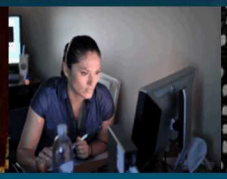
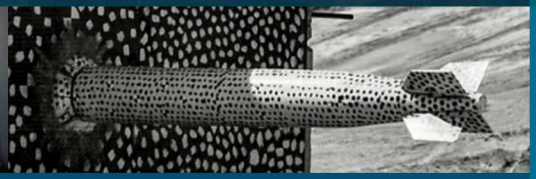
SAND2020-0818C

Securing Vehicle Charging Infrastructure Against Cybersecurity Threats





Hybrid and Electric Vehicle Technologies Symposium

Pasadena, CA

January 28-30, 2020

PRESENTED BY

Benjamin Anderson, Sandia National Laboratories

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

SAND Number XXX

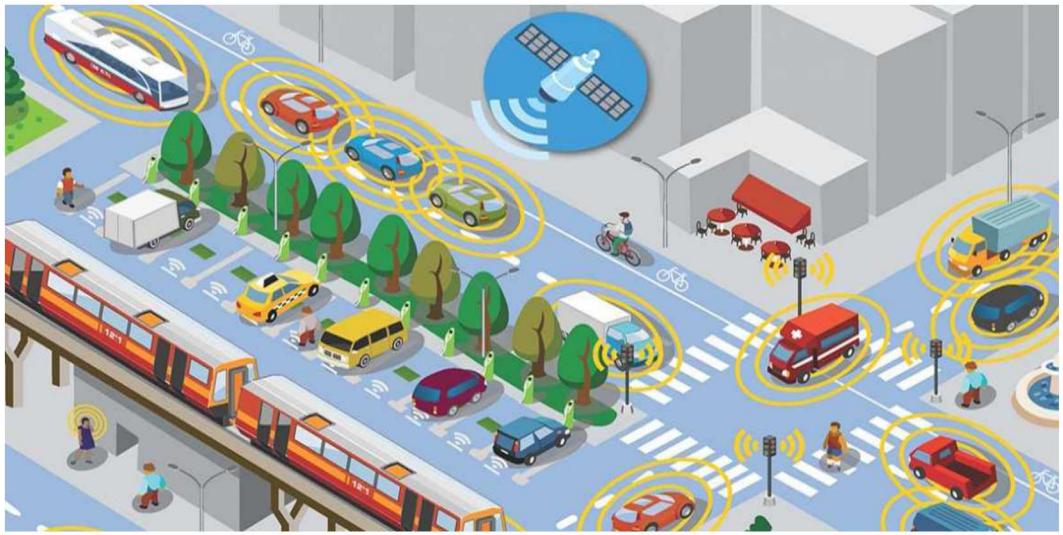
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Project 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**.



Project Overview

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

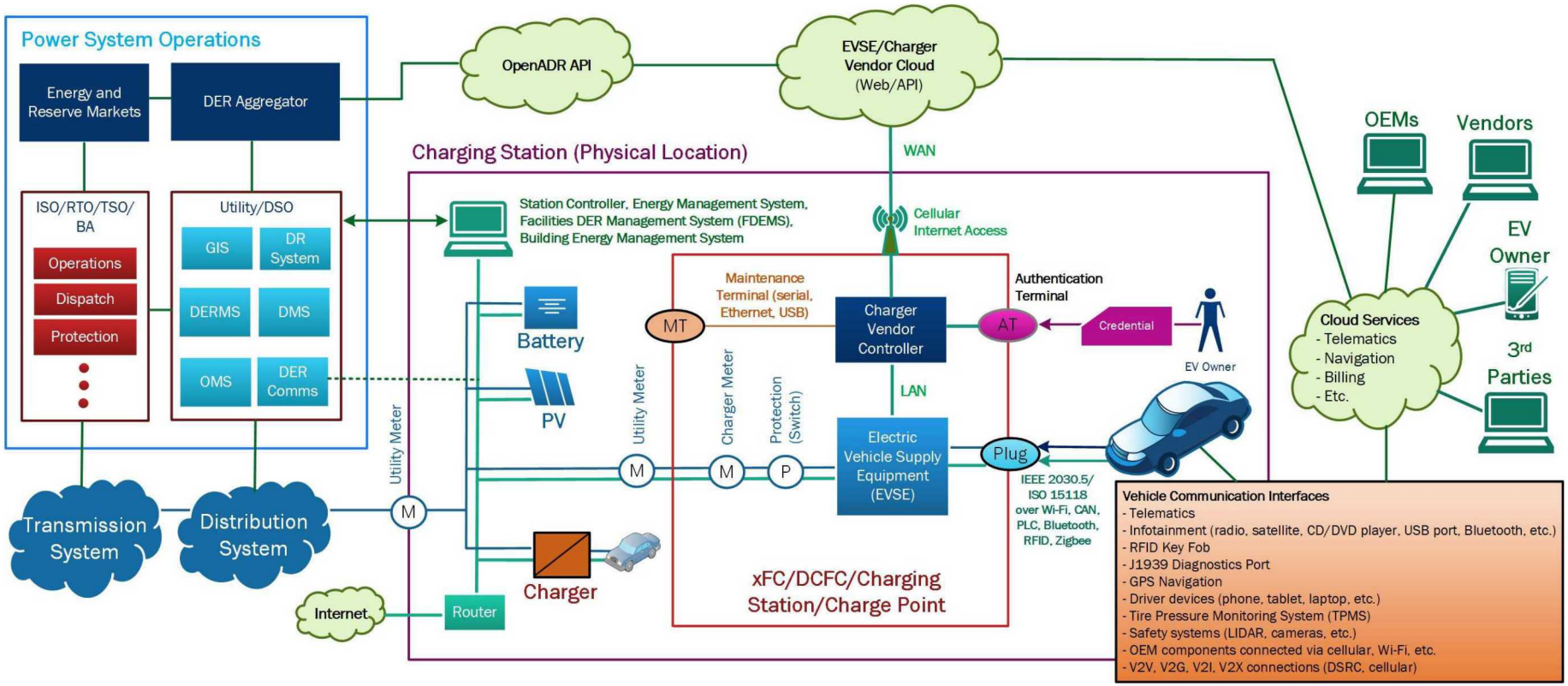
This will support:

- Development of standardized policies and best practices for managing EVSEs and other assets
- Inform the design and development of defensive systems, response mechanisms, and contingency plans

