Richard "Barney" Carlson,
Kenneth Rohde
Idaho National Laboratory

Transport Canada Panel Session
March 24, 2022

Consequence-Driven Cybersecurity for High-Power EV Charging Infrastructure

INL/MIS-21-62225

Idaho National Laboratory

Impact & Relevance:

- Significant risks from the exploit of cybersecurity vulnerabilities of EV charging infrastructure:
  - Publicly accessible EV charging systems
    - High-voltage
    - High-power
  - Increased system complexity
    - Multiple communications pathways between EV, EVSE, charge service provider, utility, etc.
    - Advanced energy management: Smart Charge Management, V2G, grid services, etc.
    - Advanced power electronics systems
    - Thermal management systems
  - Integrated into national critical infrastructure (electric grid)
    - Several MW load is possible with a mid-sized charging station/plaza (i.e. six 350kW chargers)
    - Transient (fast charging) power transfer is inherent for DC charging
      - Target EV recharge in <10 min. requires high-power transfer

Project Information and Objective

- U.S. DOE funded project focused on high-power EV charging infrastructure cybersecurity
  - Analysis, laboratory hardware evaluation, mitigation solution development
- Project Team
  - Idaho National Lab (INL)
  - Oak Ridge National Lab (ORNL)
  - National Renewable Energy Lab (NREL)
  - ABB
  - Tritium
  - Electrify America

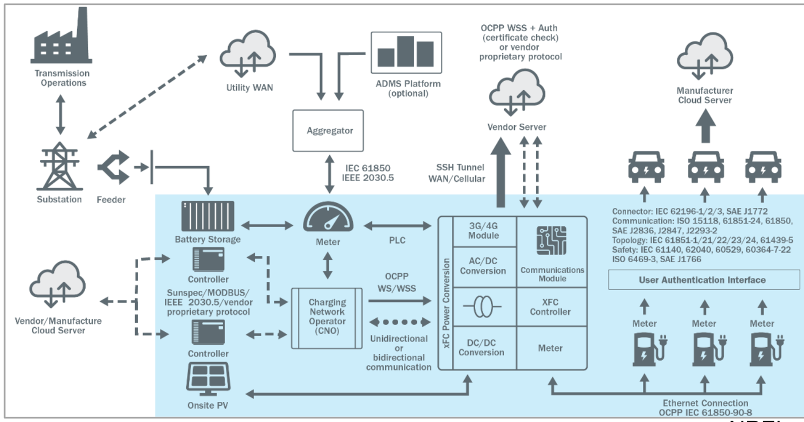
Objective:

- Quantify, analyze, and reduce risks associated with vulnerabilities and exploits of 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

Project Approach:

1. Conceptualize high consequence events (HCE)
2. Prioritize HCEs
   – Based upon **Impact Severity** scoring & Cyber Manipulation **Complexity** scoring
3. Laboratory evaluation of HCEs:
   - Cyber manipulation complexity
   - Impact severity

   – Iterative refinement of HCE scoring and prioritization based on lab results
4. Develop mitigation solutions and strategies
   – Evaluation of proof-of-concepts in laboratory
5. Publish project results, and findings



source: NREL

<u>Project Boundaries & Assumptions:</u>

- DC charging (not AC charging)
- Only events originating from cyber exploits
- Not including natural events (weather, vandalism, etc.)
- With enough time & effort, a skilled & knowledgeable adversary can access or compromise nearly any electrically controlled system

High Consequence Events (HCE) Analysis and Prioritization Ranking

HCE Ranking Prioritization

HCE Score = Impact **x** Complexity

- Impact Severity score based on 8 criteria
- Complexity Multiplier score (ease of cyber-manipulation)

Cybersecurity Complexity Multiplier Scoring

Score	Description
10	**Extremely Low Complexity** – Only a single system requires modification. System is easily reachable by the adversary (physical or virtual). No preconditions required.
8	**Low Complexity** – Only a single system requires modification. System is not easily reachable, but compromise of the system is trivial once access is available. No preconditions required.
6	**Medium Complexity** – One or more systems require modification. System(s) are reachable with effort, but compromise is generally successful. Preconditions may be required.
4	**Difficult Complexity** – More than one system requires modification. Systems are difficult to reach. Compromise requires specialized skills. Preconditions are required for successful exploit.
2	**Extremely Difficult Complexity** – More than one system requires modification. Systems are difficult to reach. Compromise is not always successful. Preconditions are required for successful exploit, and these conditions are rare.

