Consequence-Driven Cybersecurity for High-Power EV Charging Infrastructure

PI: Richard “Barney” Carlson
Idaho National Laboratory

June 24, 2021

DOE Vehicle Technologies Program Annual Merit Review
Project ID: ELT199

INL/MIS-21-62225

Idaho National Laboratory

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

Overview:

Timeline

- Start Date: Oct. 2018
- End Date: Sept. 2021
- ~85% complete
  (~2 months behind schedule)

Budget

- Total project funding
  - FY21
    - Total: $995k

Barriers

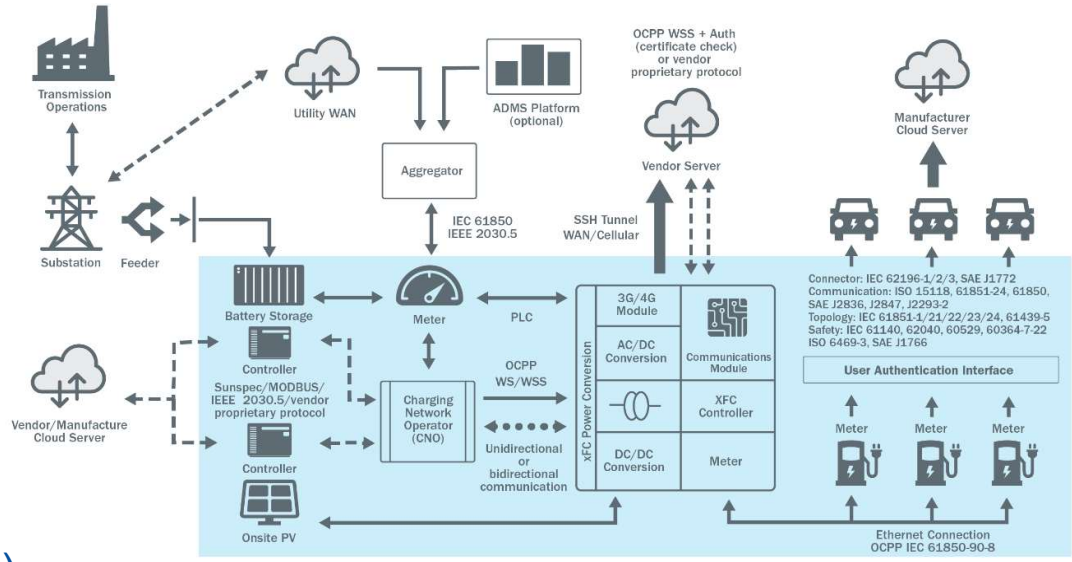
- Increased risks from exploit of cybersecurity vulnerabilities of EV charging infrastructure with:
  - Higher charge power
  - Increased system complexity
    - Multiple communication protocols
    - Advanced control systems for operational performance, energy management, autonomous operation, & public safety

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 and exploits for high power EV charging infrastructure leading to high consequence events (HCE)
  1. Safety
  2. Impact to the electric grid
  3. Hardware damage
  4. Denial of service
  5. Data theft or alteration
- With enough time & effort, nearly any electrically controlled system can be accessed or compromised