National Lab Team: SNL, PNNL, ANL

Partners: DOT, NMFTA, DHS, Navy, Army, DOE FEMP, DOE CESER

EV Charging Components and Information Flows



STRIDE Threat Model of EV Charging

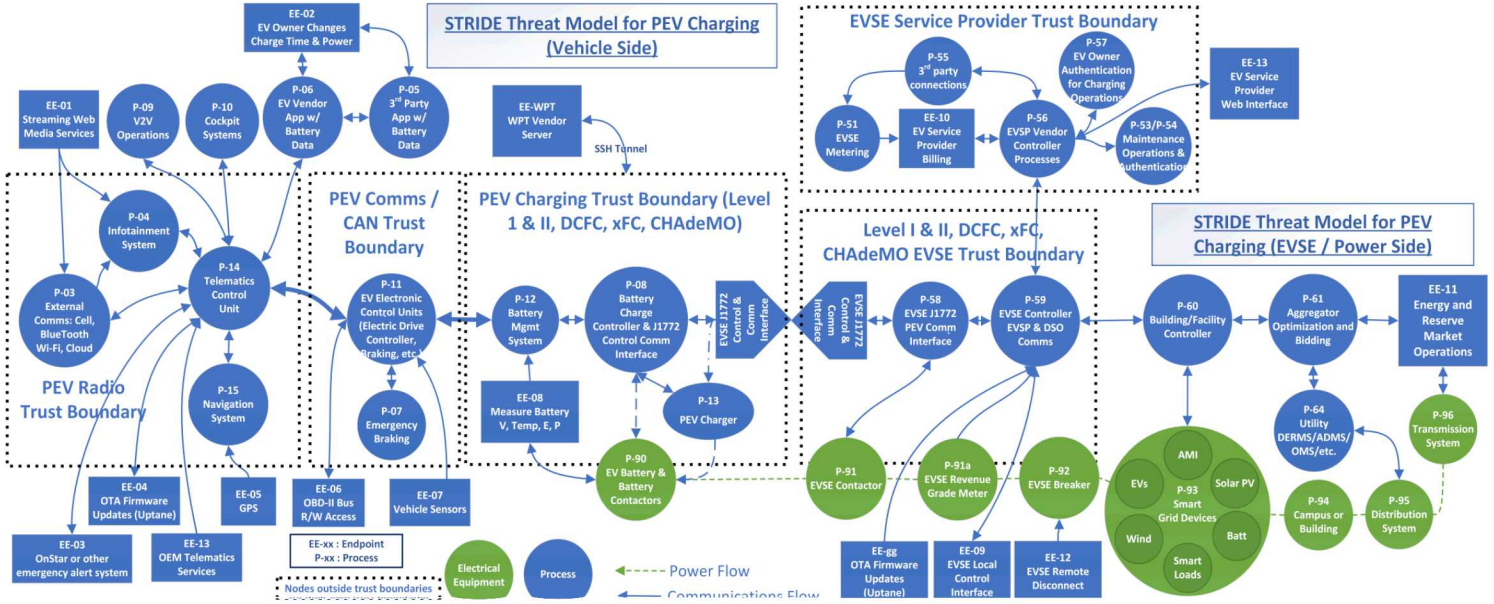
STRIDE Threat Modelling (by Microsoft)

- 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 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



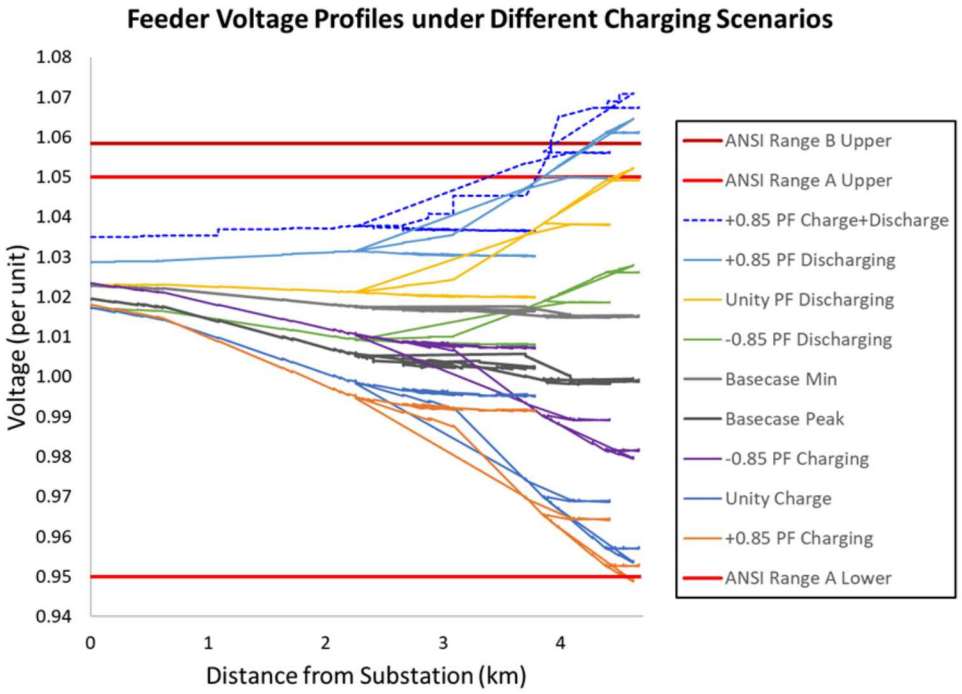
Threat model includes:

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

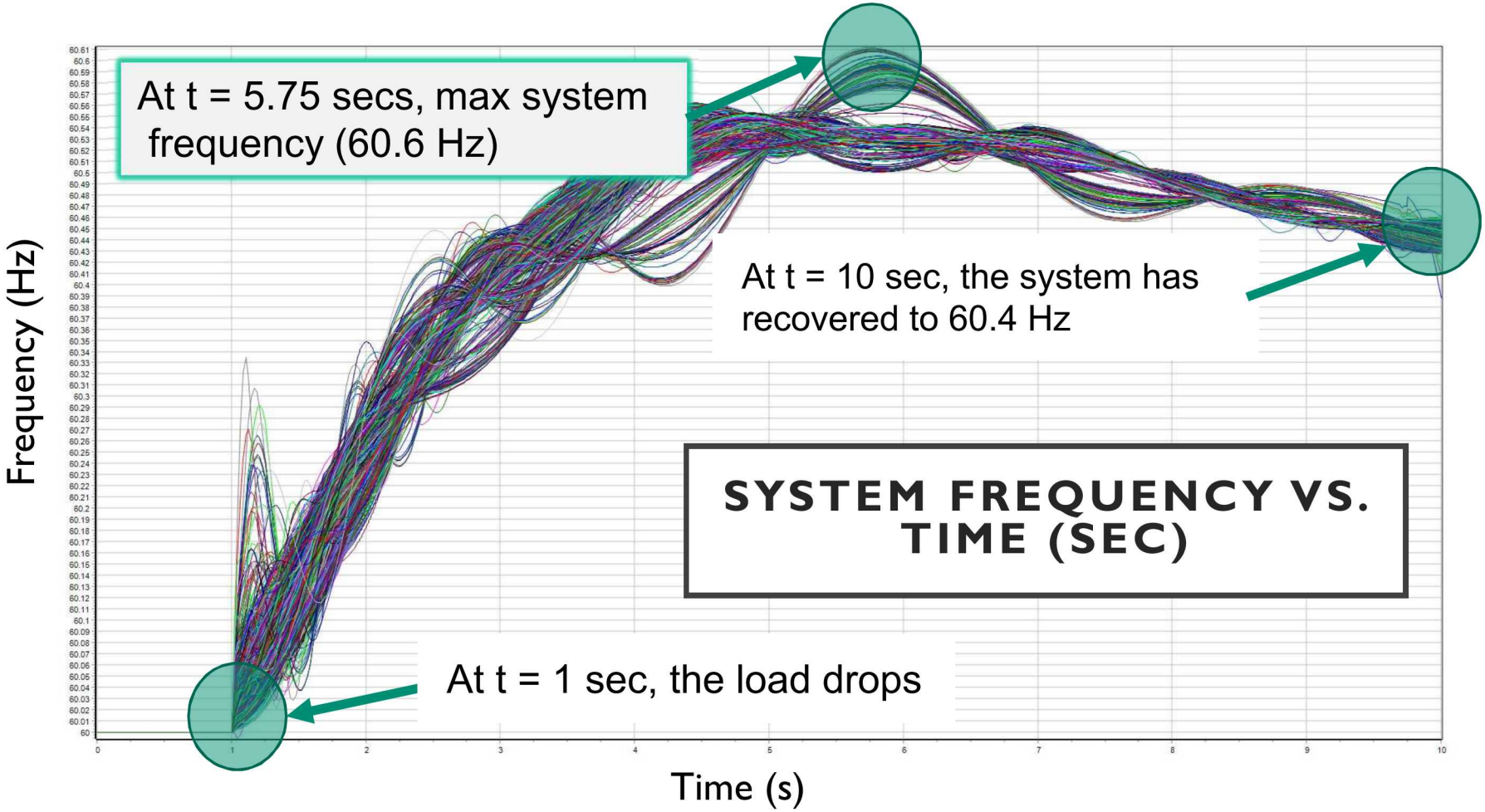
Distribution System Impact Analysis

- 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 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

Red Teaming is…

Authorized

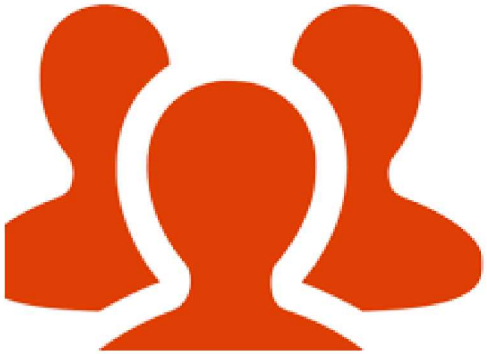
Assessments performed with permission of the system owner

Adversary-Based

Account for attackers' motivations and goals, knowledge and skills, tools and means

Defensive

We seek to improve the security posture of the system, network, or organization



Answers the question:
Secure from whom and with what motivation, goals, knowledge, skills, means, and tools?

Overview: When to Choose the Red-Teaming Approach

Red team is useful when:

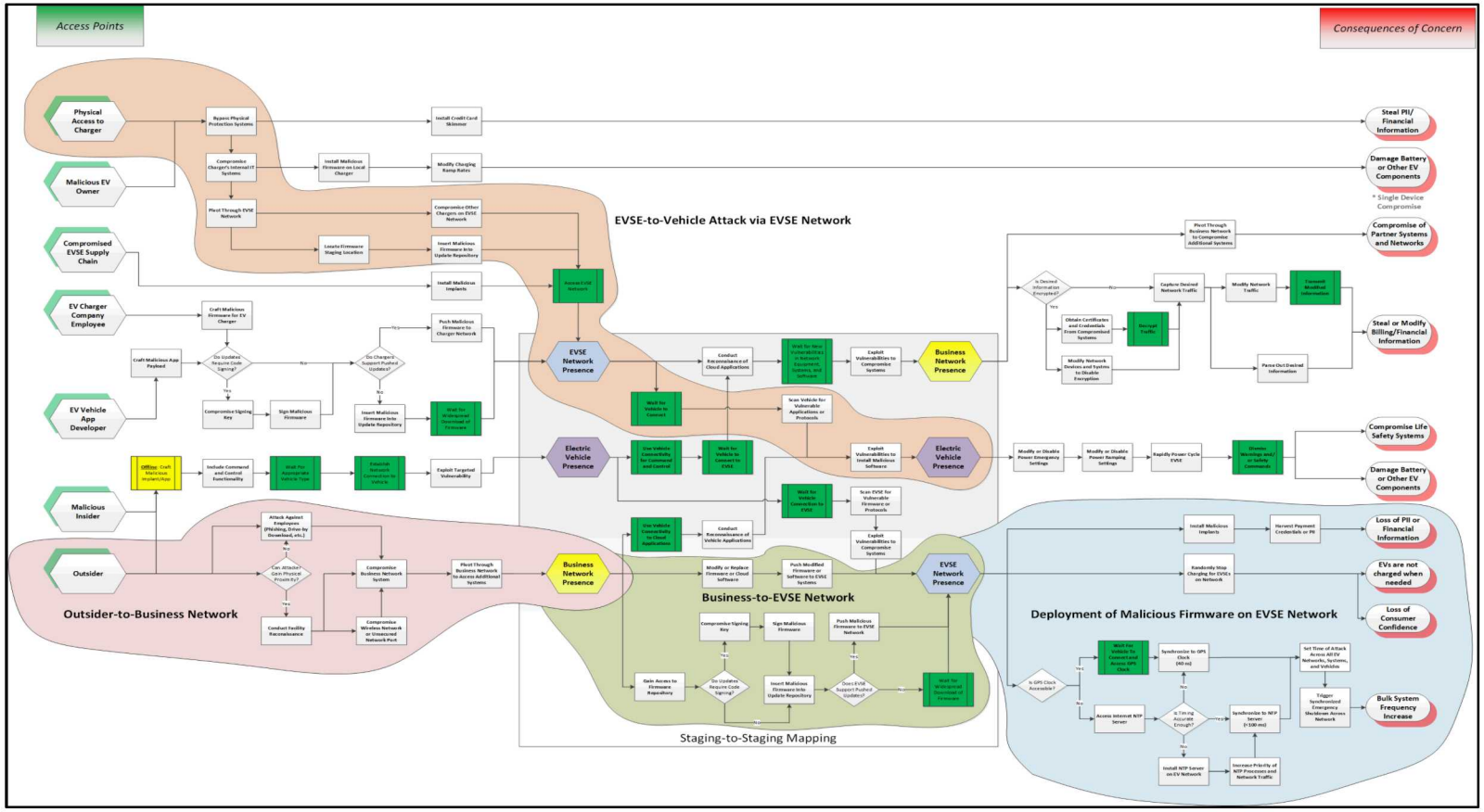
- Complex systems or systems of systems
- Developer focus is on function rather than security
- System is deployed in a hostile environment
- System is attractive to dynamic, adaptable adversaries
- Security choices must be made
- New use or new application of an existing system that may have unknown consequences
- System history shows previously discovered vulnerabilities
- A qualitative measure of system security is desired
- Need to establish or evaluate training and doctrine

Pursue other options when:

- Operational environment is unknown—the system is not well-defined or there are too many unanswered questions
- Existing, known security problems must be addressed first
- There is a greater risk of consequence from other sources
- Red-team function can be implemented by static model, test bench or tool
- Compliance testing or certification is sufficient
- Not prepared for an extreme answer

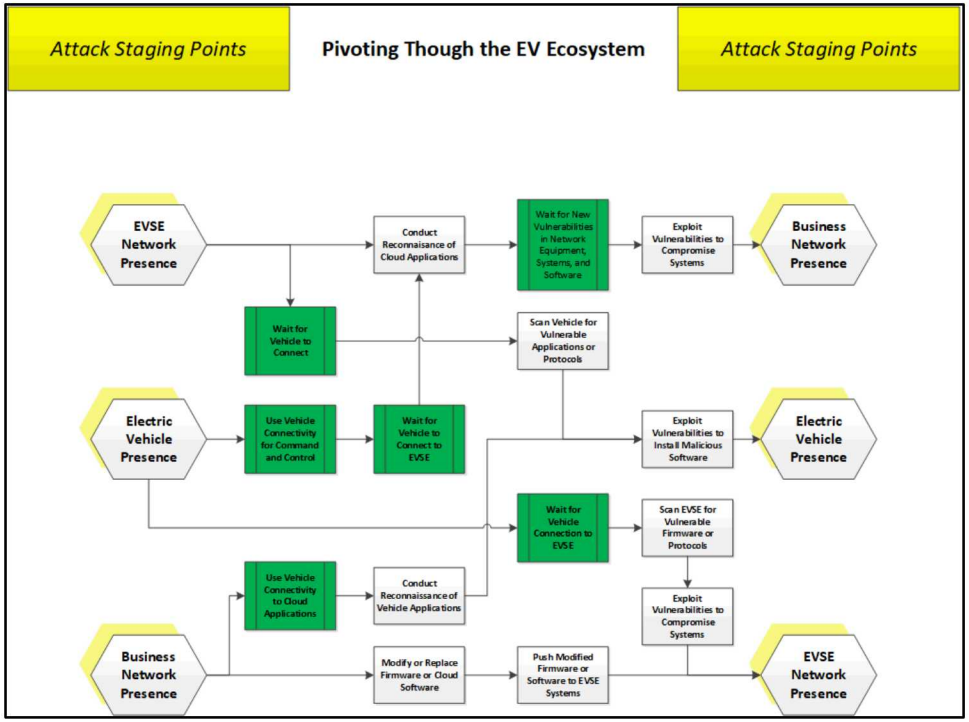
EV Charging Attack Graphs

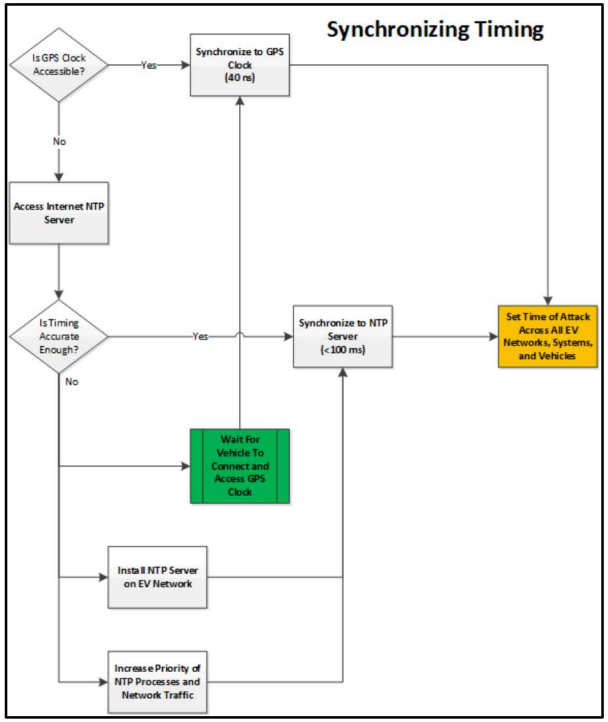
- Attack graphs show attacker actions to achieve an objective
  - Illustrates access points, staging areas, and consequences of concern
  - Graphically illustrates the steps an attacker must take to move from system/network access to the consequences of concern
  - Complex steps are displayed as images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



EV Charging Attack Graphs

- 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?