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

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

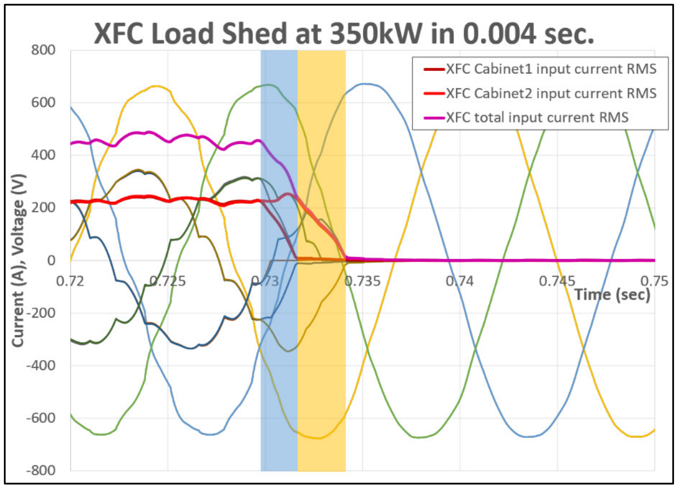
Laboratory Evaluation of Impact Severity & Cyber Manipulation Complexity

Cybersecurity Assessment of ABB TerraHP-350kW (XFC)

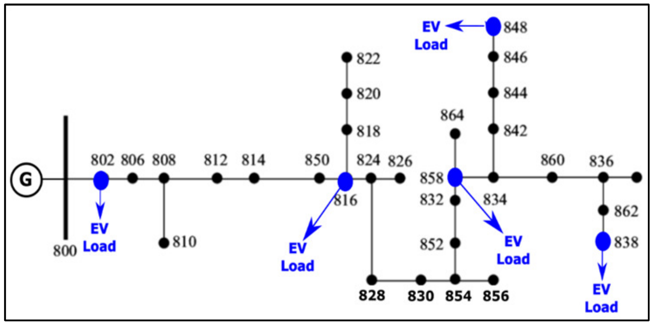
1. **Identify Attack Pathways**
   - Cellular access via ABB network, local connection, and physical access (open the enclosure)
2. **Identify Vulnerabilities**
   - Remote code execution vulnerabilities
   - OCPP “man-in-the-middle” attack techniques
   - Physical access for system compromise (risky)
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

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

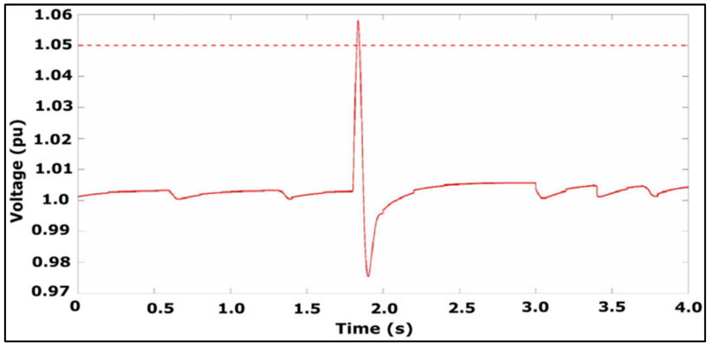
- Concurrent “stop charging” of multiple XFCs
  - Load shed from full power in **0.004 sec**
  - Multiple ways to enact the load shed (i.e. “stop charge”)
    - Normal “stop charge” request from EV, HMI, or other
    - XFC internal control error state
    - OCPP command
- Simultaneous load shed can cause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



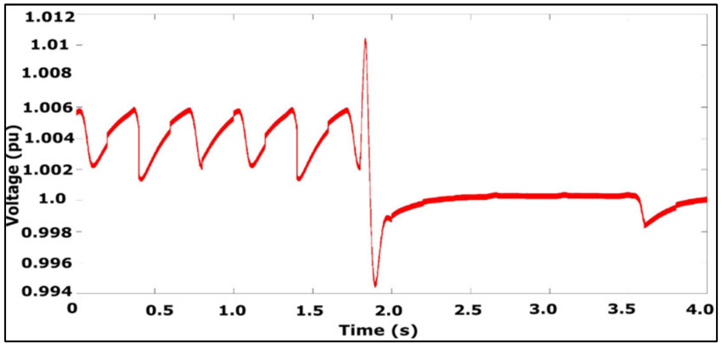
IEEE 34 bus distribution system with distributed load



