Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid

Barney Carlson – Advanced Vehicles group
Ken Rohde – Cyber Security R&D group

Sept. 12, 2018
Relevance of Cyber Security for High Power EV Charging

1. Public Safety
   - High voltage & high current charging infrastructure

2. Potential wide spread grid impact
   - Intermittent high load: ranging from 50kW to 350+ kW
   - Increasing deployment of fast chargers to meet needs of increasing EV market adoption

3. Consumer confidence in charging infrastructure
   - Reliability and robustness required to reduce range anxiety
**INL Capabilities:**

**EV Charging Grid Integration Research**

- **Charging Infrastructure Evaluation**
  - Operational performance & dynamic response evaluation
    - Conductive (L2, DCFC, XFC)
    - Wireless power transfer (WPT)
  - Dynamic Evaluation & Analysis
    - Power hardware-in-the-loop real time emulation
      - Communication
      - Dynamic transients
      - Power Electronics

- **Cyber Security R&D**
  - End-to-End research methodology
    - Integrated risk management
    - Consequence-driven Cyber-informed engineering (CCE)
    - Strategy development to close attack vector & gaps

**INL’s Capability:** Identify and mitigate EV charging infrastructure vulnerabilities capable of compromising electric grid resiliency and reliability.
Cyber Security: Electrified Transportation Charging Infrastructure

- **Vulnerabilities (Pathways and Attack Vectors)**
  - System vulnerabilities
    - Communications pathways (vehicle to EVSE, EVSE to smart grid, etc.)
    - Controls systems (power electronics, energy management, thermal controls, etc.)
    - Physical vulnerabilities (access control, electrical, thermal, etc.)

- **Risk, Threats, & Impacts:**
  - **Moderate:** denial of service (no charging)
  - **Extensive:** hardware damage / destruction
  - **Severe:** human safety; wide-spread disruption of electrical power distribution / transmission

- **Mitigation Strategies & Solutions:**
  - Prioritize mitigation of exploitable and high risky vulnerabilities
EV Charging Communications and Controls

Electric Grid

DC Fast Charger

- Communications
- Controls System
- Cooling
- Power Electronics
- Power Electronics
- Power Electronics

IEEE 2030.5 (SEP 2.0)
IEC 61850 (OCPP)
ISO 15118 (CCS)
IEEE 2030.1-1 (CHAdeMO)

AC power
DC current

Energy Aggregator

EVSE Service Provider

Open ADR

Grid Connected Vehicle
External Attack Surfaces and Attack Vectors

DC Fast Charger

Electric Grid

Energy Aggregator

IEEE 2030.5
(SEP 2.0)

Open ADR

AC power

EVSE Service Provider

IEC 61850
(OCPP)

ISO 15118 (CCS)

IEEE 2030 1.1

CHAdeMO

Cooling

DC current

Grid Connected Vehicle
Internal Attack Surfaces and Attack Vectors

DC Fast Charger

- Communications
- Controls System
- Power Electronics
- Power Electronics
- Power Electronics

Cooling
Project Scope

• Identify and evaluate high risk vulnerabilities of 50 kW DC Fast Charging system (DCFC)
  – Scope to date: internal attack vectors
    • power electronics, internal controls systems, and internal communications

• Determine extent of possible impacts
  – Hardware damage
  – Impacts to electric grid

• Develop cyber-informed engineering methodologies

• Evaluation of production DCFC (50 kW) with J1772 CCS and CHAdeMO
• Vehicles utilized during evaluation
  – 2014 EV with CHAdeMO
  – 2015 EV with J1772 CCS

Photo source: Nissan
Photo source: BMW
Photo source: CHAdeMO
Photo source: SAE International