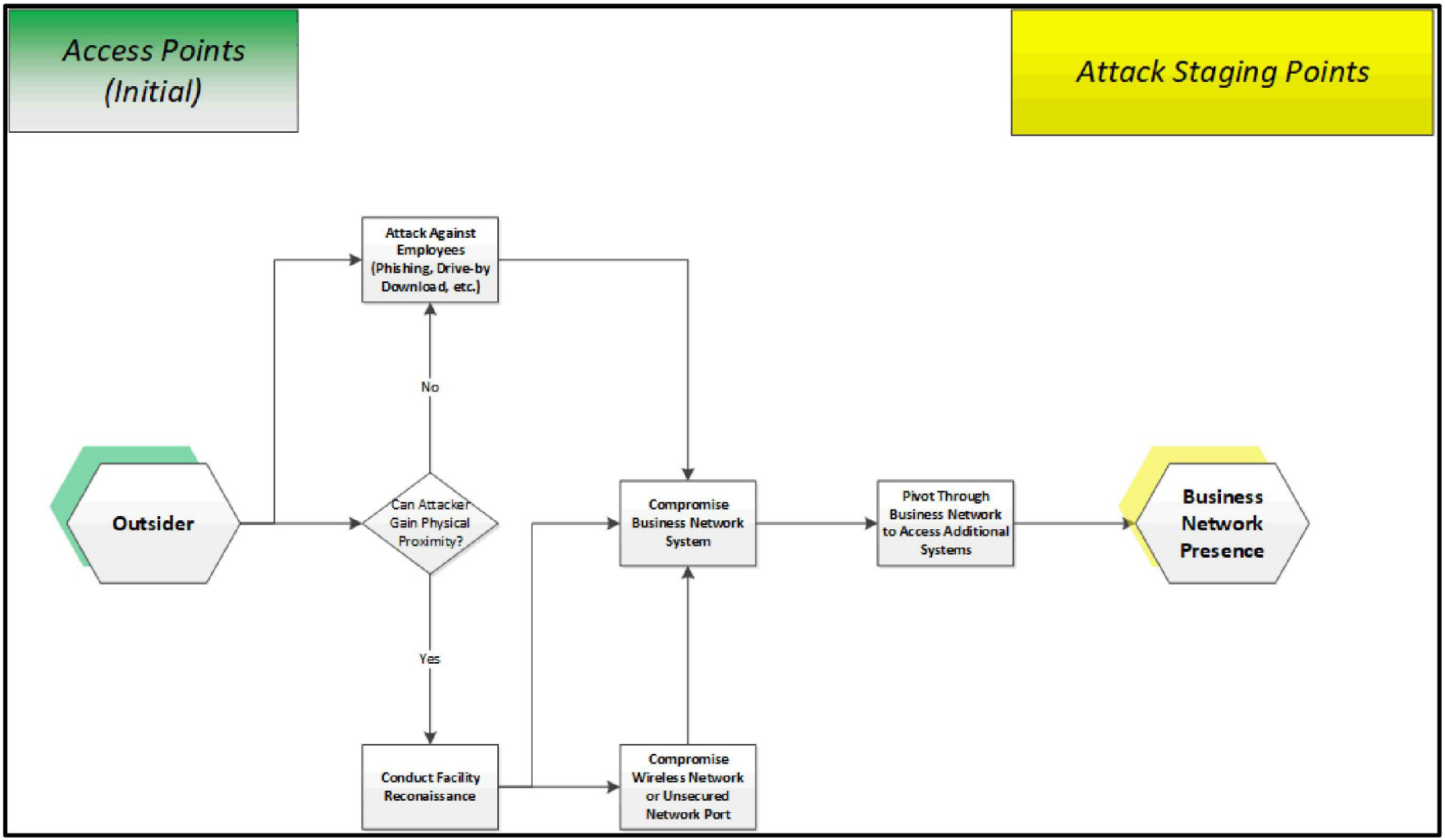


EV Charging Attack Graphs

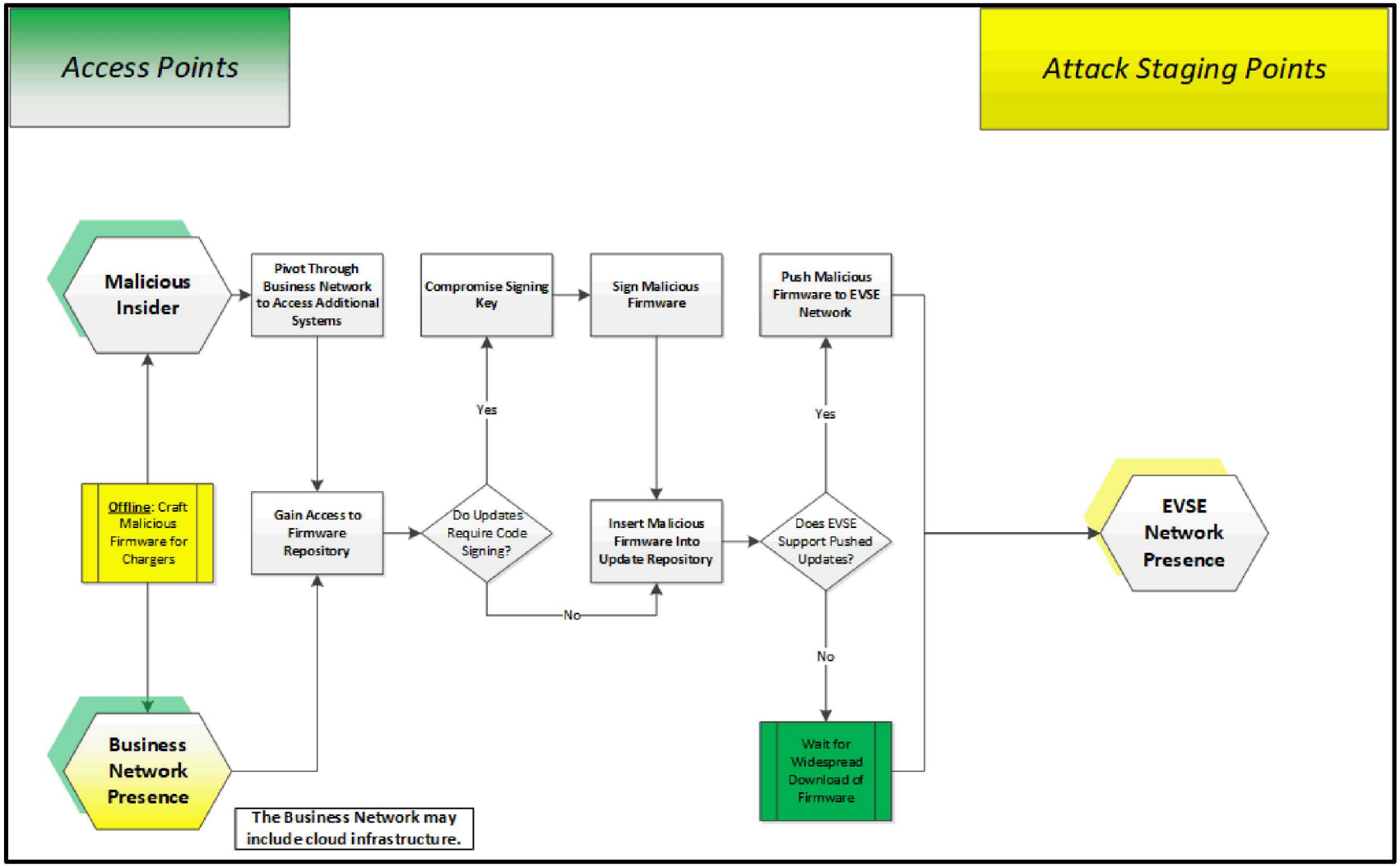
The team created attack graphs for the following use cases:

1. **Outsider to Business Network Presence**
   - Access Point: Attacker does not have authorized physical access to facility, network, or computing infrastructure.
   - Staging Point: Attacker gains presence in the EVSE Manufacturer's business network to use for follow-on activity.
2. **Deployment of Malicious Firmware**
   - Access Point: (A) Insider with physical access to the facility and has credentials to access the business network or (B) attacker gained a business network presence.
   - Consequences of Concern: (A) Bulk system frequency increase, (B) EVs not charged when needed, (C) loss of consumer confidence.
3. **Physical Compromise of EVSE**
   - Access Point: Attacker has physical access to EVSE
   - Consequences of Concern: (A) Loss of PII or financial information, (B) Compromise of partner systems and networks.
   - Staging Point: Attacker gains presence in EVSE Network
4. **EVSE to Vehicle**
   - Access Point: Attacker has malicious implant in EVSE.
   - Consequences of Concern: Compromise Vehicle Information System leading to consequences in Attack Graph 3
   - Staging Point: Attacker gains presence in Electric Vehicle