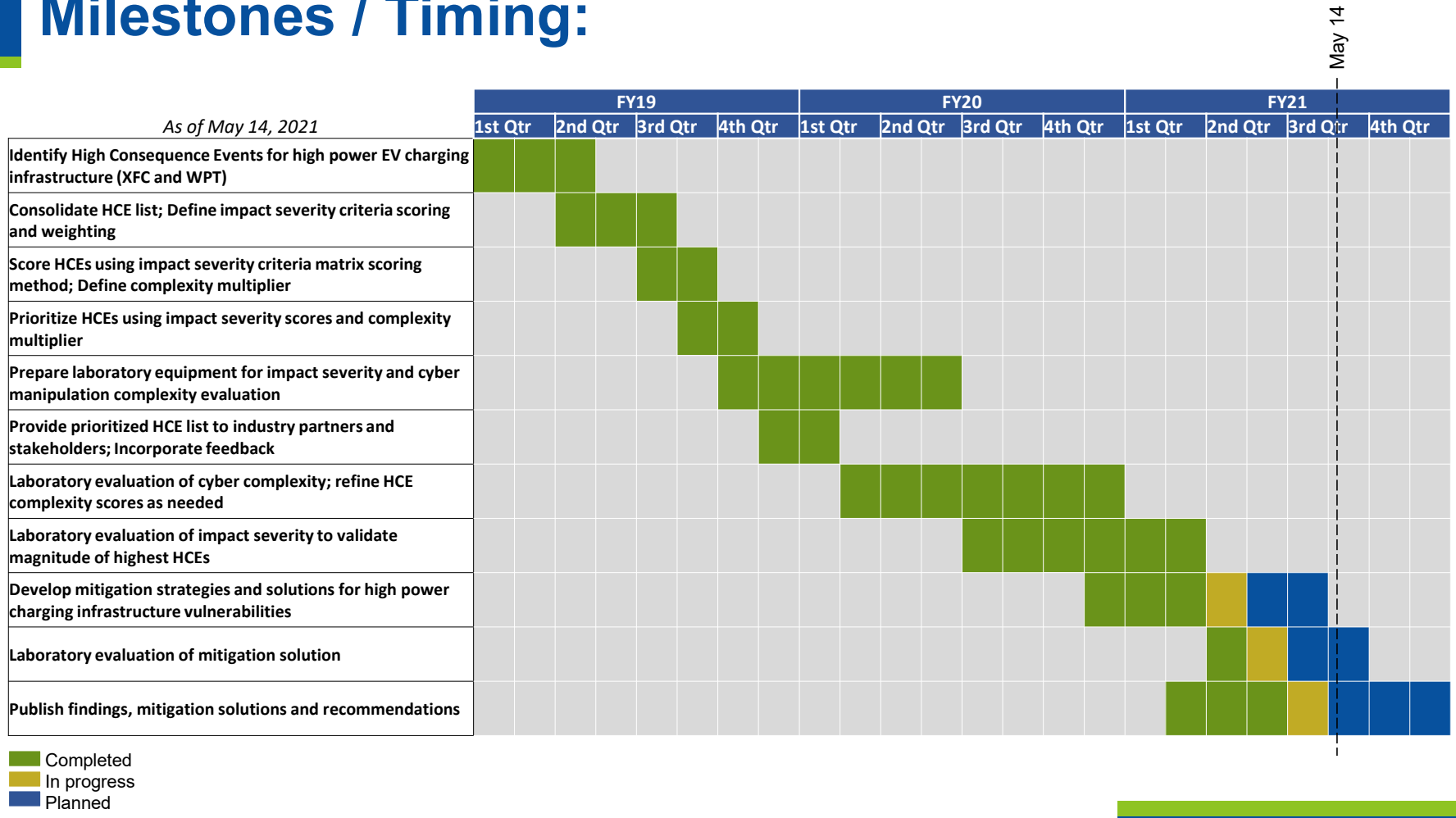


source: NREL

Objective:

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

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**
    - Scoring system is similar to DFMEA methodology
- ✓ Laboratory evaluation of HCEs:
    - Cybersecurity manipulation complexity
      - Cybersecurity assessment of hardware controls and communications
    - Impact severity
      - Laboratory testing and evaluation to quantify potential impacts
    - Refine HCE prioritization scoring based on laboratory evaluation

In Progress

- Develop mitigation solutions and strategies
  - Evaluate solutions in laboratory
- Publish results, findings, and mitigation solutions & strategies

Approach: HCE Ranking Prioritization

HCE Score = Impact **x** Complexity

- Impact Severity score
  - Severity based on 8 criteria
  - Weighting factor used for the 8 criteria
    - Additional weighting on safety criteria
- Complexity Multiplier score
  (ease of cyber-manipulation)
  - Validate complexity score with laboratory vulnerability assessments
- Scoring similar to DFMEA methodology

HCE Scoring

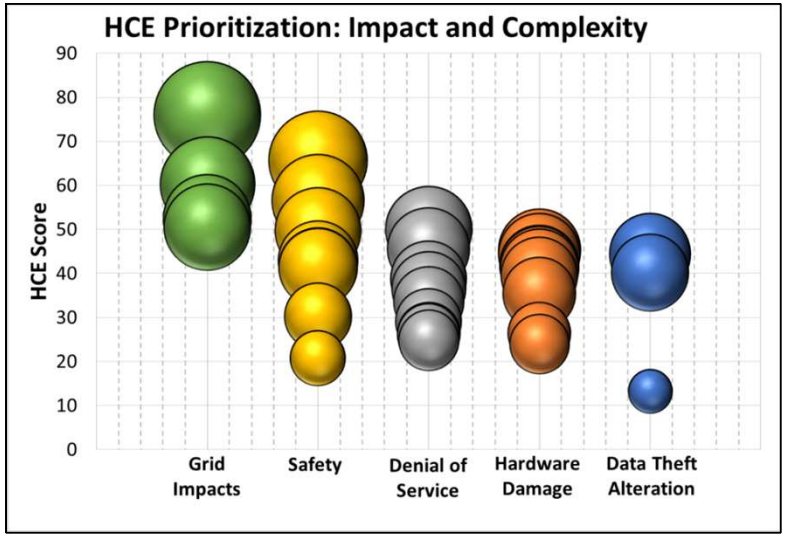
Complexity Multiplier	Impact Severity				
10	20	40	60	80	100
8	16	32	48	64	80
6	12	24	36	48	60
4	8	16	24	32	40
2	4	8	12	16	20
0	**2**	**4**	**6**	**8**	**10**

Impact Severity Scoring

Criteria	N/A (0)	Low (2)	Medium (6)	High (10)
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:
Top 15 HCE List (from list of 33 consolidated HCEs)

Rank	Category	Event
1	Grid Impact	Power Outage(s) due to sudden load shed from multiple XFCs.
2	Safety	Injury or loss of life due to electrocution, electrical shock, or burns from exposed conductors due to failed insulation of the XFC cable or connector.
3	Grid Impact	Power outage(s) due to sudden load shed or increase from on-site energy storage system manipulation.
4	Safety	(WPT Only) Medical device failure or injury caused by exposure of high electromagnetic field to implanted medical devices.
5	Hardware Damage	Damage to equipment within the feeder distribution area (transformers, switch gear, harmonics, overload capacitor bank, high reactive power).
6	Grid Impact	The XFC and Distributed Energy Resource (DER) at the site are not able to provide grid services (ex. curtailment) when needed causing decreased stability/reliability of the grid.
7	Denial of Service	System shutdown (XFC or charging site) due to creation of software error state.
8	Safety	Users are burned by hot CCS cord set without electrical insulation failure.
9	Denial of Service	System shutdown due to network outage (WiFi, cellular, or other communications outage).
10	Hardware Damage	Hardware damage to the charger over very long duration of elevated temperature.
11	Hardware Damage	(WPT Only) Induced voltage (high V/m) on vehicle components or electrical harnesses may damage harness or electrical components not associated with WPT system. Vehicle components that are not rated or shielded from high magnetic field levels may heat up.
12	Data Theft	Theft or alteration of Personally Identifiable Information (PII) data transmitted between vehicle, XFC, EV driver, network operator, etc.
13	Safety	Vehicle fire due to vehicle battery overcharge.
14	Hardware Damage	(WPT Only) Vehicle electrical component damage due to over-voltage condition of the vehicle side WPT components.
15	Hardware Damage	Hardware damage to the XFC(s).