Attack Vectors - DCFC

- Minimal details presented: do not publically disclose detailed malicious information
  - DCFC internal power electronics communications are disrupted
    - Using off the shelf communication tools (send & receive messages)
    - “Man in the middle” module was not used
  - After physical access was obtained (open DCFC enclosure), connection was easily made to the single internal communications network
  - With remote access achieved, same control manipulation is enabled since the HMI is connected to the single internal communications network
- Able to manipulate modular power electronics controls system inside DCFC
  1. Disrupt controls coordination between power electronics modules
  2. Simultaneously turn off all power electronics modules
- Unable to directly control high speed switching inside the power electronics modules
- Unable to over charge the EV (excessive current over EV requested current)
  - EV stopped charge event: shut down command or opening battery contactors
Recent Results and Findings

- Disrupt controls coordination between power electronics modules
- Response of the DCFC:
  - Fluctuation of:
    - Input power from grid
    - Input power quality
      - Power Factor
      - Current THD
    - Output power to EV
  - Results in power quality outside of industry limits
    - Power Factor: <0.8
    - Current THD: > 20%
Recent Results and Findings

- Simultaneously turn off all power electronics modules
  - Response of the DCFC:
    - Full power (50 kW) to standby power (~300W)
      - 0.020 seconds (-2.6 MW/sec)
  - No impact to grid from a single DCFC shut down
  - Potential impact to grid if simultaneously shut down of 100’s of DCFC
    - What about 350 kW XFC
Future Advancement: High Power and Complexity

- Increased vulnerabilities and risk with increased charge power and system complexity

- Increased System Complexity
  - Advanced Control System of modular components
  - Multiple communication pathways

- Increased Charge Power
  - Potential increased grid interaction impacts
  - Increased safety risks
Wireless Charging (WPT) & Xtreme Fast Charging (XFC)

- **XFC**: Higher power
  - 350 kW (500A / 1000VDC) or higher
  - Liquid cable & connector cooling system
  - Multiple standards still required (CCS, CHAdeMO, GB/T, overhead charging, etc.)
  - Likely co-located with several XFC at charge depot (>1 MW demand on grid)

- **WPT**: Higher complexity controls
  - Controls communication is wireless (from ground assembly to vehicle assembly) 802.11p & 802.11n
  - Foreign object detection system
  - Vehicle approach, pairing, and alignment system
Lessons Learned: Guidelines for improved security / robustness

• Communication and Controls Security (internal and external)
  – Encryption for external communications, verification of information origin
  – Unique keys (not the same key for all chargers deployed)
  – Remove external jacks, disable JTAG, and secure boot loaders
  – Secure remote firmware updates capable with firmware integrity verification
  – Communication message freshness verification (identify replay attacks)
  – Segmentation of control systems (GUI, power electronics, vehicle interface, energy management)
  – Log events for security forensics

• Physical security
  – Recognition of physical access (open door) or physical manipulation
  – Tamper resistant enclosure

• Procedural
  – Manufacturer software and hardware quality assurance program
Potential Mitigation Solutions and Strategies

- Decouple DCFC load transients from grid
  - Local Energy Storage
  - Charger site DC bus with DER
    - a.k.a. “DC-as-a-service”

- DCFC internal performance monitor
  - Electrical performance and characteristics
  - Monitor communication for anomalies
Next Steps:

• Develop methodologies for cyber secure engineering design of charging systems
  – Internal controls and communications
  – External communication and security

• Quantify impacts of malicious events on electric grid networks
  – Decreased Power Quality
  – Coordinated large step change in power

• Evaluation and analysis of:
  – Xtreme Fast Charging system
    • Modular designs
  – Wireless charging system
    • Wireless communications (802.11p, 802.11n)
      – Automated power transfer control
    • Safety systems
      – Live object detection, Foreign object detection, vehicle alignment and pairing
Summary

• **Cyber security** of high power charging infrastructure
  – Consequence driven, Cyber-informed Engineering (CCE) process
  – Develop cyber-informed engineering methodologies and mitigation strategies

• **Identified risks and threats**
  – Internal power electronics controls able to be maliciously manipulated
  – High priority threats / risks when coordinated attack

• **Identified vulnerability impacts**
  – Poor power quality
  – Coordinated, sudden change in load

• **Potential mitigation strategies and solutions**
  – Local energy storage
  – Security monitor within charger system