Consequence-Driven Cybersecurity for High-Power Charging Infrastructure

PI: Barney Carlson
Idaho National Laboratory

June 13, 2017

DOE Vehicle Technologies Program Annual Merit Review
INL/MIS-19-53414

Project ID: ELT199

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

Overview

Timeline

- Start Date: Oct. 2018
- End Date: Sept. 2021
- 25% complete
  (on schedule)

Barriers

- Risks due to cybersecurity vulnerabilities of EV charging infrastructure increasing with:
  - Higher charge power
  - Increased system complexity
    - Multiple communication protocols
    - Advanced control systems for operational performance, energy management, autonomous operation, and public safety

Budget

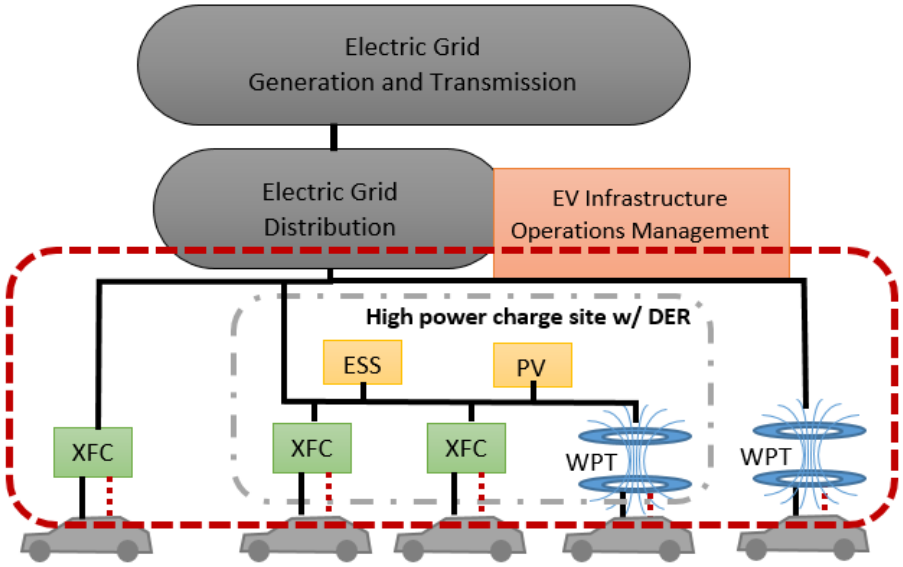
- Total project funding
  - FY19
    - Total: $1,020k
      - INL: $430k

Partners

- Project lead
  - Idaho National Lab (INL)
- National lab collaboration
  - National Renewable Energy Lab (NREL)
  - Oak Ridge National Lab (ORNL)
- Industry collaboration
  - ABB
  - Tritium
  - Electrify America