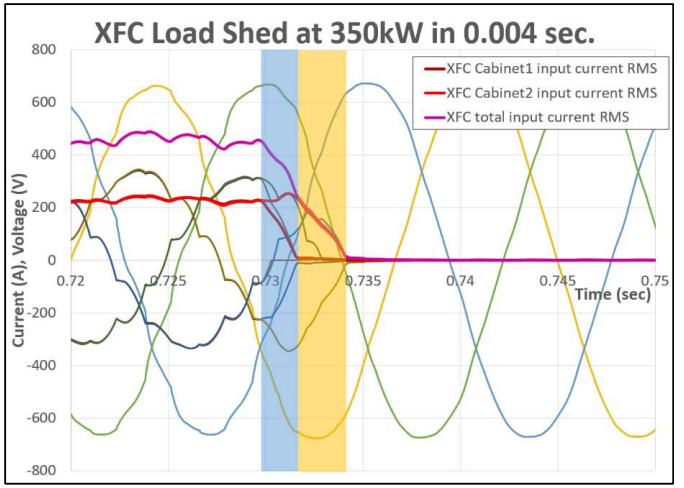


Accomplishment: Cybersecurity Assessment of ABB TerraHP-350kW (XFC)

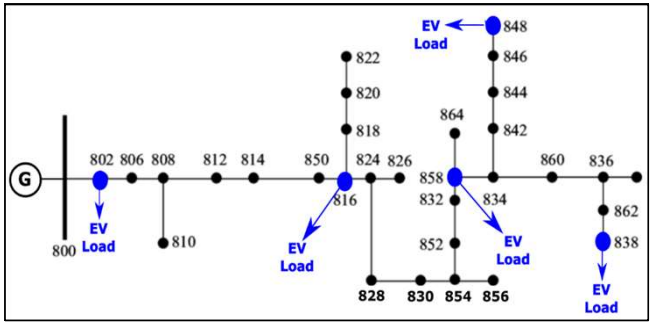
1. **Identify Attack Pathways**
   - Cellular access via ABB network, local connection, and physical access (open the enclosure)
2. **Identify Vulnerabilities**
   - Remote code execution vulnerabilities
   - OCPP “man-in-the-middle” attack techniques
   - Physical access for system compromise (risky)
3. **Attempt System Compromise**
   - Methods for remote compromise
   - OCPP client evaluation and pen testing
   - Physical access protections are strong
   - Vulnerability results report was provided to vendor
4. **Provide Mitigation Recommendations**
   - Mitigation solutions are under development and will be published at the end of this project

Accomplishment:
HCE#1: Grid Impact: Multiple Concurrent XFC Load Shed

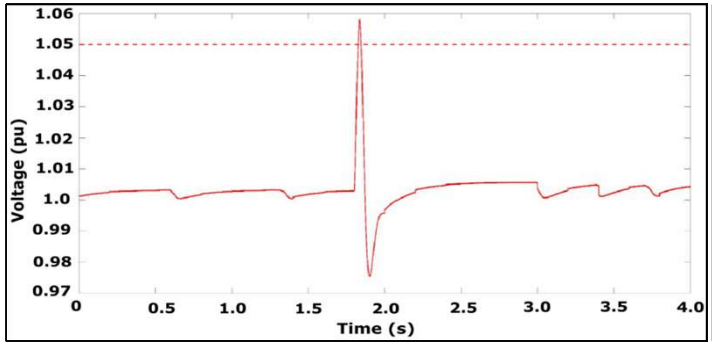
- Concurrent "stop charging" of multiple XFCs
  - Load shed from full power in **0.004 sec**
  - Multiple ways to enact the load shed (i.e. "stop charge")
    - Normal "stop charge" request from EV, HMI, or other
    - XFC internal control error state
    - OCPP command
- Simultaneous load shed can cause voltage transient >1.05pu
- Dependent upon total load and load shed amount at node



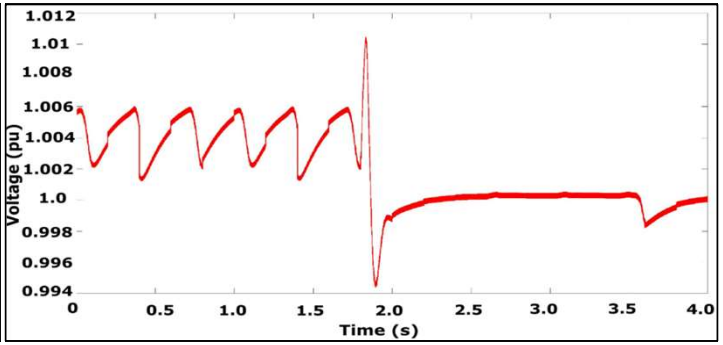
IEEE 34 bus distribution system with distributed load



