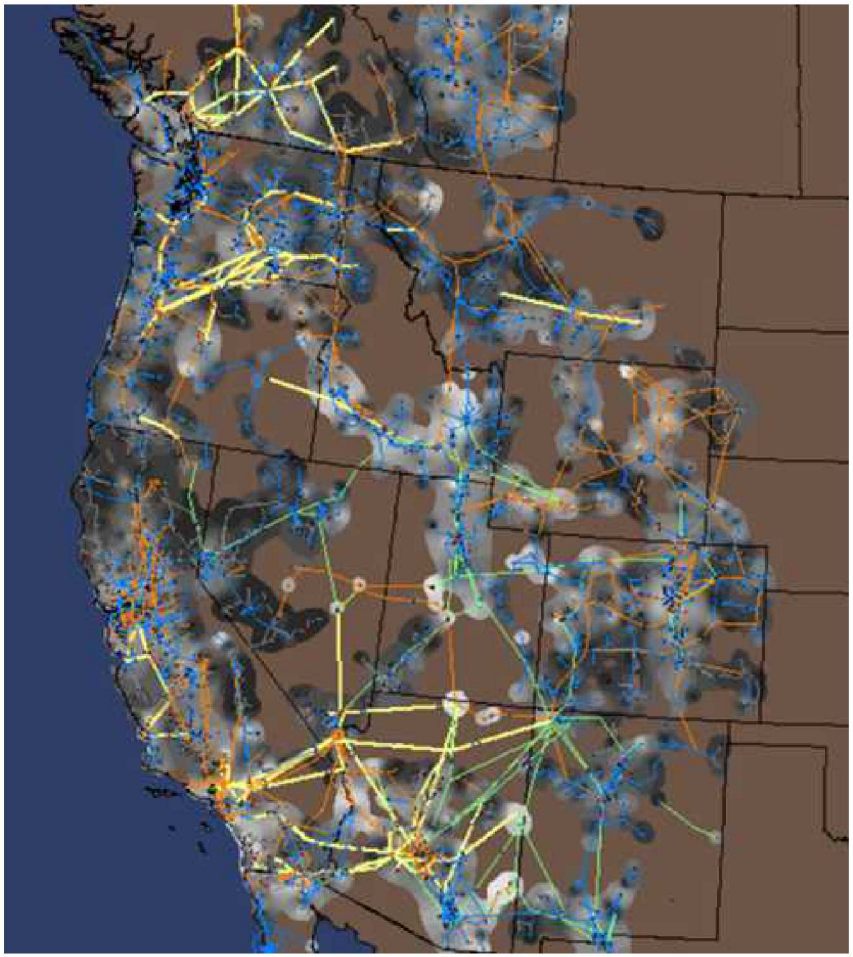
- Simulation cases:
  - Base cases with no chargers at each feeder load period (peak and min load)
  - Charging or discharging at unity PF and ±0.85 PF (i.e., with grid-support capabilities)
  - 150 s charge and then discharge case at 0.85 PF
    - charging causes the load tap changing transformer (LTC) 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



