INL/CON-18-52242-Revision-0

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

Kenneth W Rohde

January 2019

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/CON-18-52242-Revision-0

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

Kenneth W Rohde

January 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract 103040163

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

Kenneth Rohde – Cyber Security R&D
kenneth.rohde@inl.gov

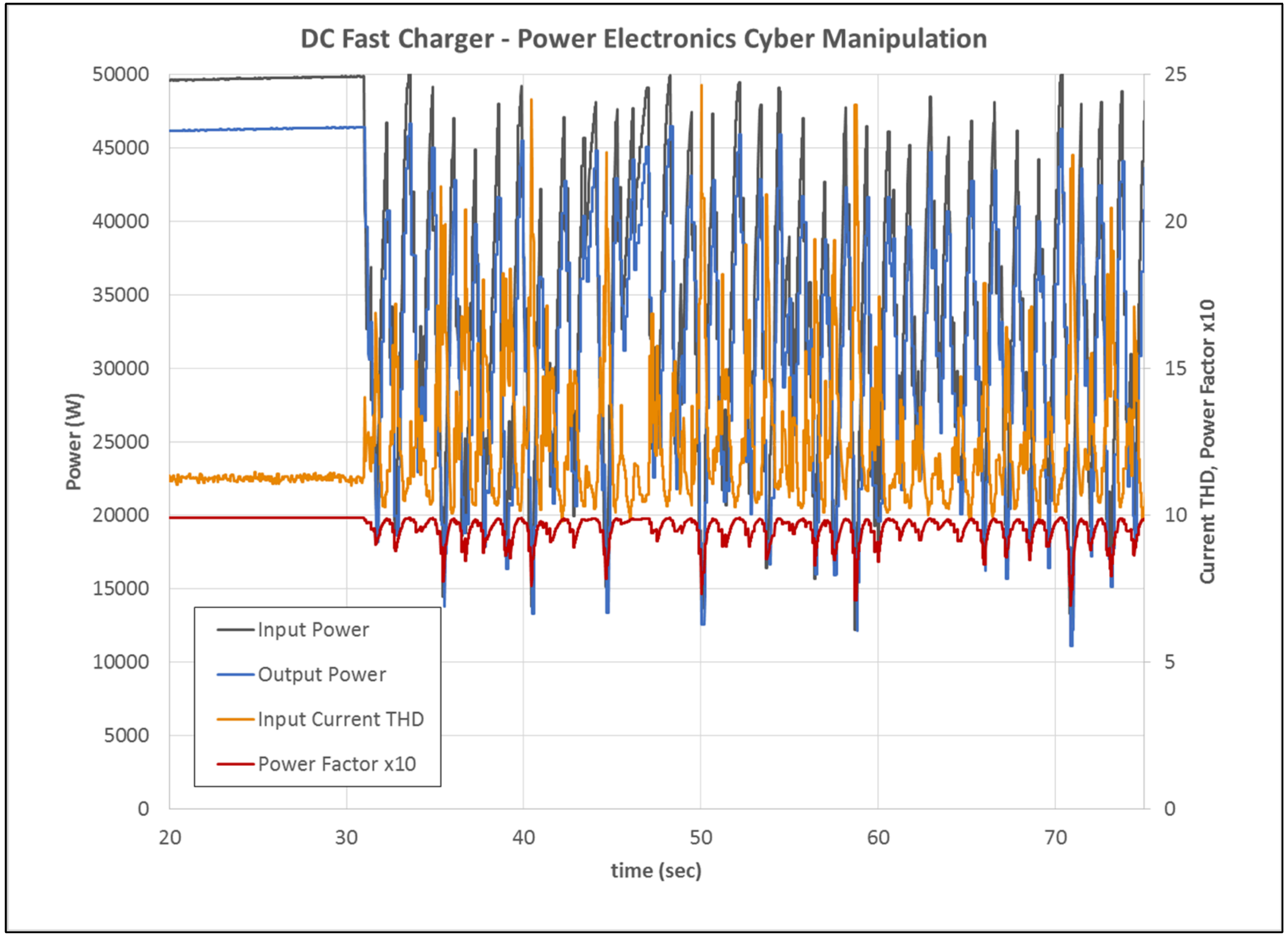
Idaho National Laboratory

INL/CON-18-52242

Video

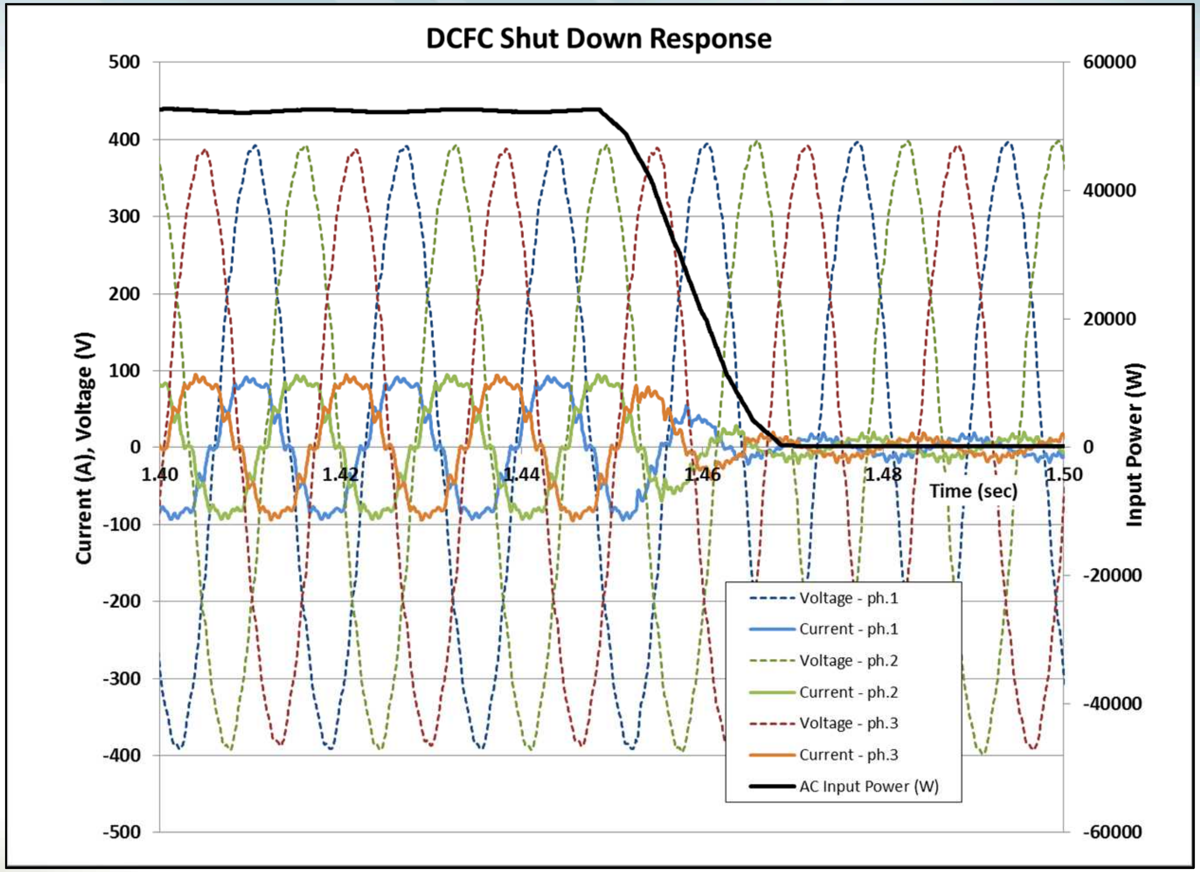
Power Quality Measurements

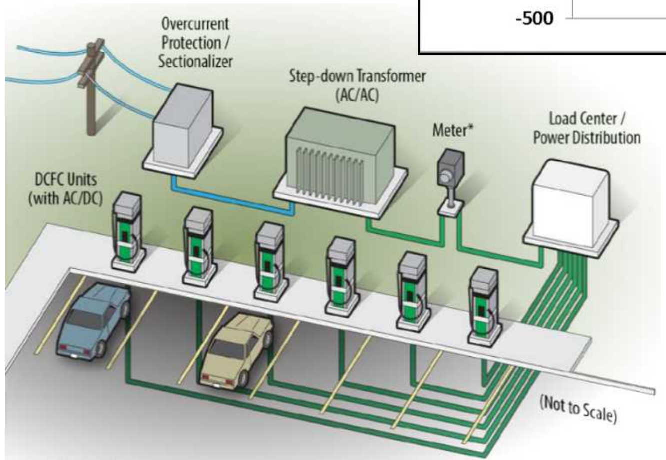