15 XFC Load Shed at node 816



15 XFC Load Shed distributed across nodes

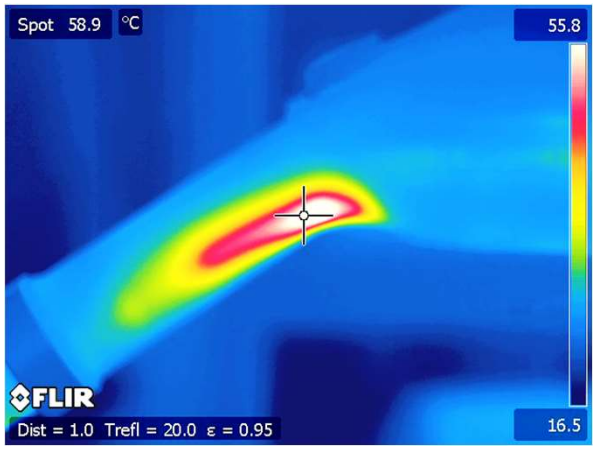


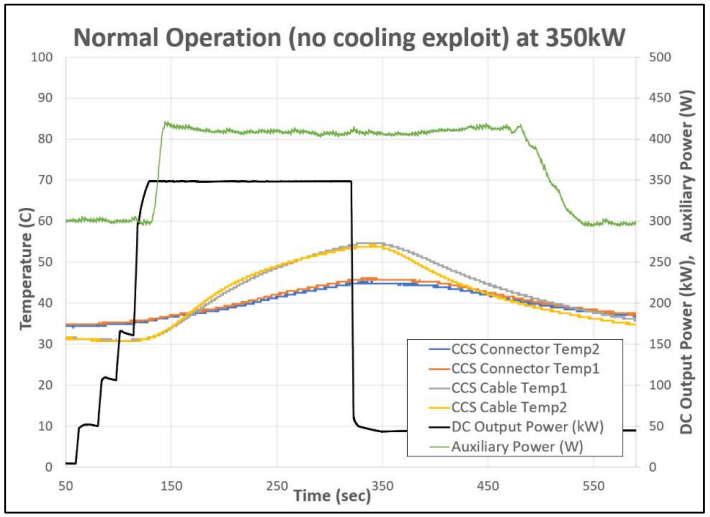
<u>Key Takeaway</u>: Simultaneous load shed from multiple XFCs may cause feeder voltage excursion or instability

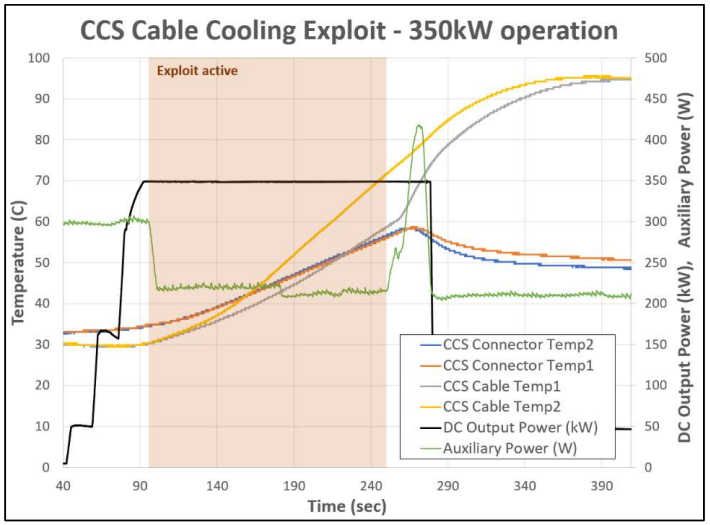
Accomplishment:
HCE#2 & #8: Cooled CCS Cable

- Vehicles <u>with</u> CCS inlet port temperature measurement
  - Exploit is significantly difficult (high cyber complexity)
- Industry standards w/ vehicle inlet port temp. measurement
  - ISO 17409
  - IEC 61851-23 ed.2

- Lab exploit: manipulation of XFC cable liquid chiller system
  - Temperature measurement
  - Coolant pump control
- Vehicle <u>without</u> CCS inlet port temperature measurement
  - Exploit shown to be successful at 350kW







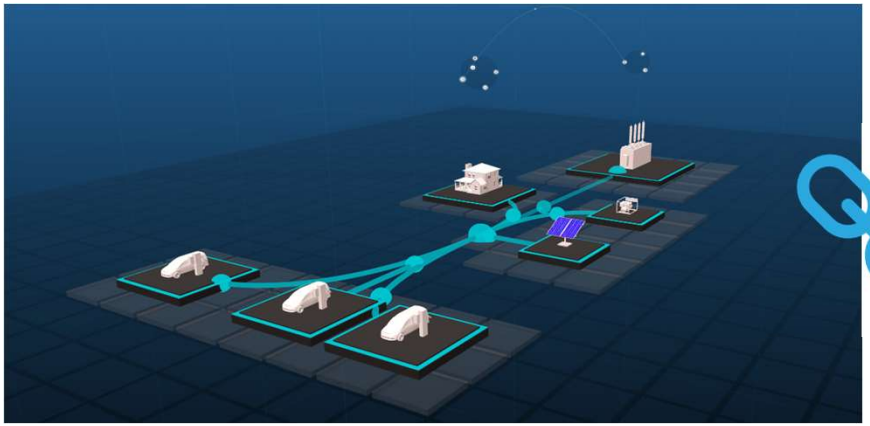
<u>Key Takeaway</u>: Exploit of cable liquid cooling system is possible when EV inlet port temperature is not monitored

