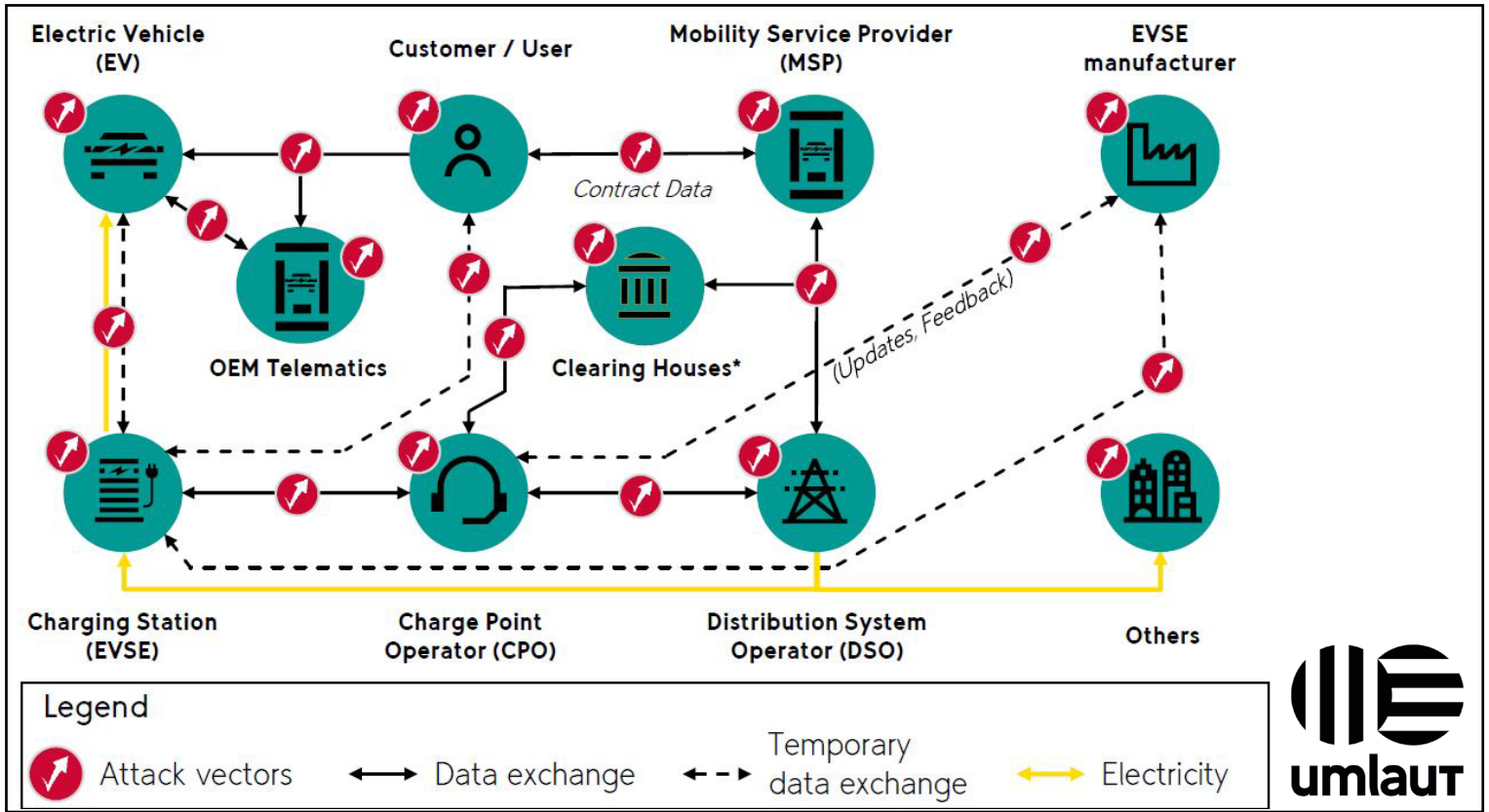
Cyber-Physical Security for High Power EV Charging Infrastructure

CERV2023: Feb. 6, 2023

INL/CON-23-70932

Vulnerabilities in EV Charging Infrastructure

- Lots of different stake holders
- Many potential attack vectors
- Inconsistent protocols and cybersecurity measures
- Most components are internet connected and allow mobile Apps interaction
- Often physical access protection can't be guaranteed



Electric Vehicles at Scale Consortium

U.S. DOE Vehicle Technologies Office

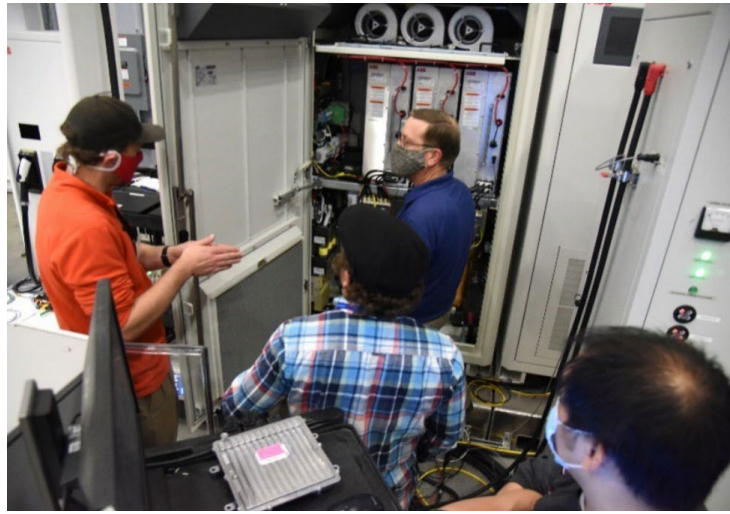
- Five Research Pillars in EVs@Scale
  - Smart Charge Management & Vehicle Grid Integration
  - High-Power Charging
  - Dynamic Wireless Power Transfer
  - **Cyber-physical Security Pillar**
  - Codes & Standards

- Cyber-physical Security Pillar focus areas:
  - Address evolving threats and challenges
  - Assess potential vulnerabilities
  - Develop mitigation solutions
  - Support training of the next generation of cybersecurity work force

EV Secure Architecture Laboratory Demonstration (EV SALaD)

U.S. DOE Cybersecurity, Energy Security, and Emergency Response (CESER) Office

- Demonstration of high-power DC charging cyber-physical security mitigation solutions
  - Detection and ranking of exploits and anomalous events
  - Response in accordance with severity of event to ensure resiliency
  - Recover back to optimal operational state
- Exploit Mitigation Demonstration
  - Power electronics controls manipulation
  - Liquid-cooled cable thermal management system exploit
  - Operational data manipulation
  - EVSE to EV communication exploits
  - EVSE to smart energy management communications manipulation



- INL is supporting CharIN Cybersecurity Task Force
  - Work package #3: Testing and evaluation (test events, hack-a-thons)

CHARIN

For more information at EV SALaD project:
www.energy.gov/ceser/articles/doe-ceser-leadership-attends-white-house-ev-cybersecurity-forum