- Disrupt controls coordination between power electronics modules
- Response of the DCFC:
  - Fluctuation of:
    - Input power from grid
    - Input power quality
      - Power Factor
      - Current THD
    - Output power to EV
  - Results in power quality outside of industry limits
    - Power Factor: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



Transient Power

- 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?





Electrify America

- Walmart in Idaho Falls – 1.2MW “Capacity”

1x 350KW CCS
1x 150KW CCS

2x 350KW CCS

1x 150KW CCS
1x 50KW CHAdeMO

2x 350KW CCS

Magic Power Electronics

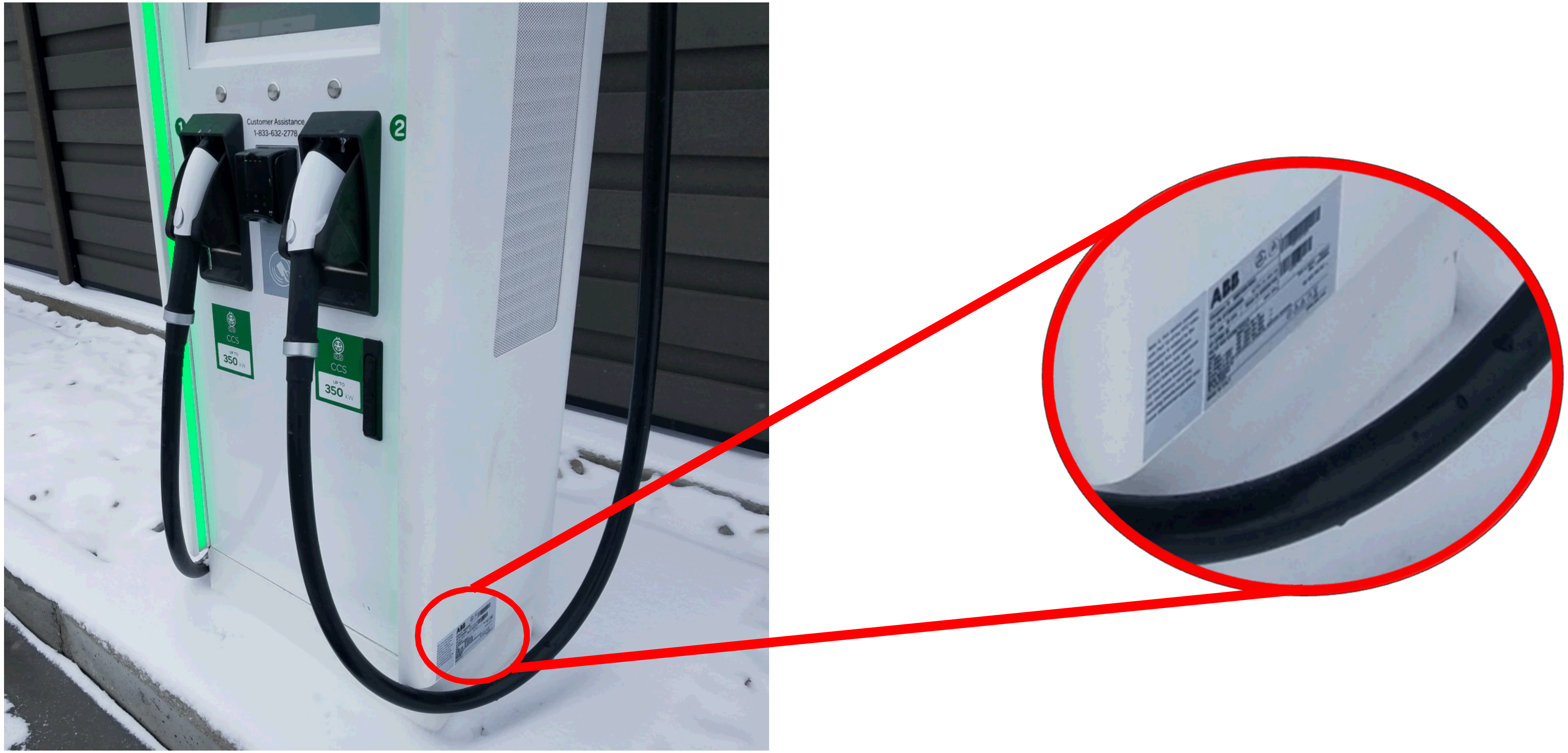
500 KVA Transformer?