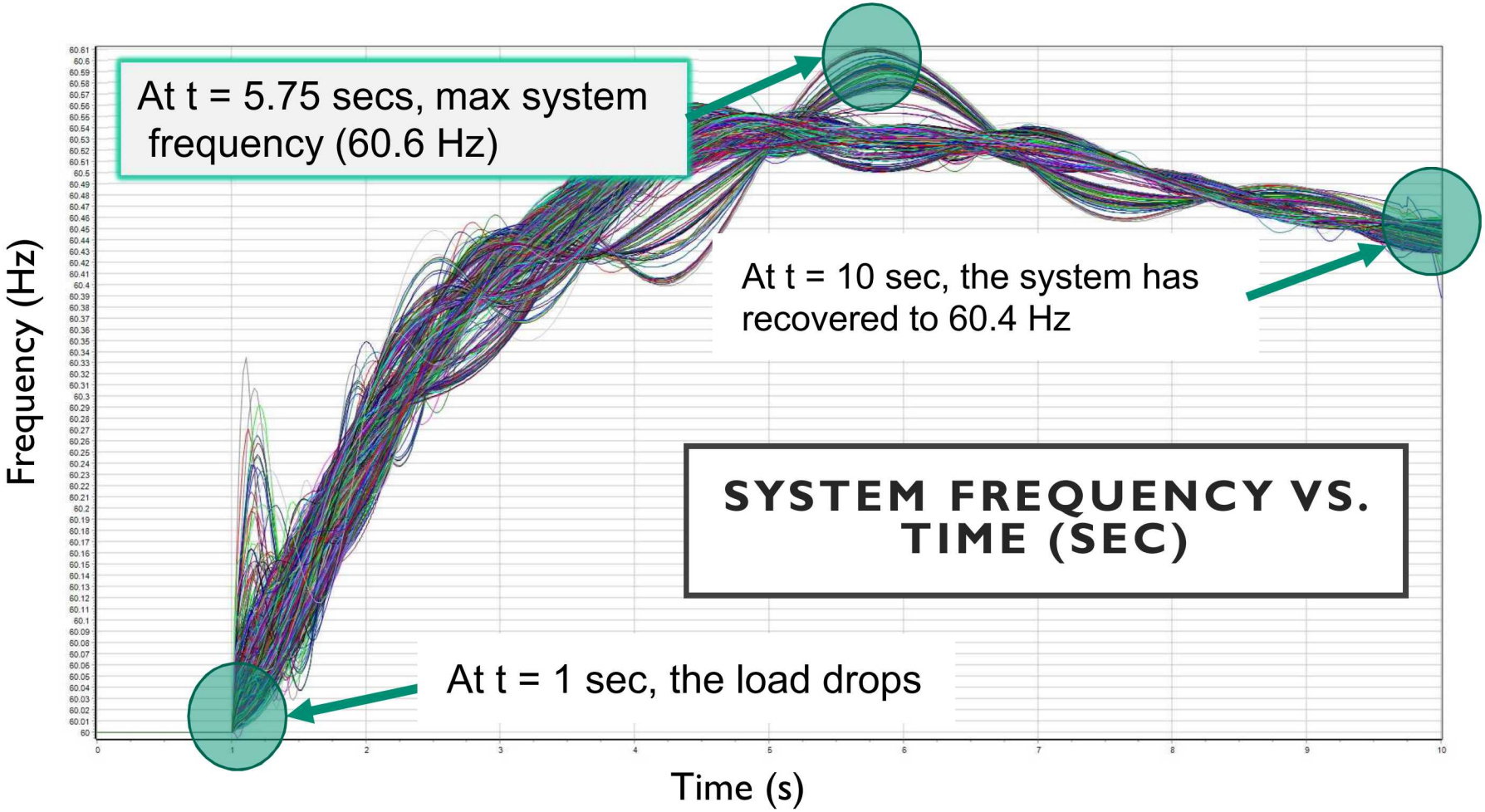
Transmission System Consequences

- 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

Partnerships/Collaborations

National Lab Team: SNL, PNNL, ANL

Government Partners: DOT Volpe Center

Industry Partners: BTCPower, NMFTA

The team worked with DOE VTO to arrange a coordination meeting April 23-24 in Albuquerque with the VTO-funded cybersecurity projects and government agencies, including:

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

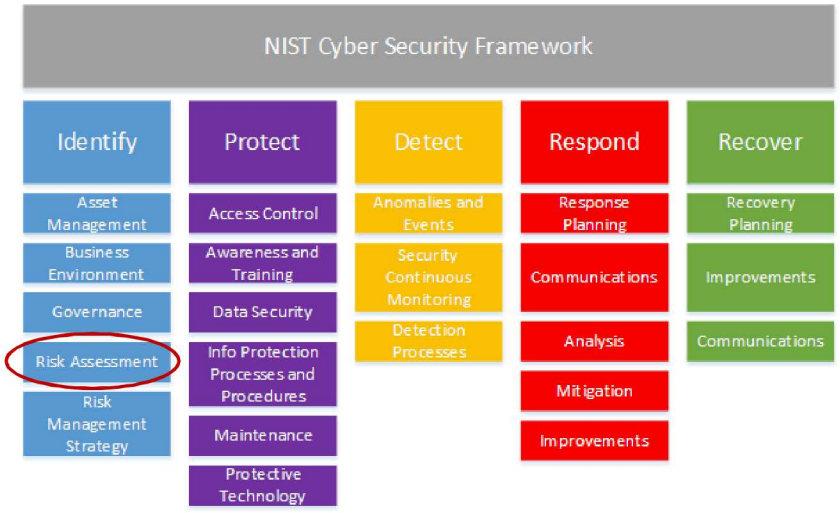
Remaining Challenges and Barriers / Future Research

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 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**.