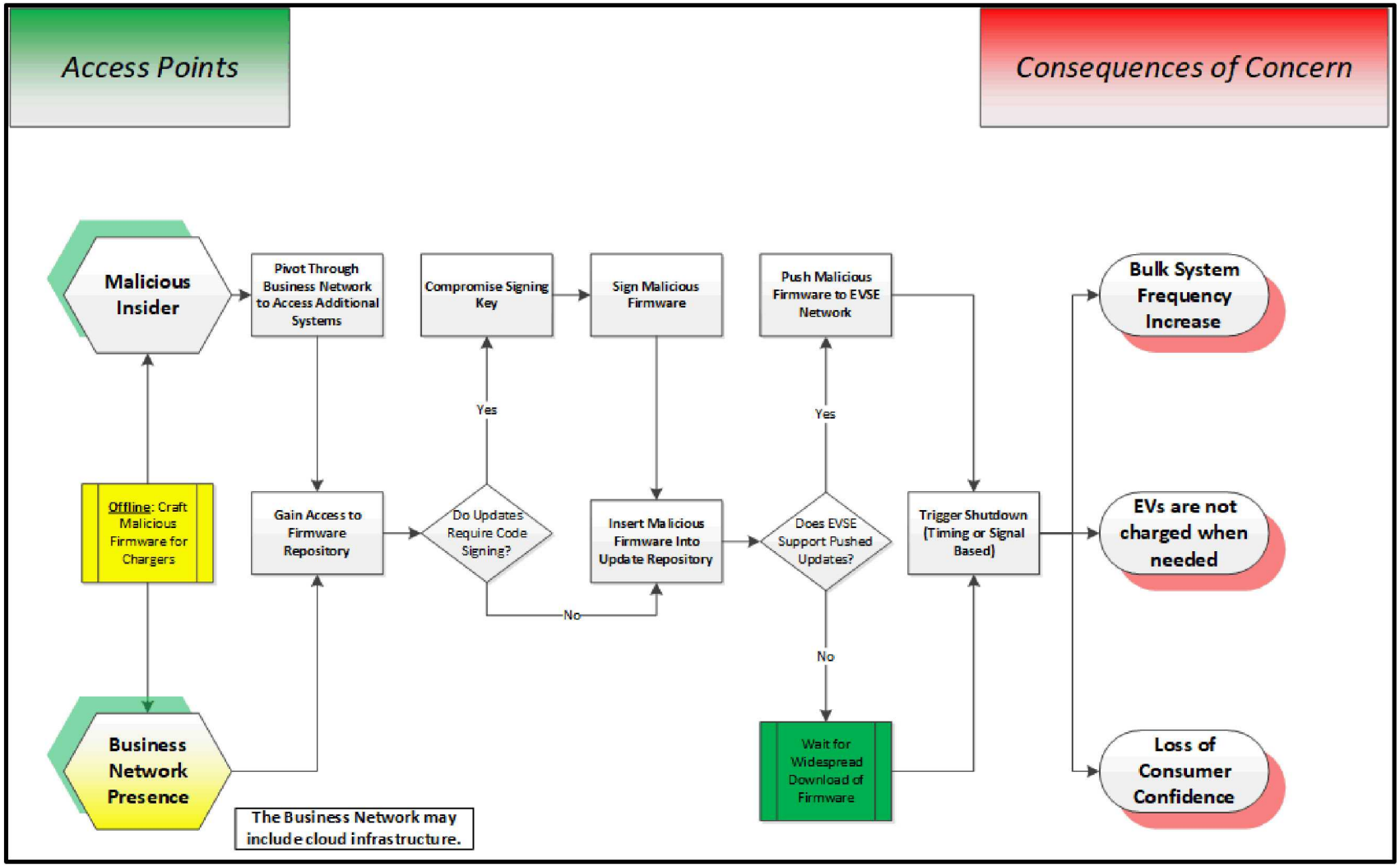
Outsider to Business Network Presence



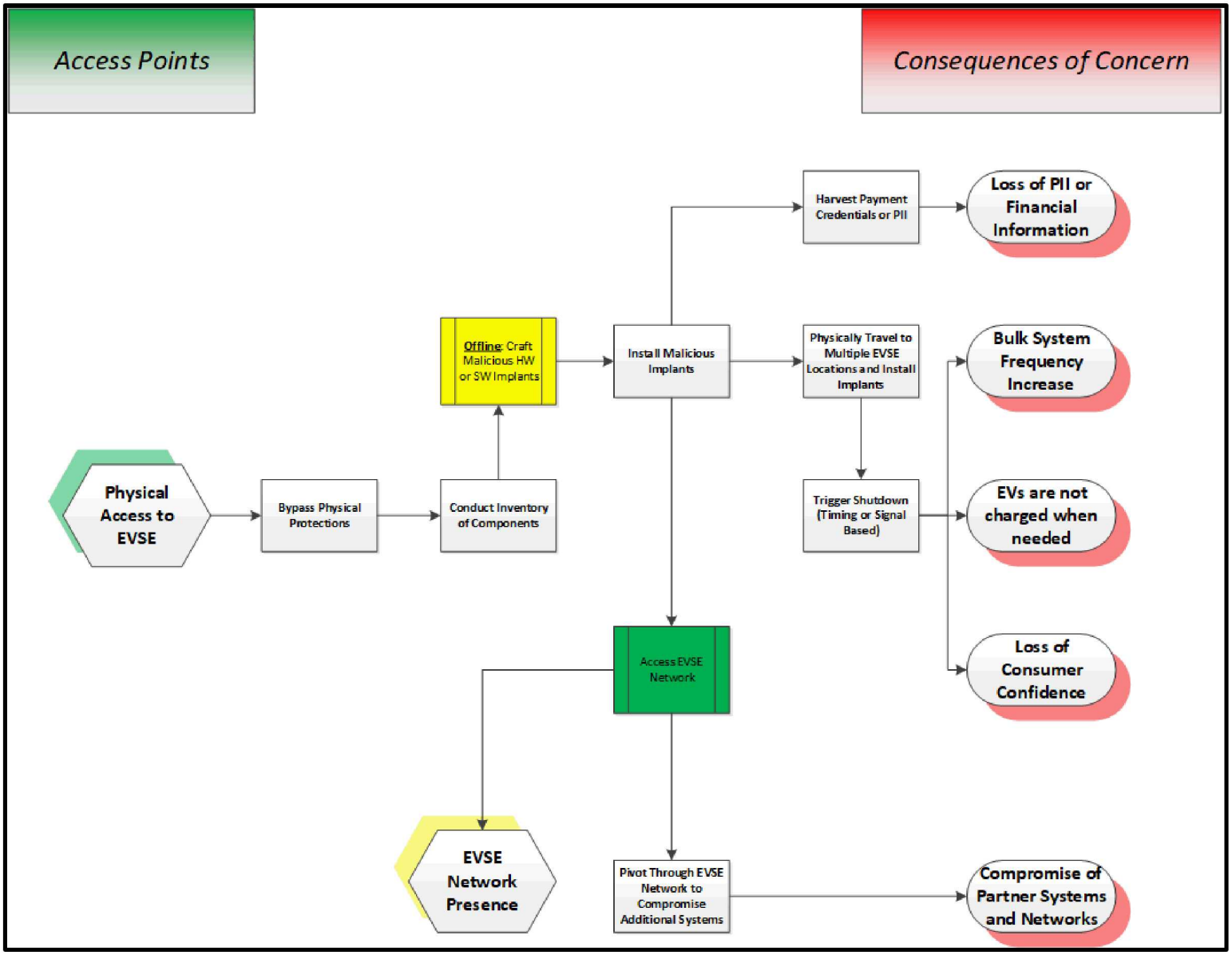
Pivoting From Business Network to EVSE Network