Electrify America

- The magic boxes…

Electrify America

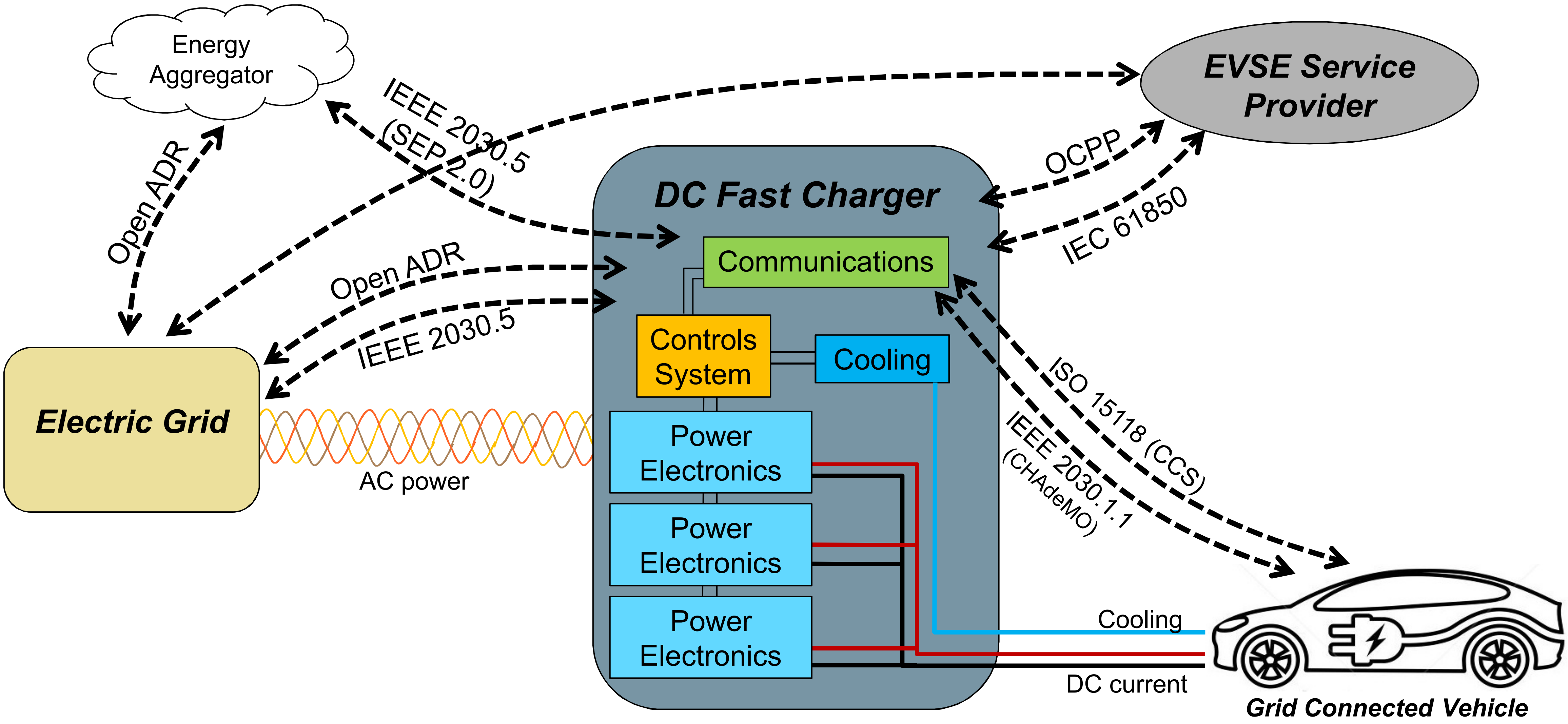
- If I only knew which vendor built these…