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

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

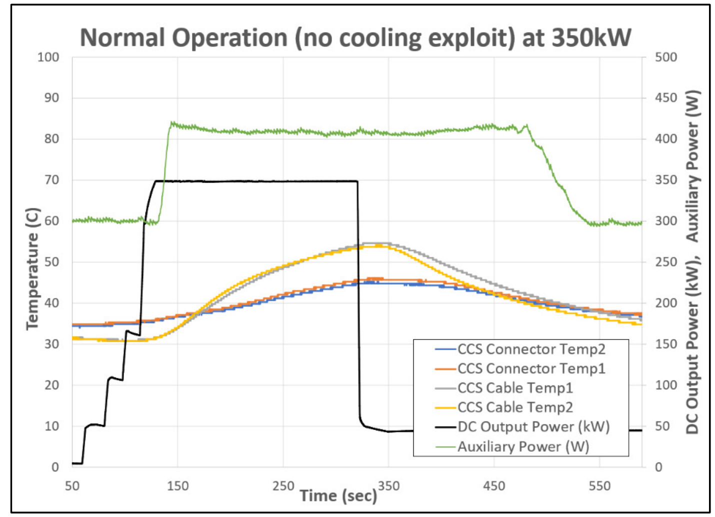
- #6: Charge site improper response to energy management requests
  - Cause: OCPP "*TxProfile*" energy management spoofing for multiple charge sites

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

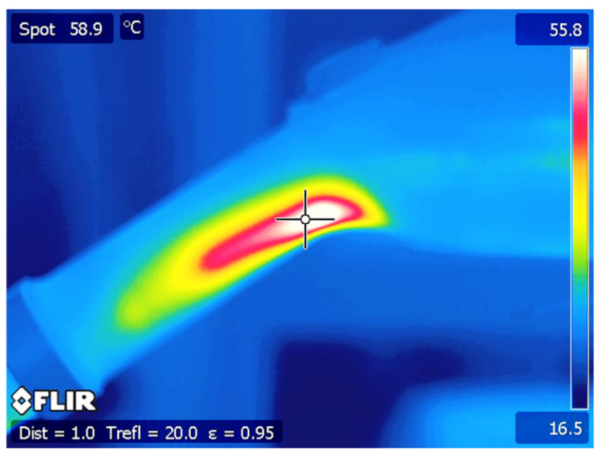
<u>Key Takeaway</u>: Correct implementation and operation of OCPP is key to avoiding several high score HCEs

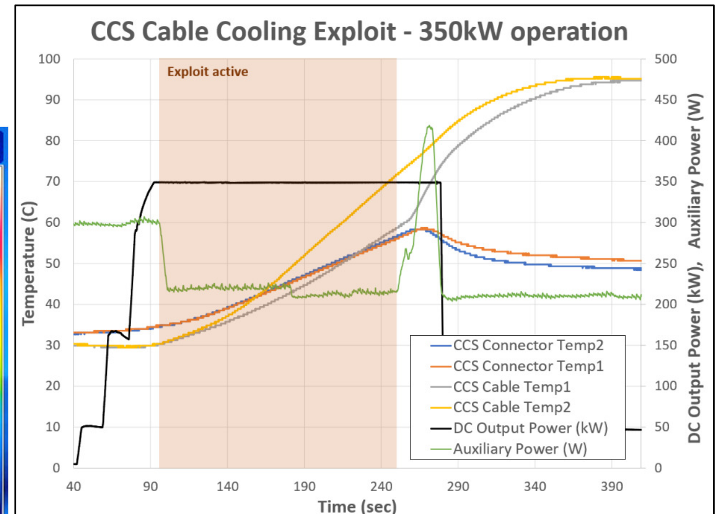
HCE#2 & #8: Exploit Liquid-cooled Cable

- EV <u>with</u> CCS inlet port temperature measurement
  - Exploit is significantly difficult (manipulate EV and XFC)
- Industry standards w/ vehicle inlet port temp. measurement
  - ISO 17409
  - IEC 61851-23 ed.2



- EV <u>without</u> CCS inlet port temperature measurement
  - Exploit is less difficult (manipulate only XFC)
- Lab exploit evaluation of XFC cable liquid chiller system
  - Temperature measurement
  - Coolant pump control
- Exploit shown to be successful at 350kW