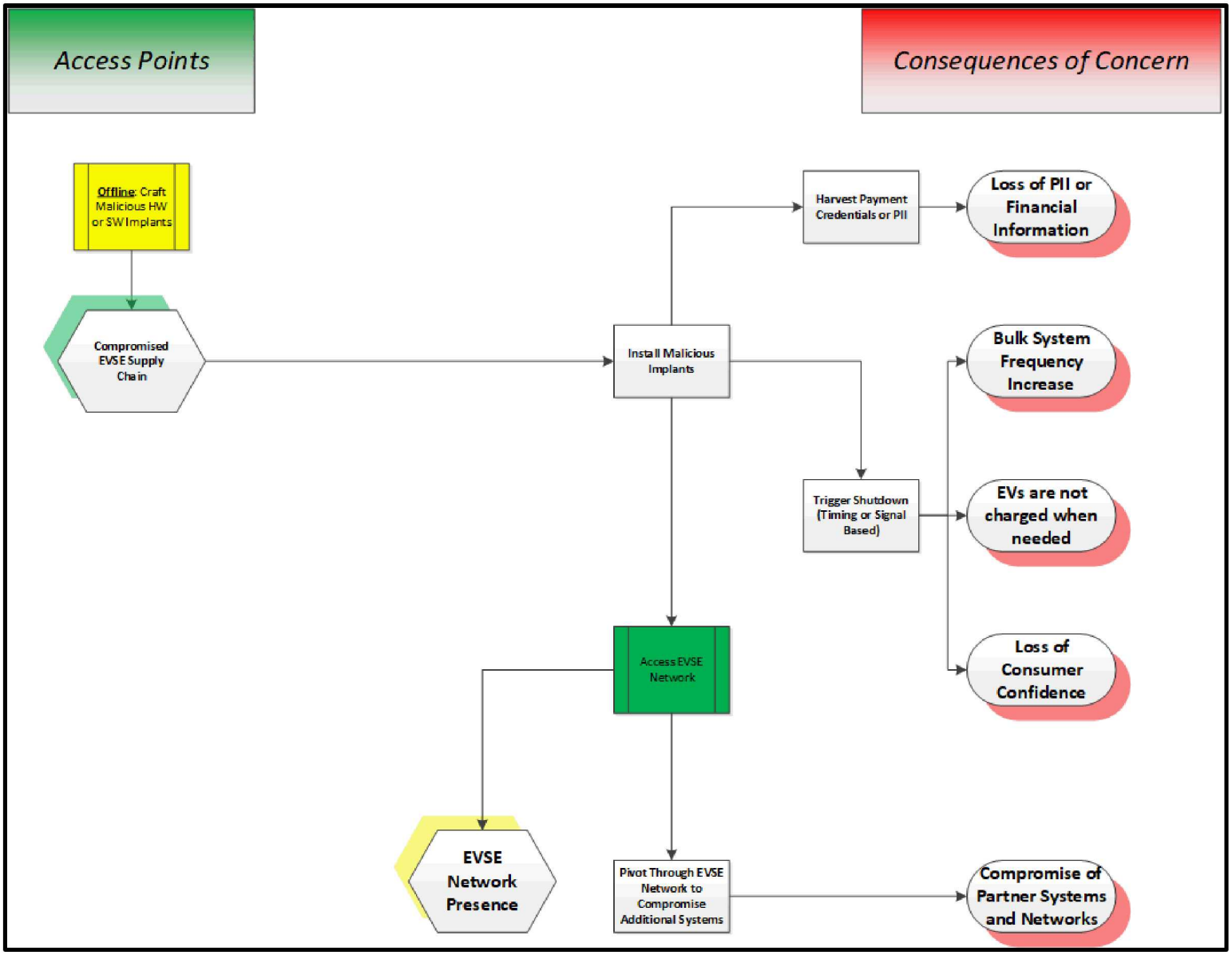
Deployment of Malicious Firmware



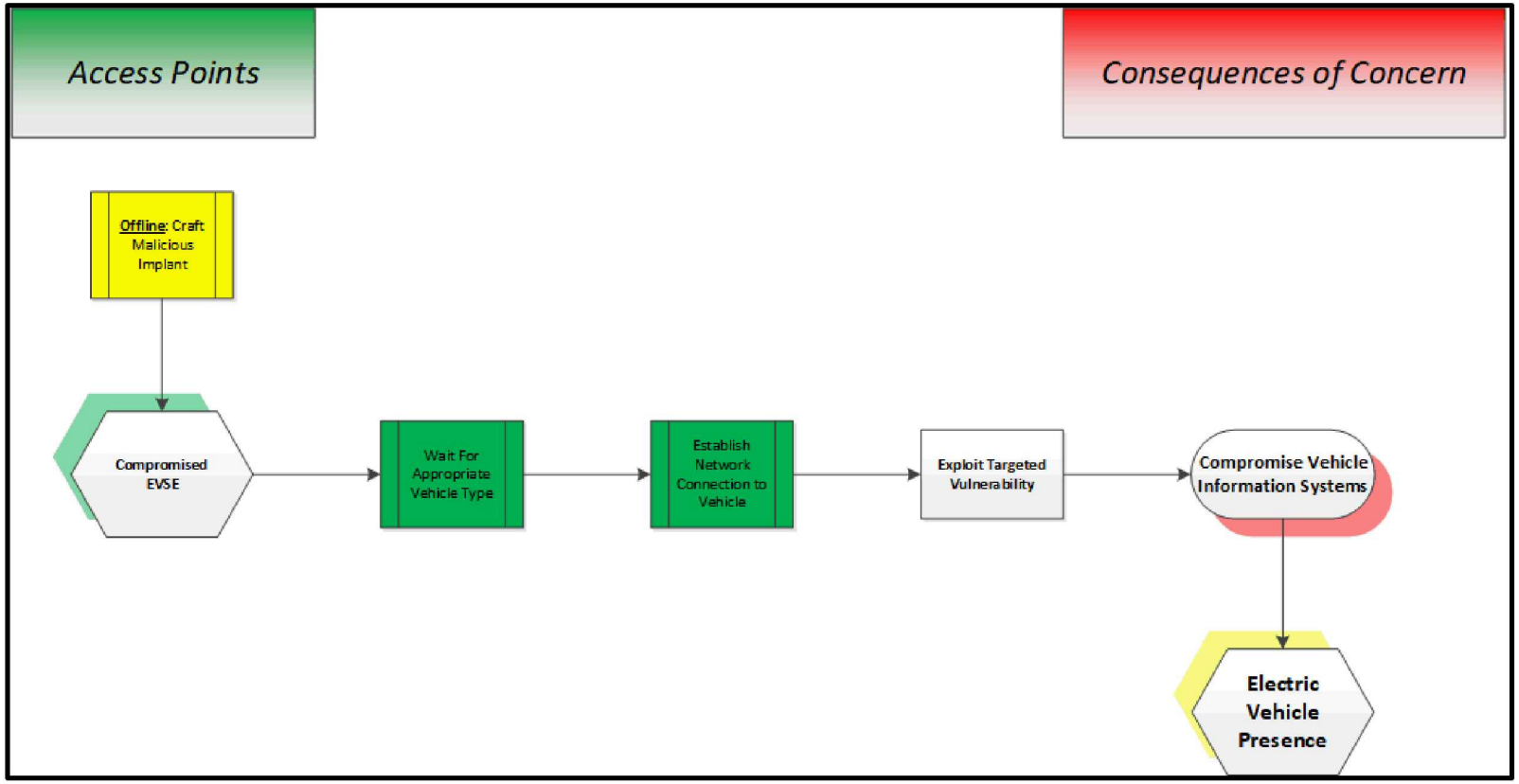
Physical Compromise of EVSE



Compromise of EVSE Supply Chain



EVSE to Vehicle



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

Questions?