HCE#3: Focus on DER Integration Impacts

Risk Assumptions

- Fuel station-integrated DER is intended to manage energy and power flows
- Site controls (local or cloud) trust information from meter, fast charger, PV, and energy storage and make coordination decisions
- Both device and communications channels susceptible to attack

EV fueling station power and networking layers were created in Cyber Energy Emulation Platform



Hardware XFC linked to station emulation

Summary and Next Steps

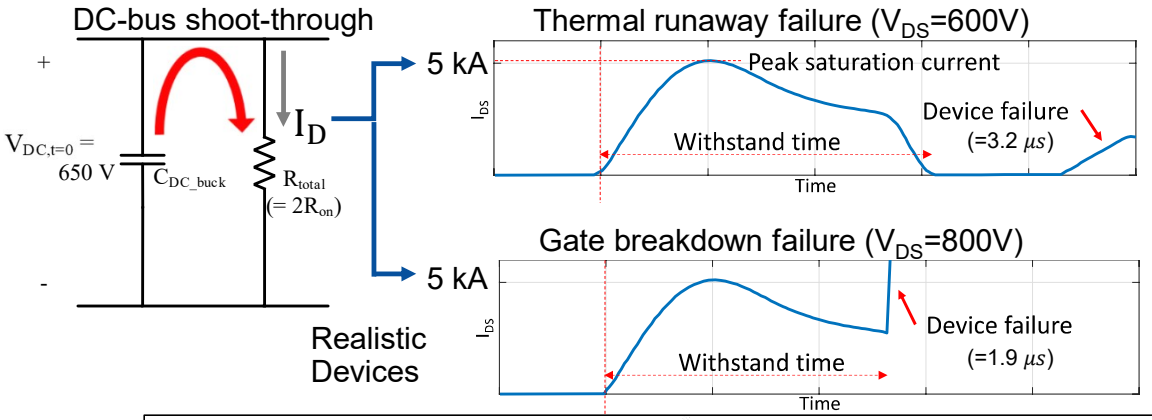
- Outcomes
  - HCE scenarios developed for DER
  - Emulation environment linked to XFC for scenario evaluation
  - Tested OCPP version and implementation-specific cyber risks
- Outlook
  - XFC, Battery, PV and site controller integrated for DER-related risk assessments
    - Mitigation strategies (e.g. battery load ramp compensating XFC change) to be explored
  - Contribute to the industry engagement and strategies sharing effort through project closeout

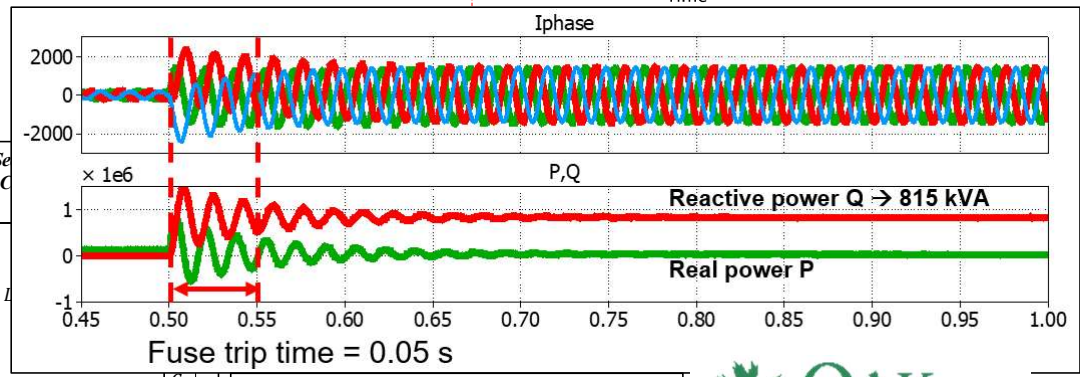
NREL
NATIONAL RENEWABLE ENERGY LABORATORY

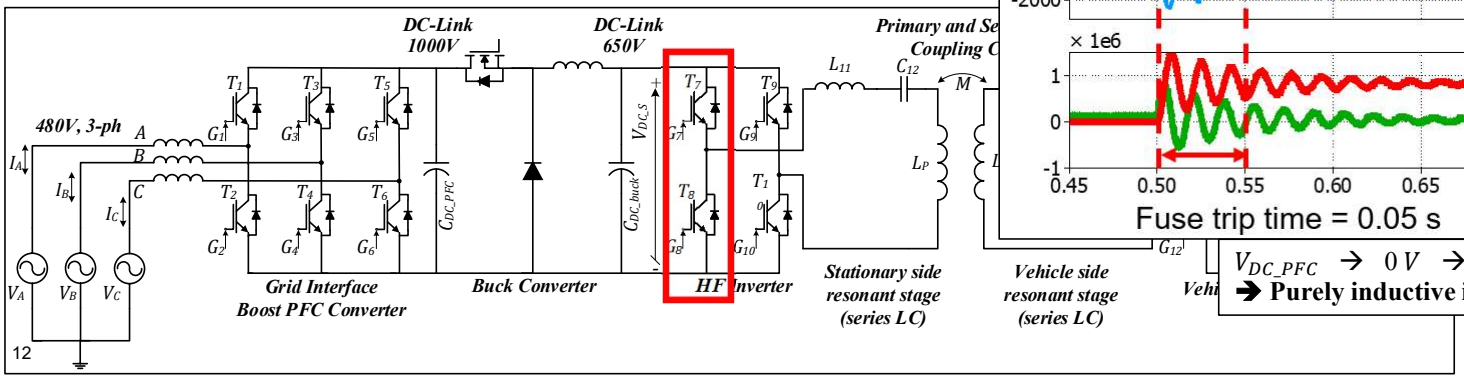
Accomplishment:
HCE#4, #11, & #14: WPT Safety and Equipment Damage