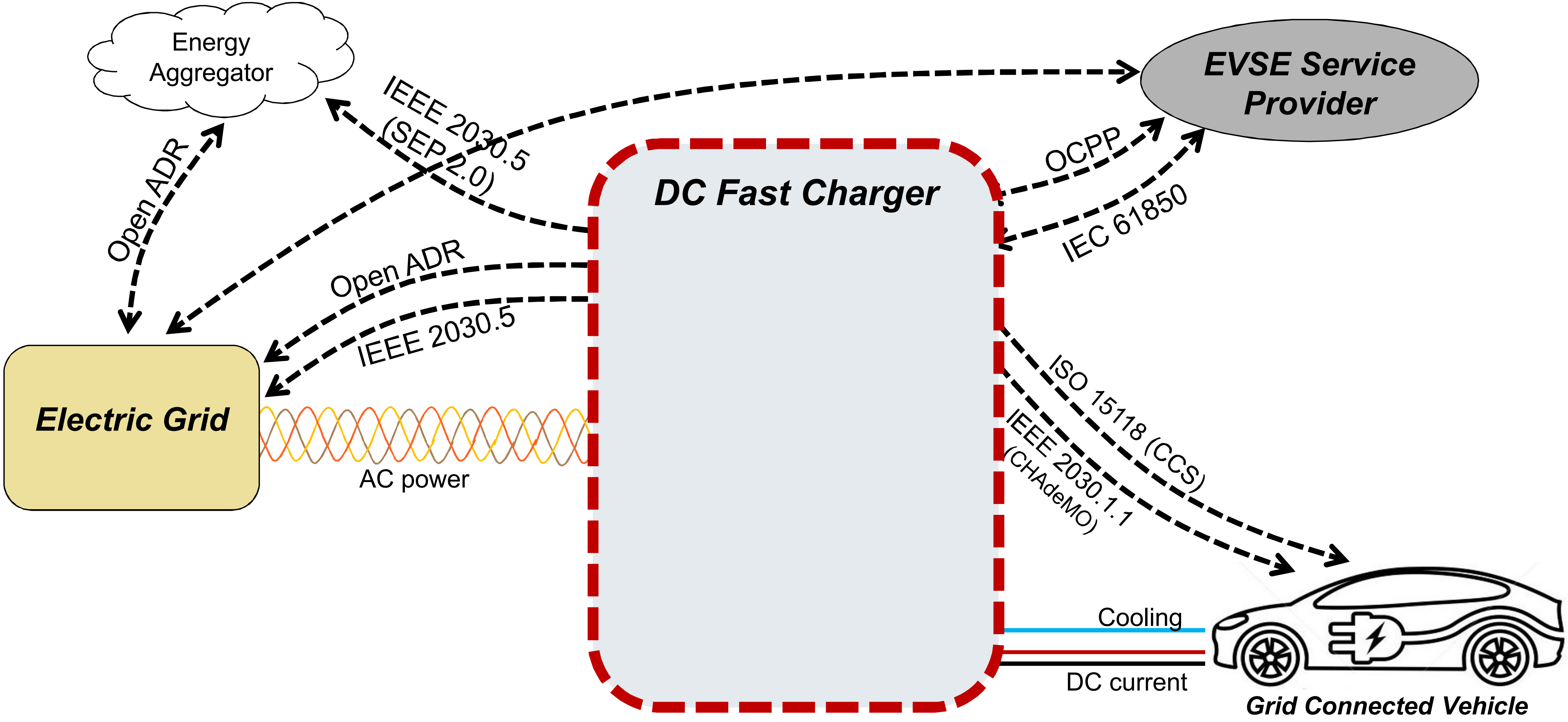
Cyber Security: EV Charging Infrastructure

- **<u>Vulnerabilities (Pathways and Attack Vectors)</u>**
  - Communications pathways (vehicle to EVSE, EVSE to service provider, EVSE to grid, etc.)
  - Controls systems (power electronics, energy management, thermal controls, etc.)
  - Physical vulnerabilities (access control, electrical, thermal, etc.)
- **<u>Risk, Threats, & Impacts</u>**:
  - *Moderate*: denial of service (no charging)
  - *Extensive*: hardware damage / destruction
  - *Severe*: human safety; wide-spread impact to electrical grid
- **<u>Mitigation Strategies & Solutions:</u>**
  - Prioritize mitigation of high risk, exploitable vulnerabilities

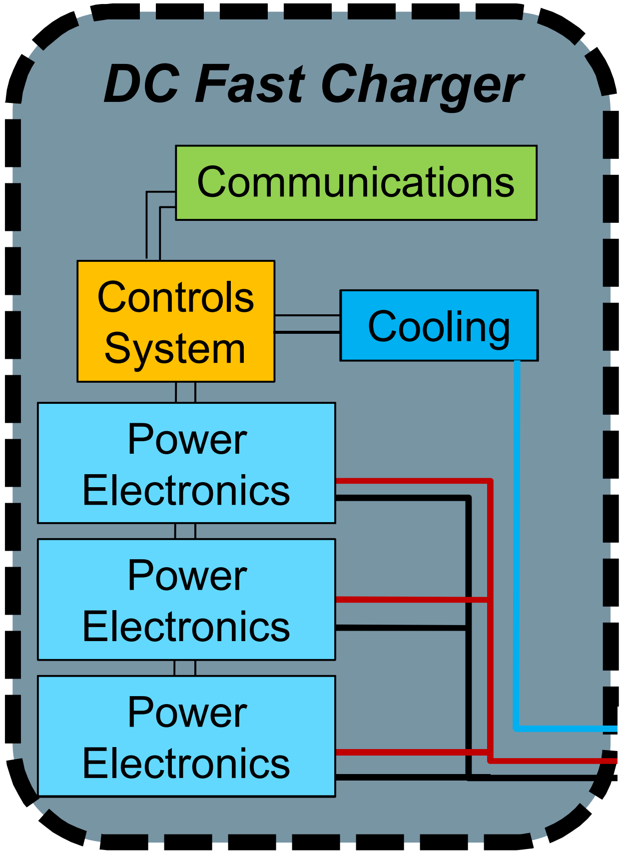
EV Charging Communications and Controls



External Attack Surfaces and Vectors



Internal Attack Surfaces and Vectors



Demonstration Details

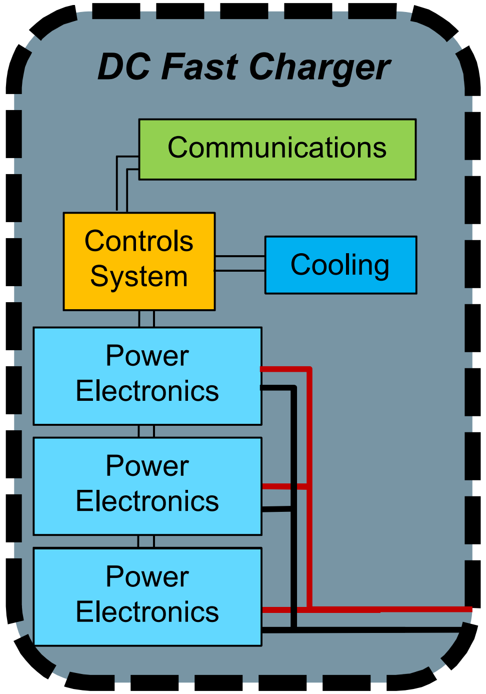
Note: minimal malicious details will be presented

- To not publically disclose detailed manipulation information

- DCFC internal power electronics communications were disrupted
  - Using off-the-shelf communication tools
    - Transmit & receive messages
  - "Man in the middle" module was not used
    - Intercept and retransmit modified messages

- After physical access was obtained (open DCFC enclosure), connection was easily made to the single internal communications network