Relevance

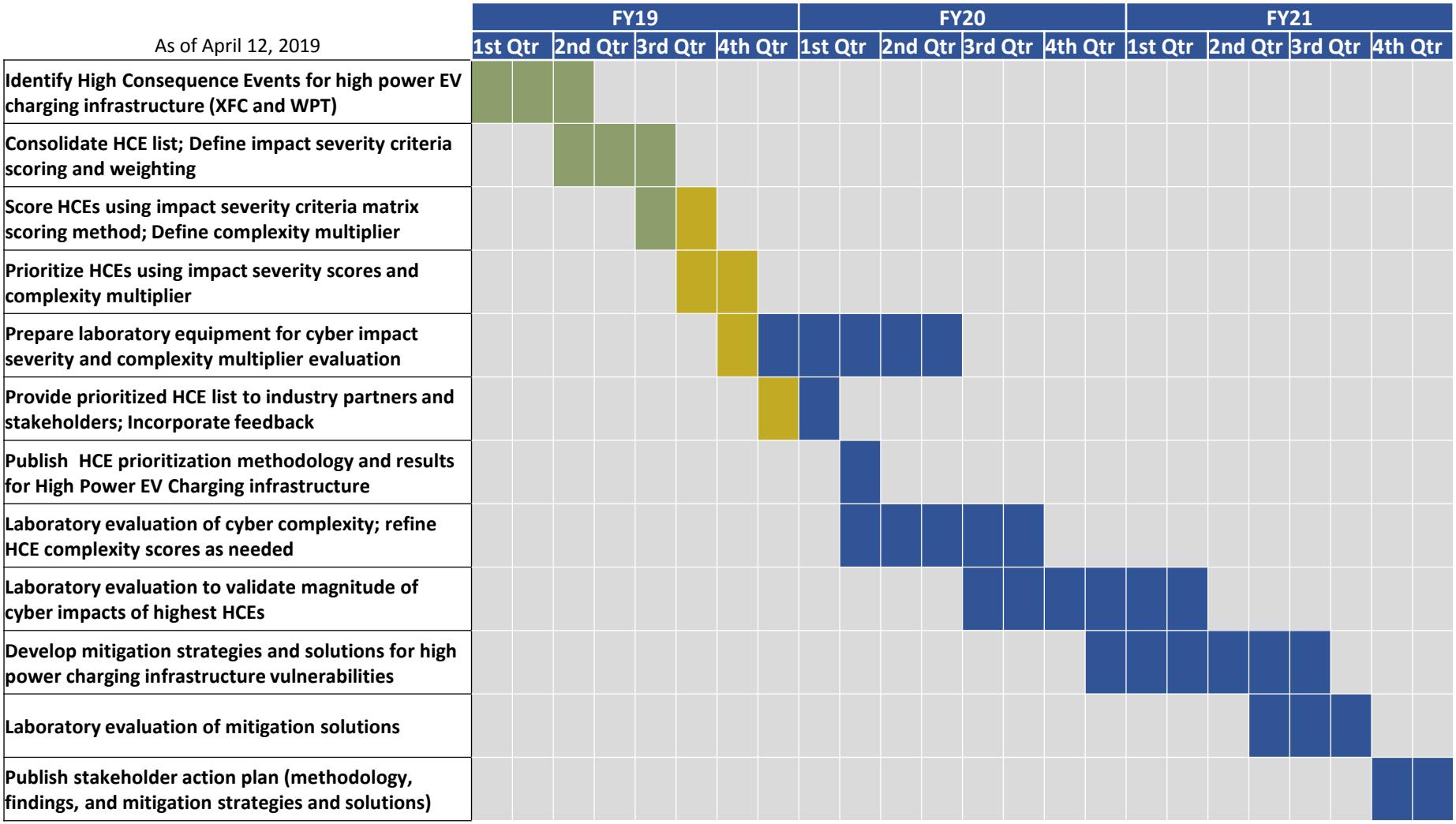
- Reduce risks associated with potential vulnerabilities for high power EV charging infrastructure leading to high consequence events (HCE)
  - Public Safety
  - Impact to the electric grid
  - Hardware damage
  - Denial of service
  - Data theft or alteration
- With enough time & effort, nearly any connected system can be accessed or compromised



Objective

- Determine high consequence events (HCE)
- Prioritize HCEs to guide future research efforts
  - Based on impact severity & cyber manipulation complexity
- Develop mitigation strategies and solutions
- Feedback solutions, information, and lessons learned to industry

Milestones / Timing



Any proposed future work is subject to change based on funding levels

Approach

- Conceptualize high consequence events (HCE)

- Prioritize HCEs
  - Based upon **Impact Severity** & cyber manipulation **Complexity Multiplier**

- Laboratory evaluation of HCEs:
  - Impact severity
  - Cyber manipulation complexity

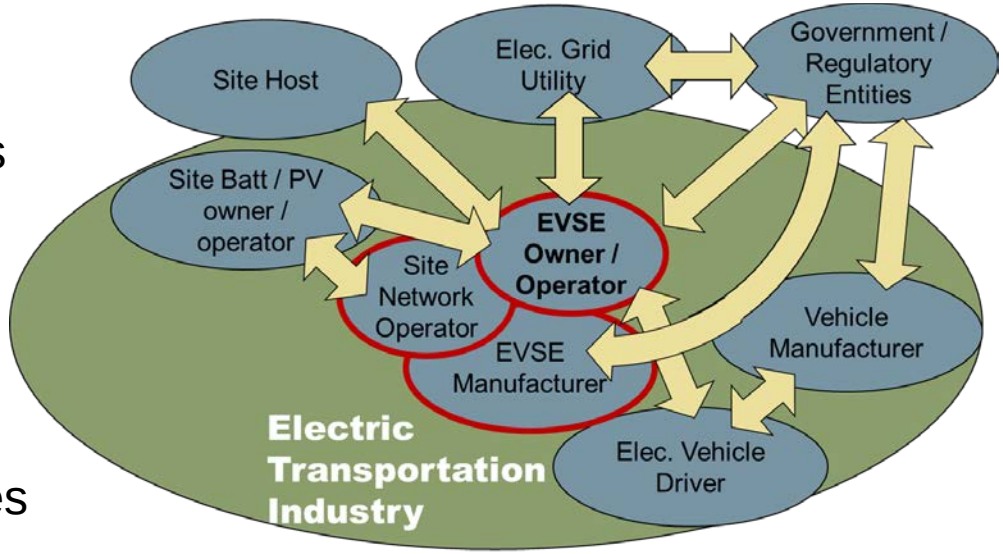
- For the highest prioritized HCEs
  - Recommend methods to harden attack surfaces
  - Develop mitigation strategies and solutions
  - Recommendations for safe resilient operation during cyber event
    - Cyber informed engineering practices
  - Recommend methodology(s) to safeguard personal information & data
  - Means to identify cyber malicious event