- WPT architecture review & attack path analysis for HCEs cyber complexity, impact severity, & mitigations
- HF inverter control manipulation
  - Timing manipulation can cause a short, causing thermal failure or gate breakdown failure
  - Result: sudden large current draw w/ upstream grid impacts
  - Preventable w/ low-cost hardware safeguard mitigation solution

1200V – 300A phase-leg module experimental results *F. Blaabjerg et. Al, 2017 [1]







V_{DC_PFC} → 0 V → $Z_{in} = L_{filter}$
➔ **Purely inductive input impedance**

OAK RIDGE National Laboratory

Accomplishment:
HCE#1, #6, #7, & #9: OCPP Manipulation Resulting in Load Shed, Poor Load Management, or Denial of Service

- #1: Concurrent load shed of multiple XFC causing grid instability impacts.
  - Cause: OCPP "*RemoteStopTransaction*" command initiated simultaneously for multiple XFC

- #6: Charge site improper response to energy management requests
  - Cause: OCPP "*TxProfile*" energy management spoofing for multiple charge sites

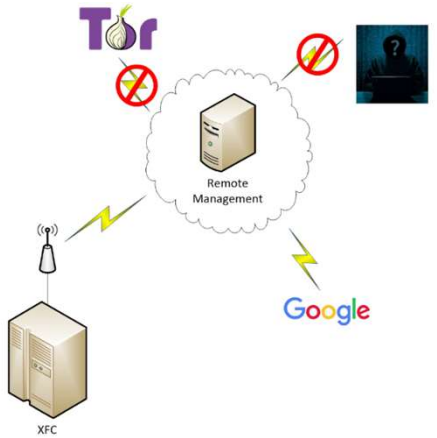
- #7 & #9: Denial of Service of multiple charge sites
  - Cause: OCPP "*Change Availability: Inoperative*" command sent to multiple charge sites resulting in "Out of Order"

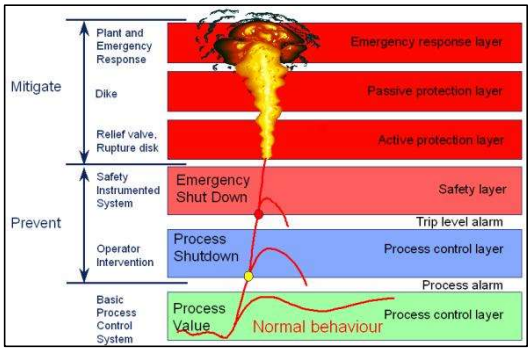
<u>Key Takeaway</u>: Correct implementation and operation of OCPP is key to avoiding several high score HCEs

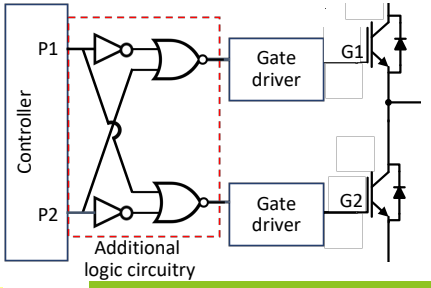
Accomplishment: Mitigation Strategies & Solutions

- General Mitigations:
  - Implement secure boot: utilize chip manufacturer features
  - Control network segmentation (isolate from internet connected devices)
  - Implement secure code signing of patches & firmware updates
  - Use secure network communication methods (e.g. SSH, SSL/TLS)
  - Intrusion Detection and Prevention (IDS/IPS) on remote access server(s)
  - Implement a zero-trust network architecture
- Specific Mitigations:
  - Controlled shutdown during a stop charge event
  - Local energy storage to buffer grid connectivity
  - Wire mesh shielding of CCS cable
  - Additional gate driver logic (μm-technology CMOS transistors)
  - Host Intrusion Detection (HIDS) to monitor critical system files
  - Safety Instrumented System (SIS) monitoring XFC operation
    - Electrical performance, temperatures, communications, etc.
  - Manage and filter internet connectivity (tunnel or VPN)

source: Emerson *DeltaV* SIS







INPUT		OUTPUT	
P1	P2	G1	G2
LOW	LOW	LOW	LOW
LOW	HIGH	LOW	HIGH
HIGH	LOW	HIGH	LOW
HIGH	HIGH	LOW	LOW

Key Takeaway: Several general and specific mitigation solutions are available to improve XFC and WPT security & reduce potential HCEs

Remaining Research (In Progress)

- Completion of Safety Instrumented System (SIS) mitigation solution
  - Monitors XFC performance, communications, and function to determine anomalies
    - Power transfer
    - Thermal control
    - Communications
  - Respond accordingly to the severity of the anomaly