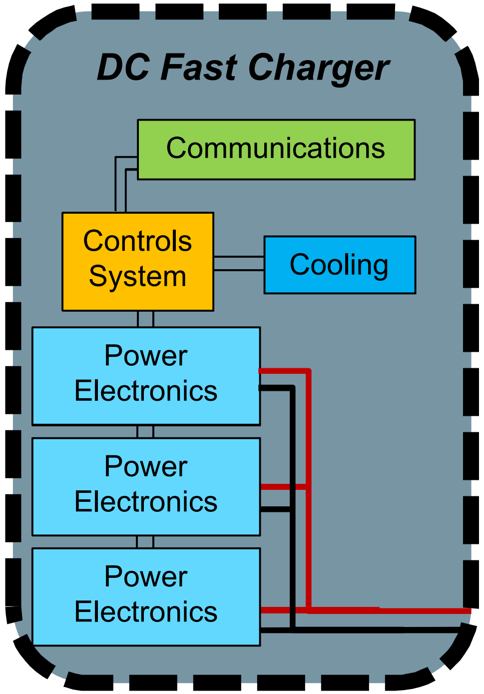
- With remote access achieved, same control manipulation is enabled since the HMI is also connected to the single internal communications network



Demonstration Details

Successful:

- Able to manipulate the controls system inside DCFC
    1. Modify the HMI front panel display indicating charging status
        1. SOC, time remaining, charge power, etc.
    2. Disrupt controls coordination between power electronics modules
    3. Simultaneously turn off all power electronics modules



Unsuccessful:

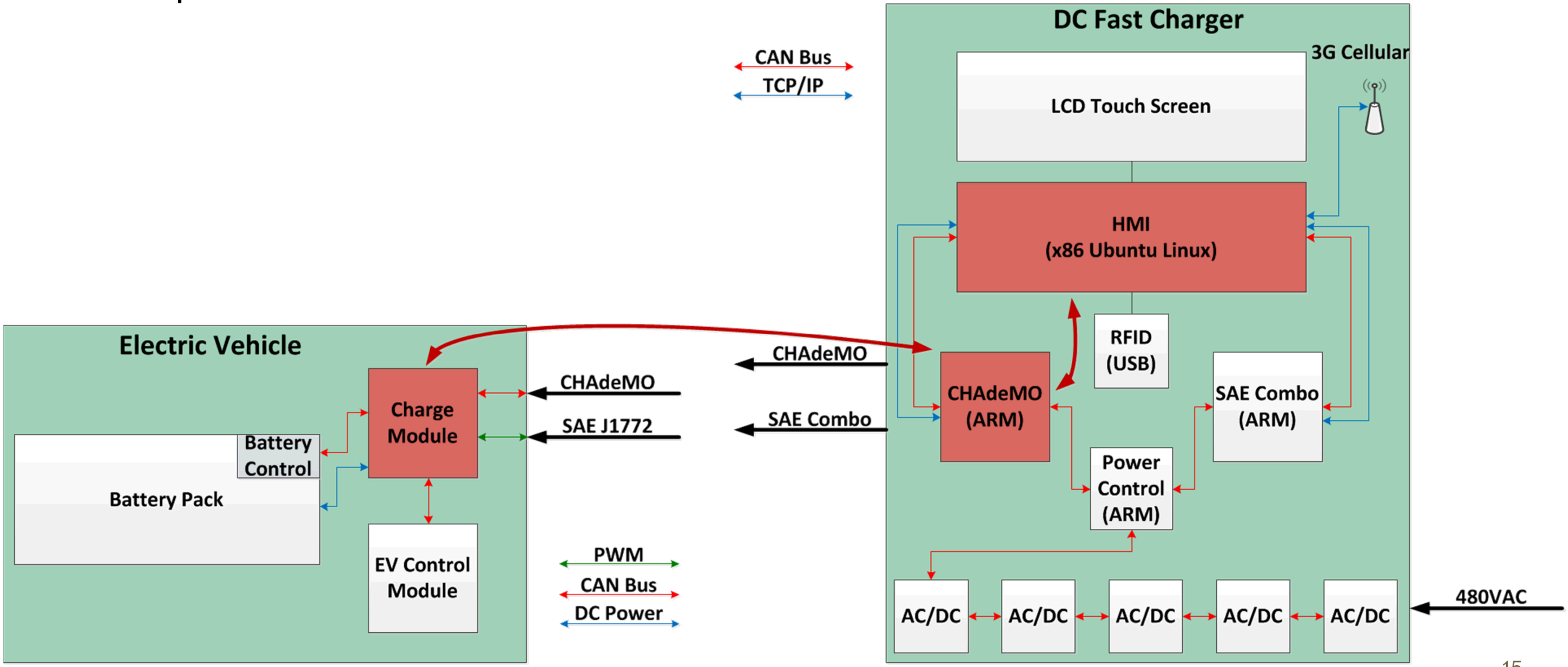
- Unable to directly control high speed switching inside the power electronics
    – Pwr. elec. modules control is independent from single control network
- Unable to over charge the EV
    – EV stopped the charge event:
        - Shut down command sent by EV
        - Open battery contactors