If you want to request more information, want to partner with us, or just have general questions, please email us:

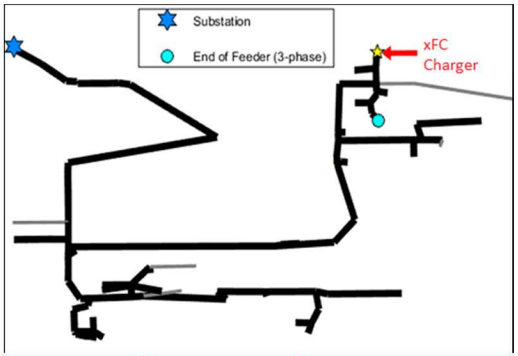
- Ben Anderson: brander@sandia.gov
- Jay Johnson: jjohns2@sandia.gov

Additional Reference Slides

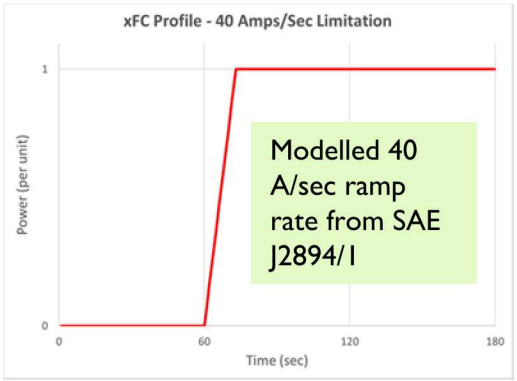
Distribution system impact analysis

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).

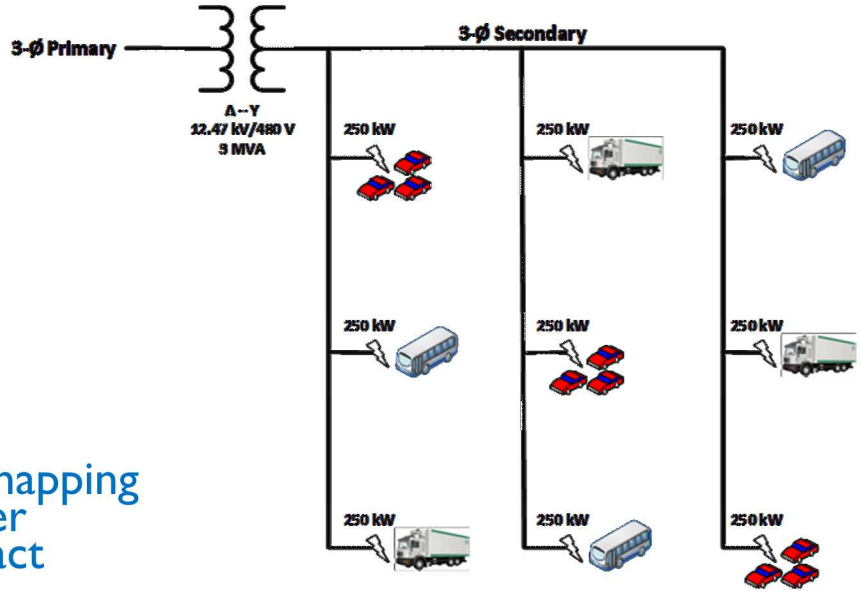


Load Period	Date/Time	Feeder Demand (kW)
Peak	7/22 @ 13:00	3946
Minimum	3/22 @ 23:00	1483



xFC Interconnection Model

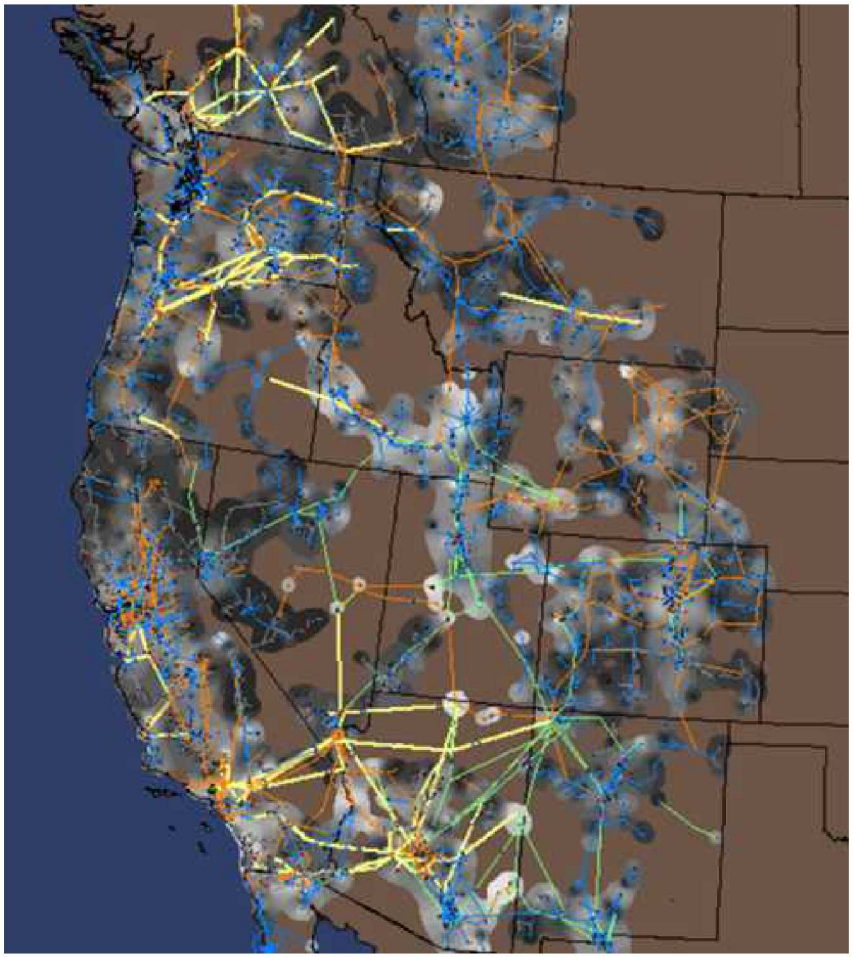
- 9x250 kW, 3-phase, 480 V stations simulated at the end of the feeder (2.25 MW total)
- Scenarios include charging sequences with and without V2G capabilities to generate high and low feeder voltages during peak and min load periods.
- Limited to ramp rate of 40 amp/sec, i.e. chargers get to full output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



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

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