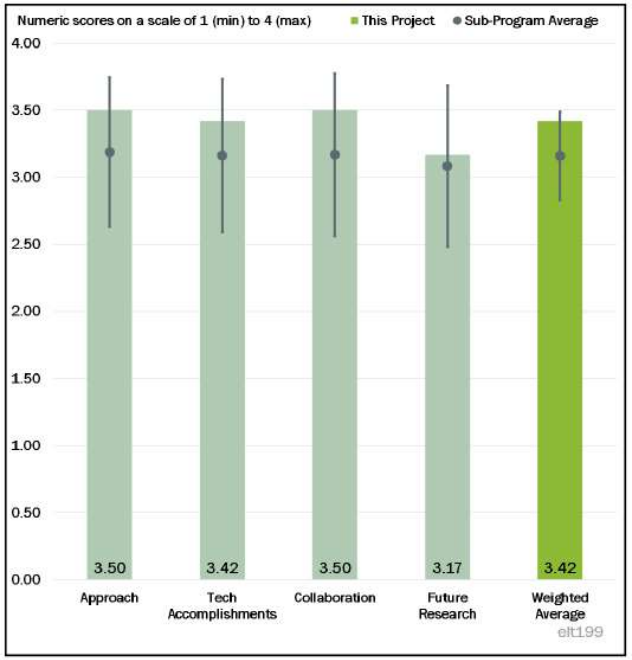
- Publish findings and lessons learned
  - HCE prioritization and analysis
  - Assessment findings
  - Laboratory evaluations results and findings
    - Impact Severity
    - Cyber manipulation complexity
  - Mitigation solutions and recommendations

Key Takeaway: Project tasks and deliverables are nearly complete

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

Response to Previous Year Reviewer Comments & Questions

- *Reviewer comment*: "….consider a sliding scale along the severity index, and perhaps even some of the rows are more consequential than others."
  - *Response*: A weighting value for each severity scoring criteria was considered. Ultimately an increased weighting value was applied only for safety criteria.
- *Reviewer question*: "The project team seems to put a lot of emphasis on a direct entry point by actual contact and less on introducing a deviant over-the-air or transmitted through a communication apparatus."
  - *Response*: Direct entry is the method used for determining the exploit feasibility. Yet, in practice the exploits will likely be conducted remotely (via energy management control, software patches, firmware updates, etc.) after the system functionality is determined through direct access.
- *Reviewer question*: "The methodology developed is intended to be published for use by system developers for future use. It would be most relevant if the development would be continued, and this process became a standard in partnership with the system developers and user groups."
  - *Response*: I agree. To reach the widest user base, this methodology for analysis, assessment, and mitigation development should be collaboratively continued within industry working group or standards based organizations.



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

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: MD/HD truck high power charging infrastructure
    - cybersecurity guidelines and recommended best practices
  - 21st Century Truck Electrification Tech Team: Charging & Infrastructure Working group
    - cybersecurity requirements and guidelines
  - Motor Coaches Industries (MCI)
  - WAVE Inc.: MD/HD wireless charging at 250+ kW
  - Utah State Univ.: static & dynamic WPT control strategies strategy development
  - Four other US DOE funded, EV charging infrastructure cybersecurity projects
    - Sandia National Lab, Virginia Tech, EPRI, ABB “CyberX”

Summary:

- Completed: conceptualization of high consequence events (HCE) for high power EV charging infrastructure

- Completed: prioritization of HCEs
  - Based upon **Impact Severity** & cyber manipulation **Complexity Multiplier (**similar to DFMEA)

- Completed: laboratory evaluation of HCEs:
  - Cybersecurity manipulation complexity
    - Hardware controls and communication systems evaluation
  - Impact severity
    - Laboratory testing and modeling simulation
  - Refine HCE prioritization scoring based on laboratory evaluation

- In progress: Develop mitigation solutions and strategies

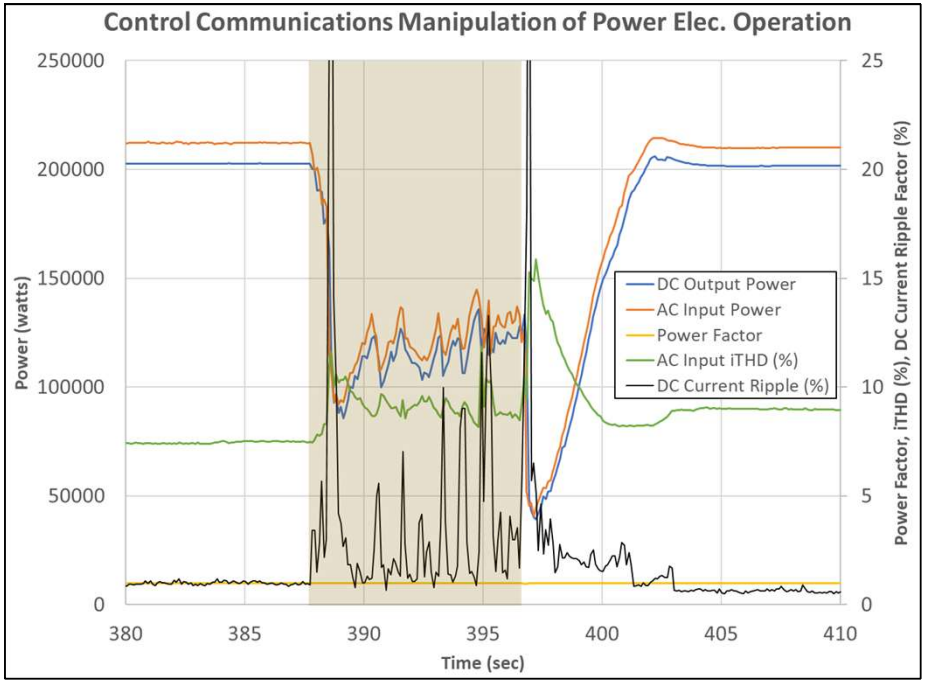
- In progress: Publish results, findings, and mitigation