Our Lab Environment

- The actual hardware…

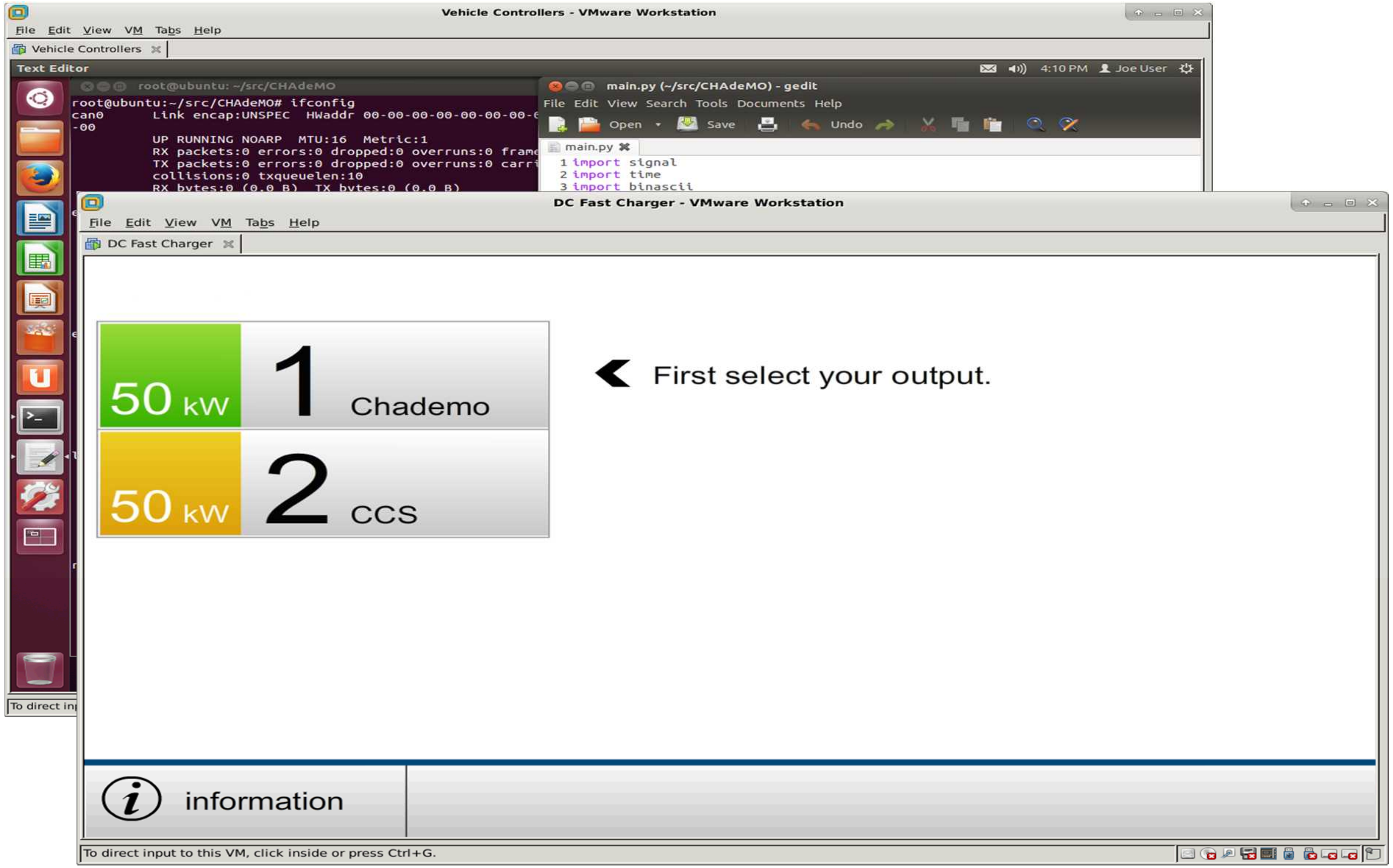
Attack Pathway

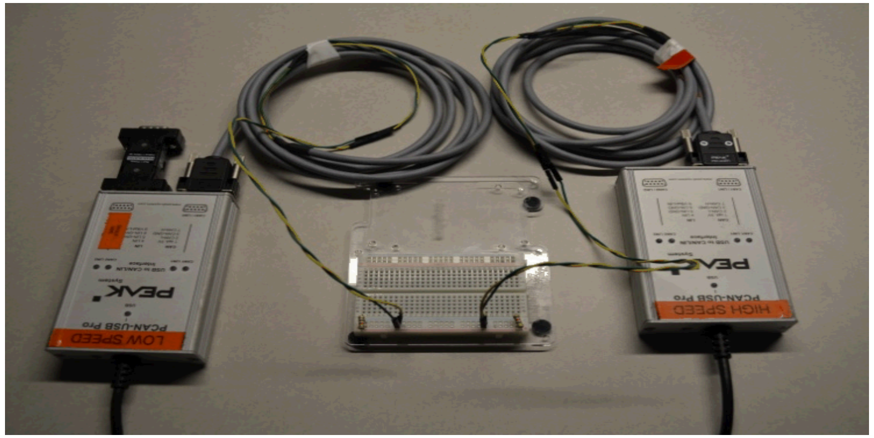
- Compromised PEV infects DCFC and vice versa