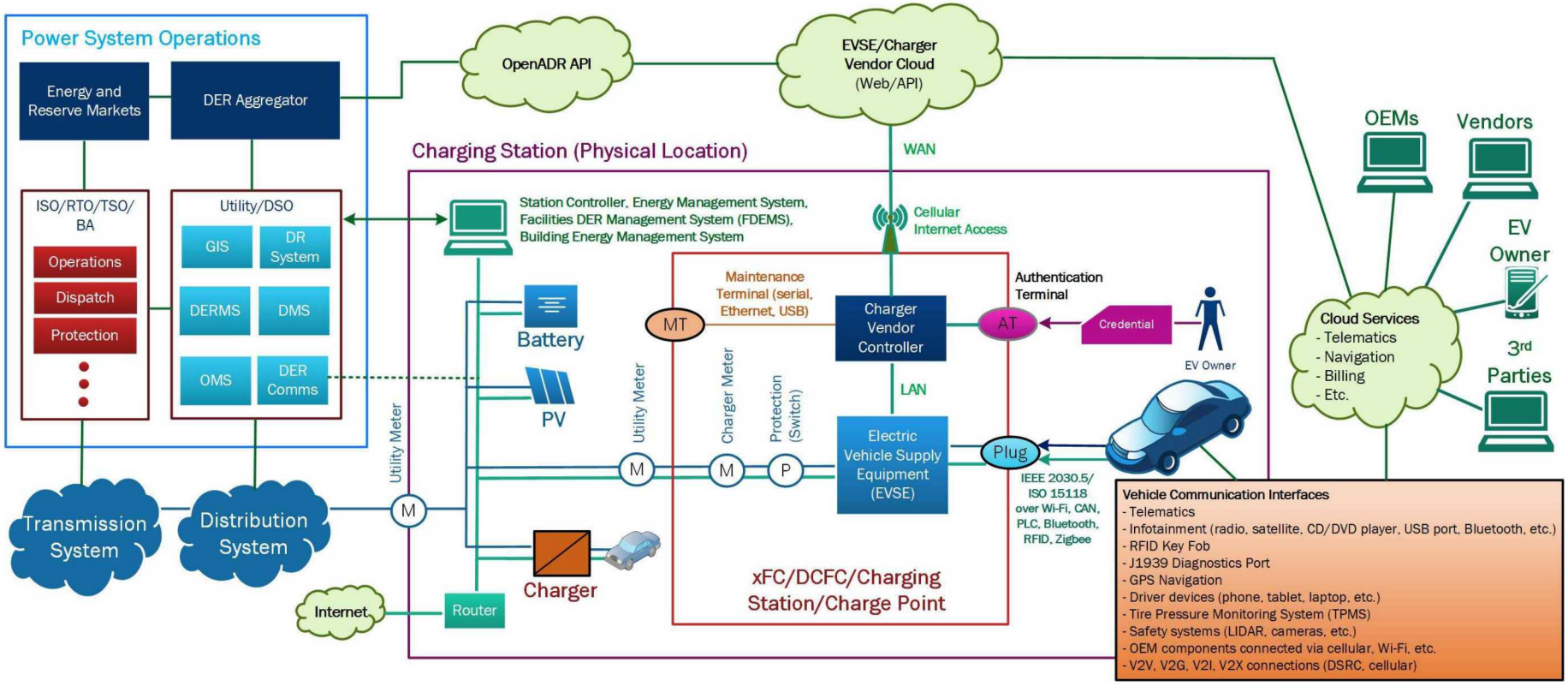
Summary

- **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

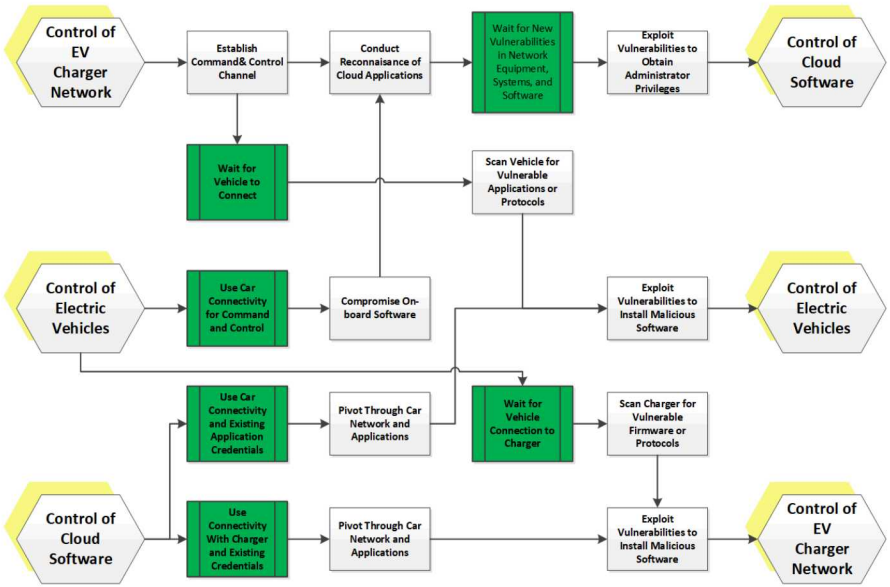
EV Charging Components and Information Flows

Created common nomenclature and enumerate assets and interfaces.