Technical Back-up Slides

Technical Back-up Slide

Accomplishment: HCE#5, #10, & #15: XFC Hardware Manipulation

- XFC internal controls message manipulation
  - Power module disruption of control & coordination results in oscillation:
    - Increased:
      - DC current ripple
      - AC input current THD
    - Decreased
      - Power quality
      - Power transfer
      - Stability
- XFC temperature measurement manipulation
  - Altered temperature measurements may result in higher XFC operating temperature

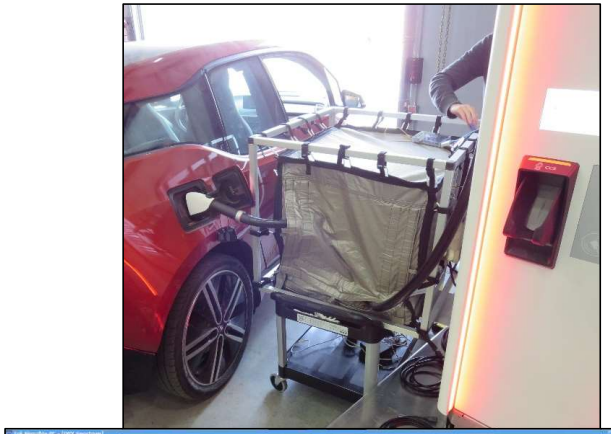


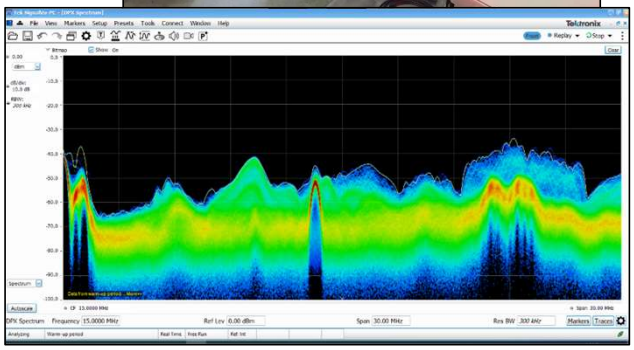
Key Takeaway: XFC internal controls message manipulation has been demonstrated which reduces power quality, charge power, and stability

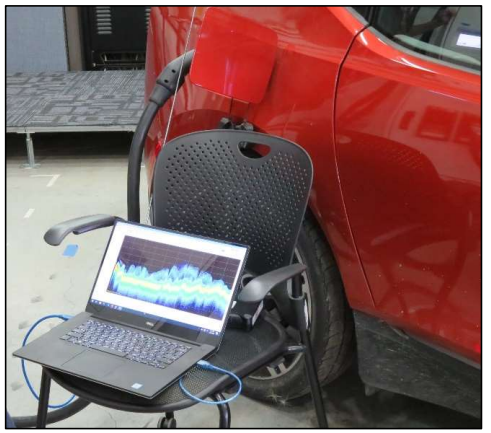
Technical Back-up Slide

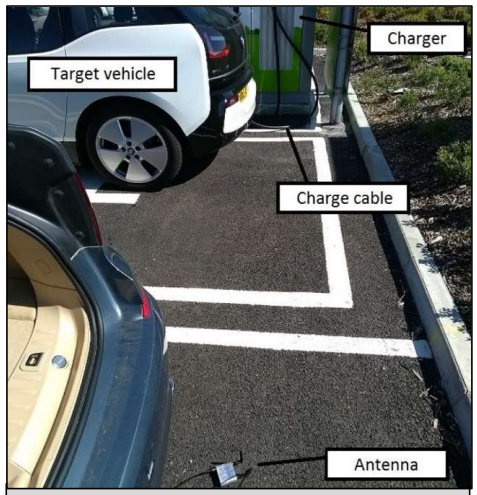
Accomplishment: HCE#12: Theft or Alteration of Data / Information

- Data theft of CCS communication is possible without physical connection (i.e. “wireless sniffing”)
  - Hardware demonstrations confirm effectiveness for CCS “wireless sniffing”
    - Univ. of Oxford demonstrated waveform capture and decryption of data packets with DCFC air-cooled CCS cable
    - INL demonstrated same waveform capture of CCS information with XFC liquid cooled cable









“Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging”. Richard Baker and Ivan Martinovic, *University of Oxford* https://www.usenix.org/conference/usenixsecurity19/presentation/baker

Key Takeaway: With the right knowledge & equipment, some CCS charging information can be obtained wirelessly several meters away from the XFC

Technical Back-up Slide

Accomplishment:
HCE #6, #7, & #9: Non-responsive to Load Management (Denial of Service)

- Communication to XFC or charge site is disrupted or manipulated
  - Curtailment requested manipulation: no change in load (or even increase in load)
  - Non-responsive operation to load management / scheduling
  - XFC forced into “Off-line” status

- Manipulation of OCPP or other charging management communications

- Result:
  - Increased demand charges (cost)
  - Potential overload on feeder
  - Increased curtailment required of other loads on the same feeder

Key Takeaway: Potential of increased costs or grid impacts; Security is crucial for OCPP or other energy management systems for effective XFC site load management and operation

Technical Back-up Slide

Publications and Presentations

- Sanghvi, A., Markel, T., "Cybersecurity for Electric Vehicle Fast-Charging Infrastructure." IEEE Transportation Electrification Conference. June 21-25, 2021.