Virtual Environment

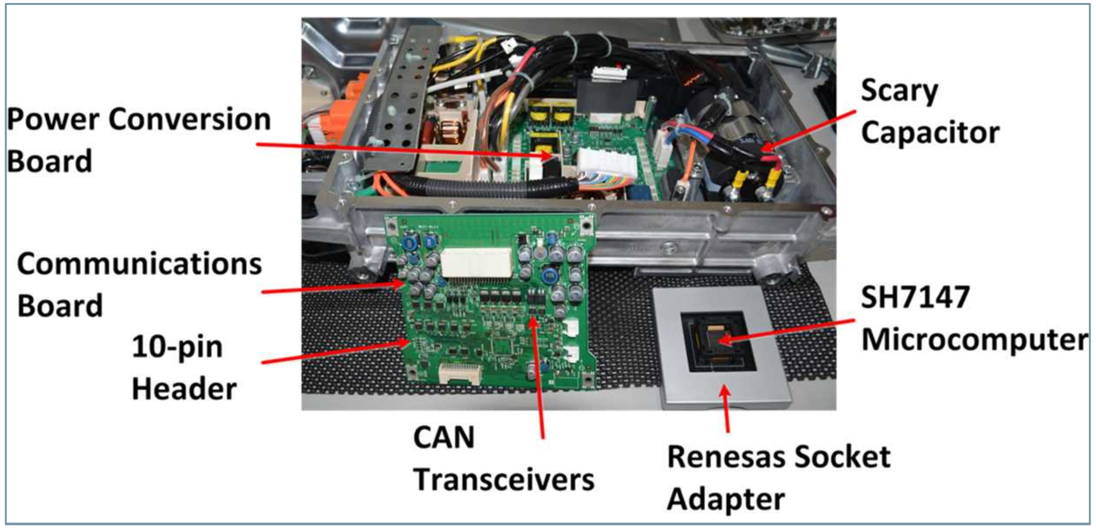
- For exploit development and testing…



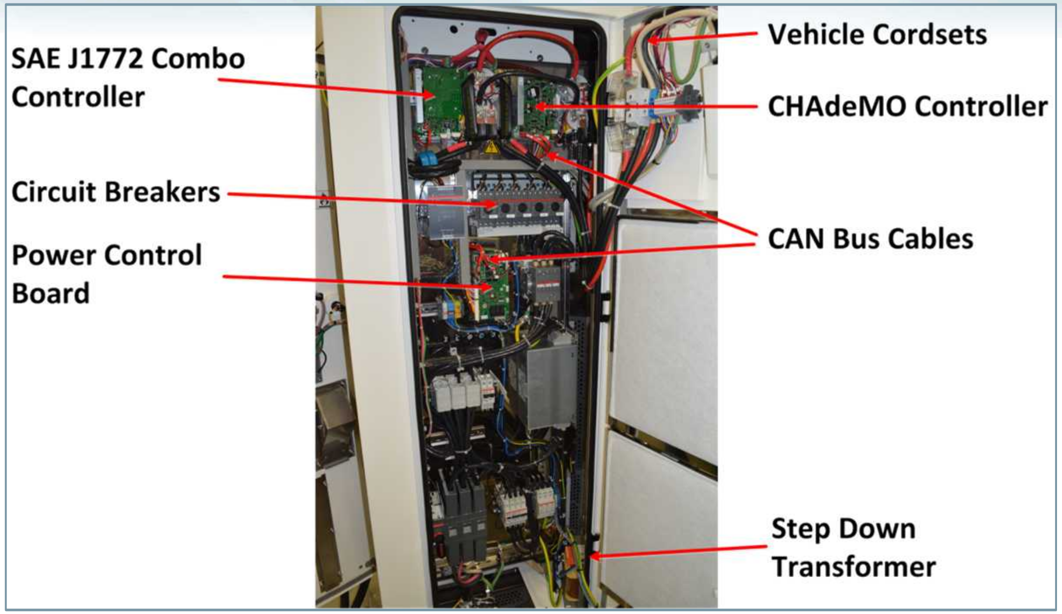


Scenario Components

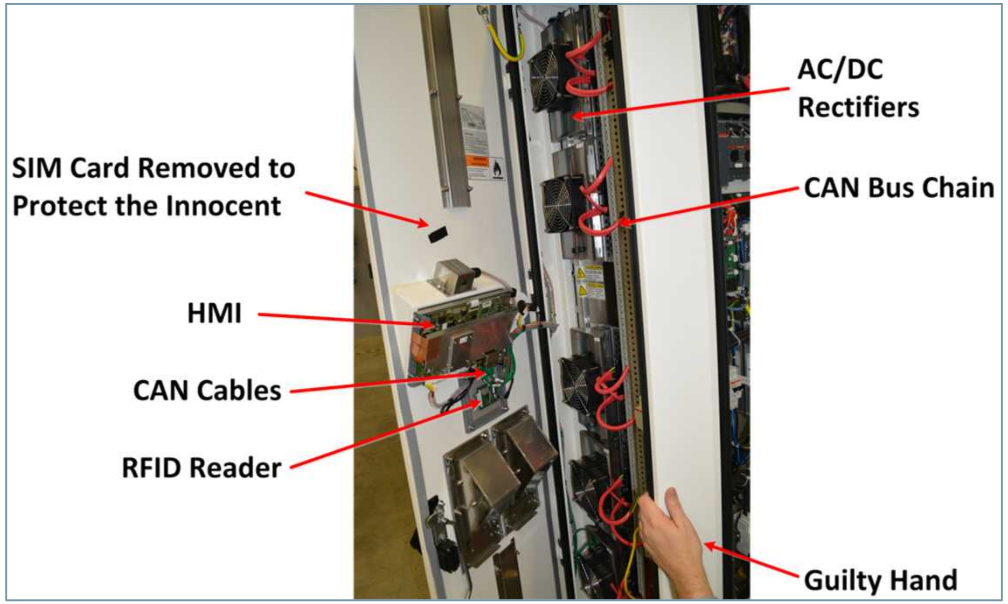
1. PEV Module



2. Vehicle Controllers



3. DCFC Local Server

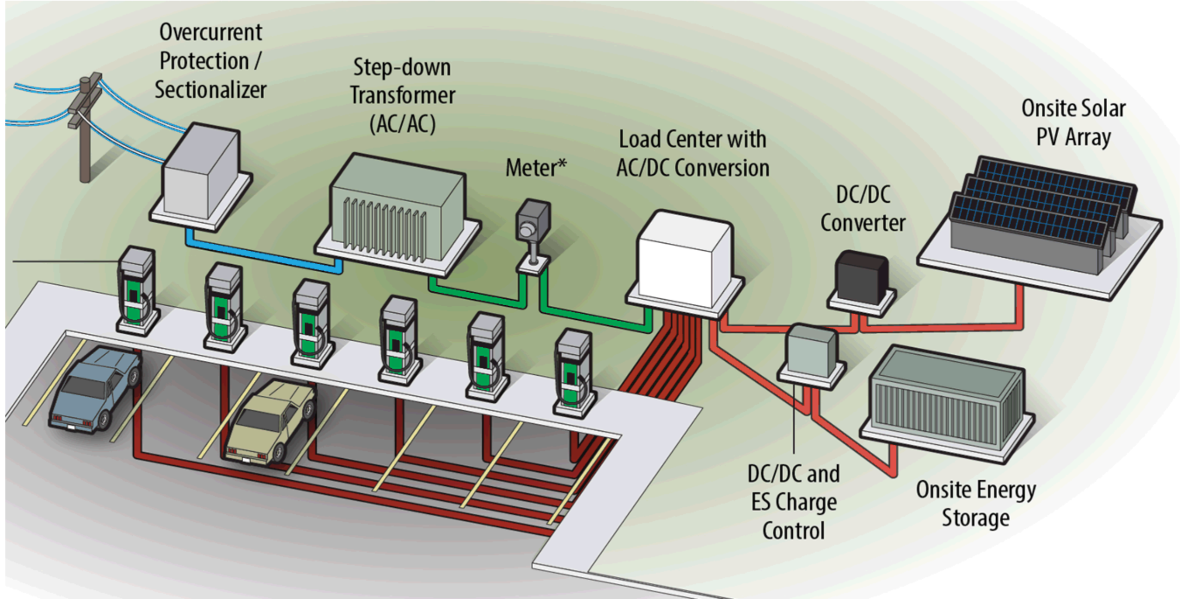


Scenario Components

1. PEV Charge Module
   - Successful removal of microcontroller from communications board
   - Successful extraction of firmware
     - Reverse engineering ECU firmware is painful
2. DCFC Vehicle Controllers
   - Successful extraction of firmware
   - Successful reflash of factory firmware via CAN from the HMI
3. DCFC Human Machine Interface (HMI)
   - Successful extraction of flash memory
     - Running Ubuntu Linux 12.0.4 LTS
   - All factory firmware located in the file system