- Publish stakeholder action plan

Approach

- Categories of HCEs for high power charge sites (XFC and WPT)
  - Impact to the electric grid
  - Safety
  - Hardware damage (charger, vehicle, etc.)
  - Loss of service
  - Data theft or alteration

- Stake holders:
  - Charge Site Owners / Operators
  - Charge Network Operator
  - EVSE Manufacturers
  - Electrical Utilities
  - EV Drivers
  - EV Manufacturers (OEMs)
  - Government / Regulatory Entities
  - Site host
  - Electric Transportation Industry



Accomplishments: Recommended Approach to Cyber Security

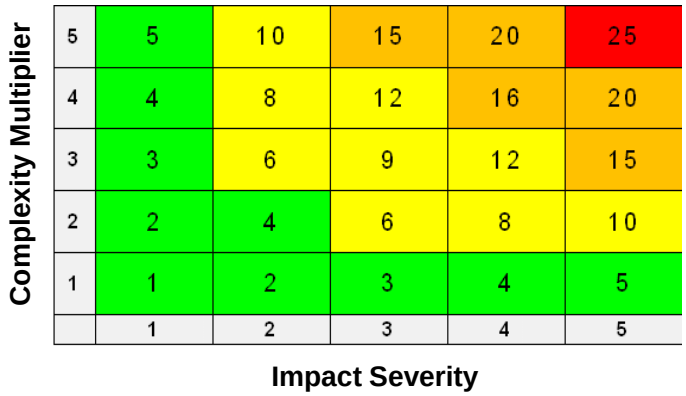
- **Prepare**
  - Identify potential system vulnerabilities
  - Harden attack surfaces of vulnerabilities
  - Develop a methodology to safeguard personal information & data
  - Develop response plan & mitigation strategies and solutions
  - Design system for safe resilient operation during cyber event
- **Attack Response**
  - Identification of cyber malicious event
  - Execute response plan
  - Communication to stake holders
  - Data collection for forensics
- **Clean-up and Close-out**
  - Forensics analysis
  - Clean-up efforts to get system back to full operation
    - Ensure attack vector has been completely closed and event has ended (not merely dormant)
  - Share lessons learned w/ others in industry

Accomplishments: HCE Ranking Prioritization

HCE Score = Impact x Complexity

- Impact Severity score
  - Severity based on 8 criteria
  - Weighting factor used for the 8 criteria
- Complexity Multiplier score
  (ease of cyber-manipulation)
  - Validate complexity score with laboratory vulnerability assessments