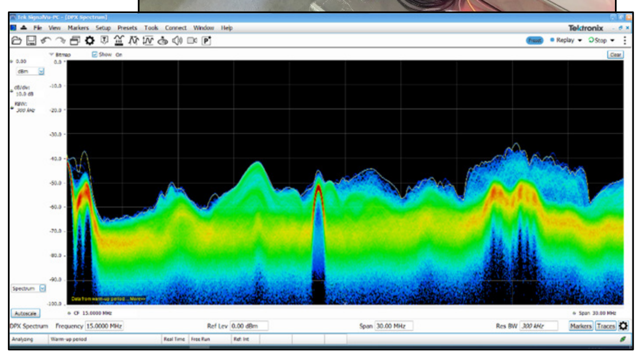


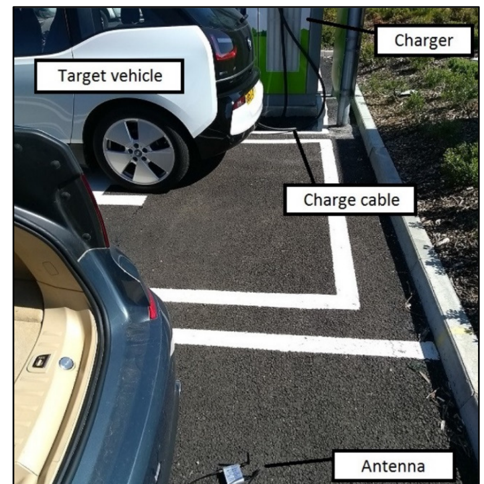


<u>Key Takeaway</u>: Exploit of cable liquid cooling system is possible when EV inlet port temperature is not monitored

HCE#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 similar waveform capture of CCS information from XFC liquid cooled cable





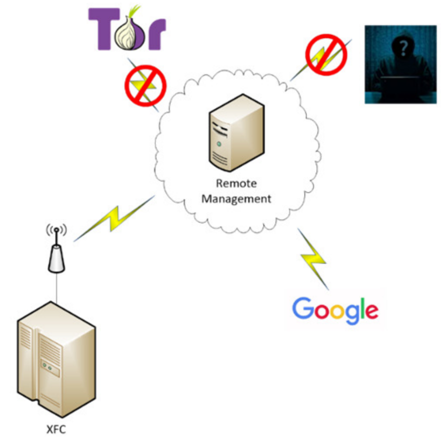
“Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging”. Richard Baker and Ivan Martinovic, *University of Oxford* https://www.usenix.org/conference/usenixsecurity19/presentation/baker

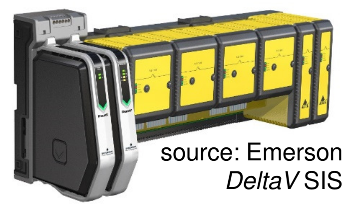
Key Takeaway: With the right knowledge & equipment, some CCS charging information can be obtained wirelessly several meters away from the XFC

Mitigation Solutions

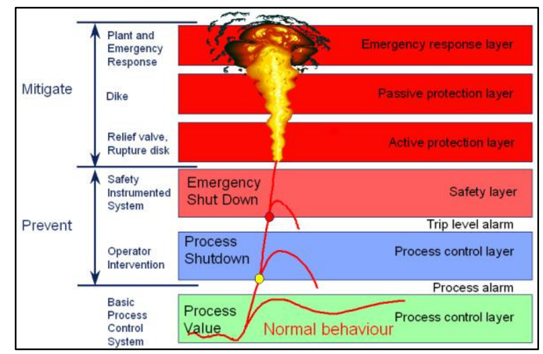
Mitigation Strategies & Solutions

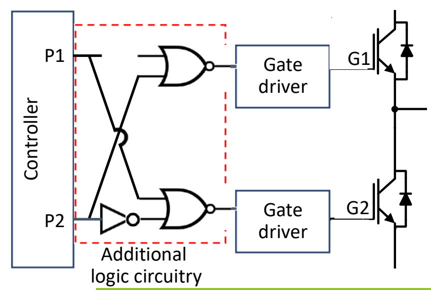
- General Mitigations:
  - Implement secure boot: utilize chip manufacturer features
  - Control network segmentation (isolate from internet connected devices)
  - Implement secure code signing of patches & firmware updates
  - Use secure network communication methods (e.g. SSH, SSL/TLS)
  - Intrusion Detection and Prevention (IDS/IPS) on remote access server(s)
  - Implement a zero-trust network architecture
- Specific Mitigations:
  - Slower, 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

Summary:

- High consequence events (HCE) conceptualized for high power EV charging infrastructure

- HCE prioritization and ranking:
  - 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
  - Iterative refinement of HCE prioritization scoring based on laboratory evaluation results

- Development of mitigation solutions and strategies

- Publish results, findings, and mitigation
  - Draft publication under review by U.S. DOE VTO intended for *Energies* Journal: Special Edition "Cybersecurity Solutions for Electric Vehicle Chargers"