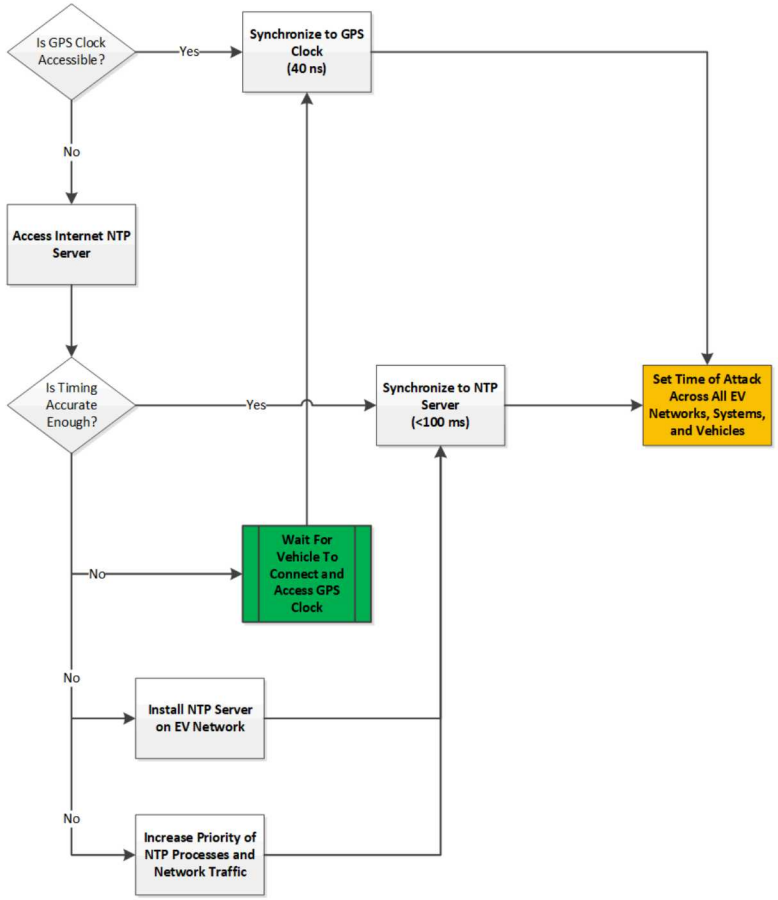


Two Major Concerns in Large-Scale Attack

Pivoting Between Systems to Access Desired Data Flows



Synchronizing Attack Timing



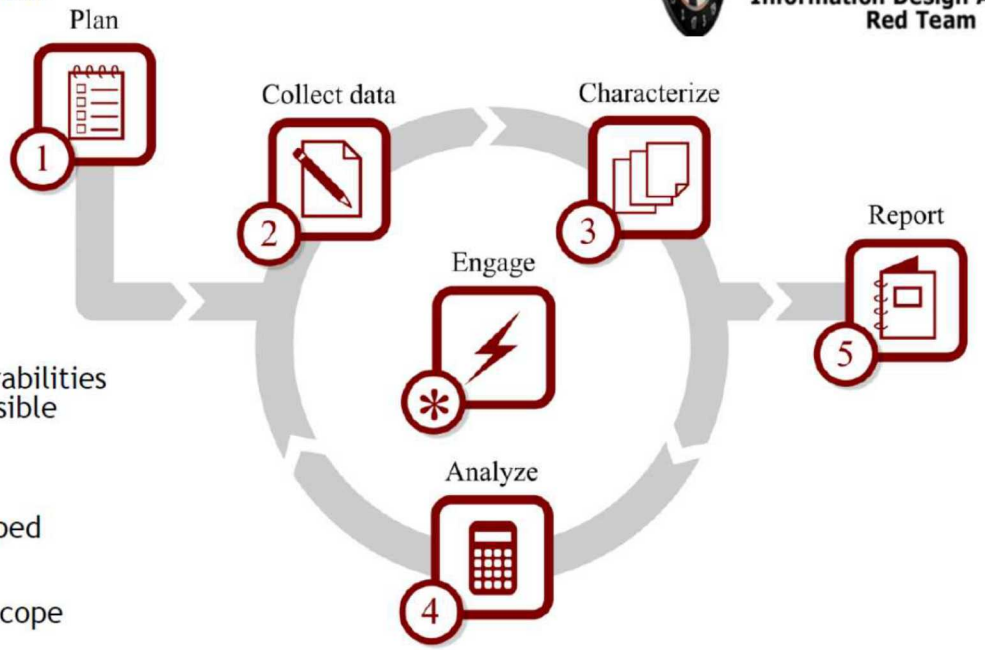
Legend:

- 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)

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



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