HCE Scoring

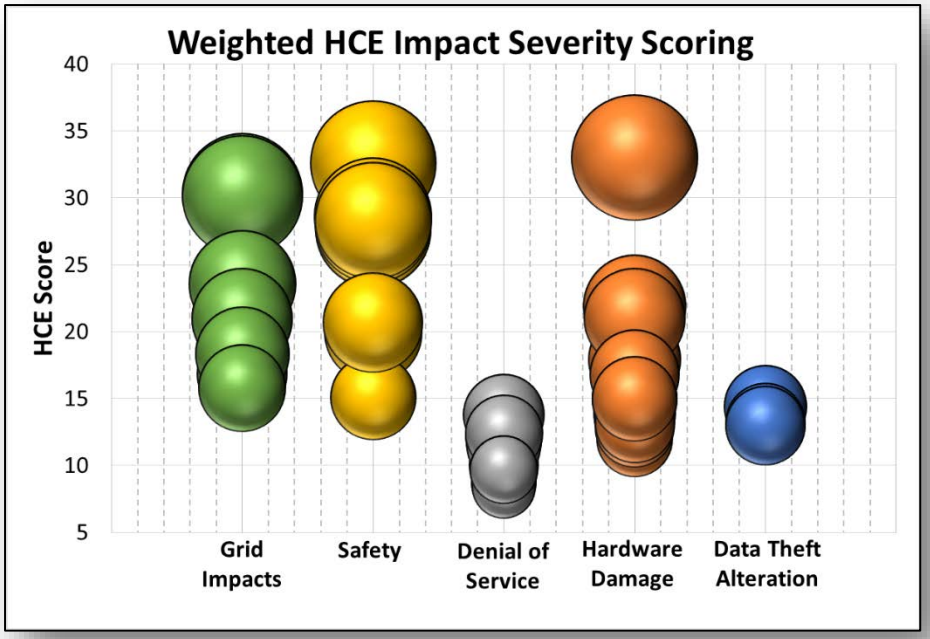


Impact Severity Scoring

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

Accomplishments: Preliminary HCE Impact Severity Scoring

- Highest scored events:
  - Hardware damage:
    - Battery fire due to overcharge (site ESS or EV battery)
  - Safety:
    - Shock or burn hazard from damaged cord set due to thermal manipulation (XFC)
    - Exposure of high EM-field to public (w/ implanted medical devices) (WPT)
  - Grid Impacts:
    - Power outage impacting multiple feeders due to sudden load shed or change in load from multiple XFC concurrently or multiple stationary ESS at charge sites



Accomplishments: In-depth analysis of highest scored HCE

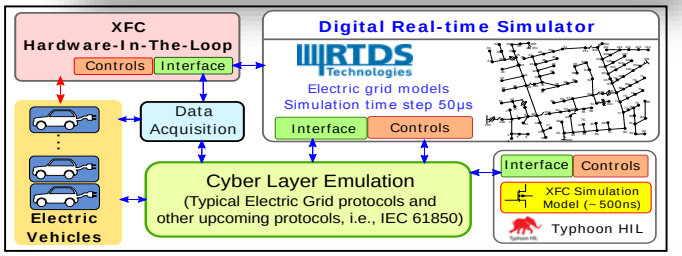
- XFC thermal system manipulation
  - Thermal sensors spoofed causing no cooling of cable and connector (insulation failure)
  - Unique vulnerability to XFC
- Event:
  - XFC cable failure / melting
- Impact:
  - Public safety & hardware damage
    - Burn hazard
    - Shock hazard
      - depending upon state of insulation
    - Cable replacement required
- Mitigation solution:
  - Minimum coolant flow rate
  - Redundancy:
    - Flow rate based on current & thermal sensors used to trim flow rate

Future Research: Validation & Mitigation Strategies

Assess the *highest* prioritized HCEs:

- Validation of cyber manipulation complexity:
  - Laboratory hardware evaluation
  - Power hardware-in-the-loop research

- Evaluation of impact severity:
  - Potential impact to the grid
    - Using power hardware-in-the-loop capabilities
  - Charge system hardware manipulation in laboratory
    - Electrical operation
    - Thermal systems
    - Communications and controls



- Develop strategies and solutions for prioritized HCEs
  - Develop mitigation strategies and solutions
  - Solutions to hardened attack surfaces of vulnerabilities
  - Methodology to safeguard personal information & data
  - Method to identify occurrence of cyber malicious event

Any proposed future work is subject to change based on funding levels

Future Research: Stakeholder Action Plan

- Recommendations for high power EV charging infrastructure stakeholders
  - Prioritized list of HCEs
    - Based on weighted impact severity and complexity multiplier
    - Results from laboratory evaluation
      - Evaluation of impact severity
      - Validation of cyber manipulation complexity
  - Recommendations and Lessons Learned
    - Methods to harden attack surfaces of vulnerabilities
    - Develop mitigation strategies and solutions
    - Recommendations for safe resilient operation during cyber event
    - Recommend methodology(s) to safeguard personal information & data
    - Means to identify cyber malicious event

Any proposed future work is subject to change based on funding levels

Response to Previous Year Reviewer Comments

- New project starting FY19

Collaboration

- Team collaboration includes:
  - National labs
    - INL, NREL, ORNL
  - Charger equipment manufacturers
    - Tritium, ABB
  - Charge Site owner / operator
    - Electrify America

- Additional EV charging infrastructure cybersecurity collaboration:
  - VOLPE / NMFTA: cybersecurity guidelines for MD/HD truck high power charging infrastructure
  - WAVE Inc.: MD/HD wireless charging at 250+ kW
  - Utah State Univ.: wireless charging control strategies strategy development for static and dynamic WPT

Summary:

- Prioritize high power EV charging infrastructure high consequence events
  - Guides future research direction and efforts

- Recommended cybersecurity approach methodology
  - Harden attack surfaces
  - Safeguard personal information & data
  - Methods to identify cyber malicious event
    - Assumption: all connected systems can be compromised
  - Mitigation strategies and solution
  - Safe resilient operation during cyber event
    - Cyber informed engineering practices
  - Strategies and solutions to recover and clean-up from event