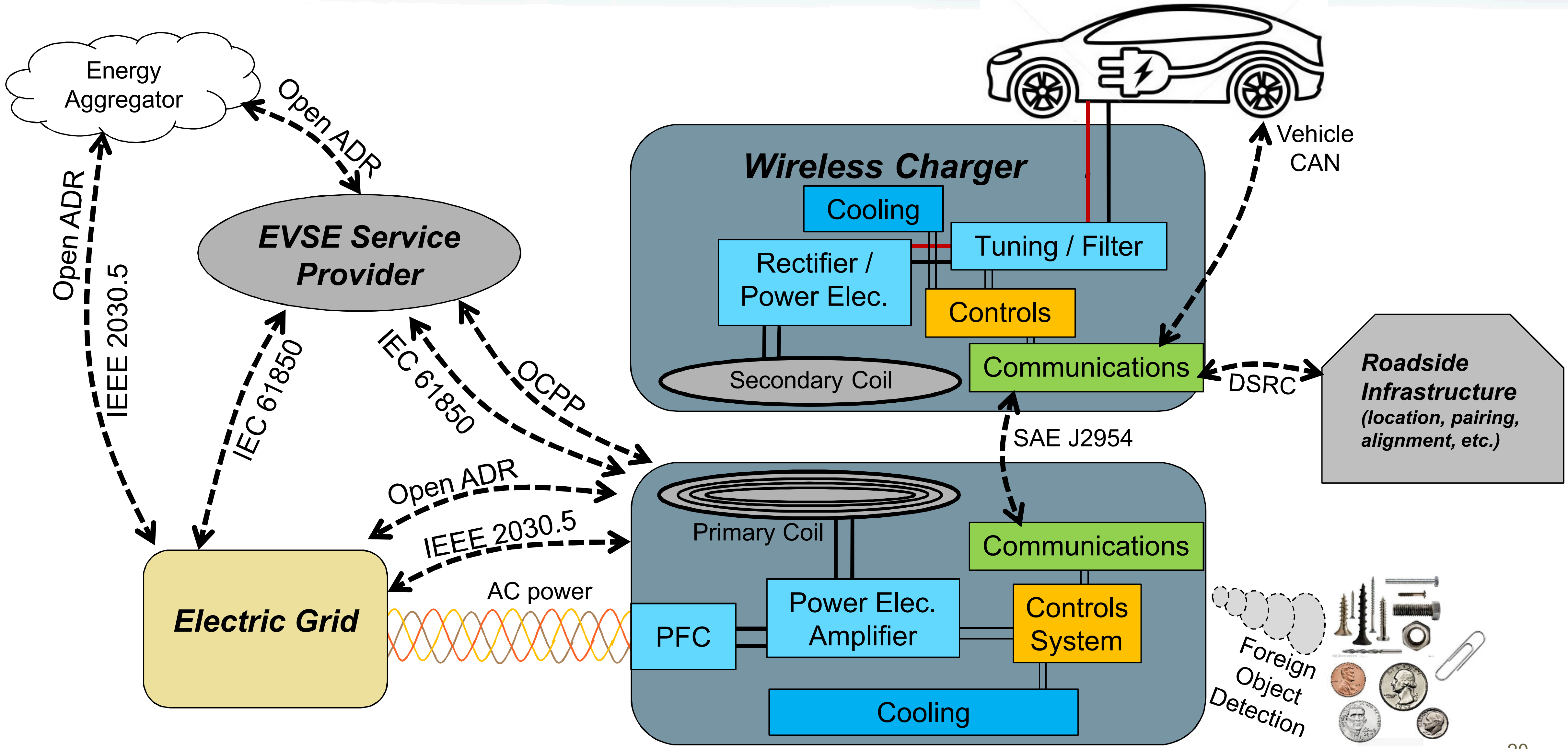
Potential Mitigation Solutions and Strategies

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



- Internal performance monitor
    - Electrical performance and characteristics
      - Monitor for change in performance
    - Monitor for communication anomalies

Wireless Power Transfer



INL's Focus:
Wireless Charging (WPT) &
Xtreme Fast Charging (XFC)

1. **XFC**: Higher power
   - 350 kW (500A / 1000VDC) or higher
   - Liquid cooled cable & connector
   - 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)
2. **WPT**: Higher system complexity & controls
   - Controls communication is wireless
     - from ground assembly to vehicle assembly
   - Foreign object detection system
   - Vehicle approach, pairing, and alignment system

INL is developing cyber consequence engineering methodology guideline for advanced charging systems

Photo source: Electrify America

Photo source: companycartoday.co.uk

Summary

- **Cyber security** of charging infrastructure
  - Critical to safety, reliability, and resiliency
  - INL is developing cyber-informed engineering methodologies and mitigation strategies
    - Extreme Fast Charging
    - Wireless Power Transfer
  - INL uses a Consequence driven, Cyber-informed Engineering (CCE) process

- **Vulnerabilities, risks, and threats**
  - Internal controls: Power electronics controls manipulation
  - External communications: multiple attack vectors / pathways
  - Increased complexity and charge power = increased risks and threats

- **Mitigation strategies and solutions**
  - Priority high consequence threats / risks
  - Utilize cyber informed engineering designs
  - Integrate inherent engineering solutions to minimize impact if system is compromised

Questions