Sandia National Laboratories

energy.sandia.gov

THREAT MODEL OF VEHICLE CHARGING INFRASTRUCTURE

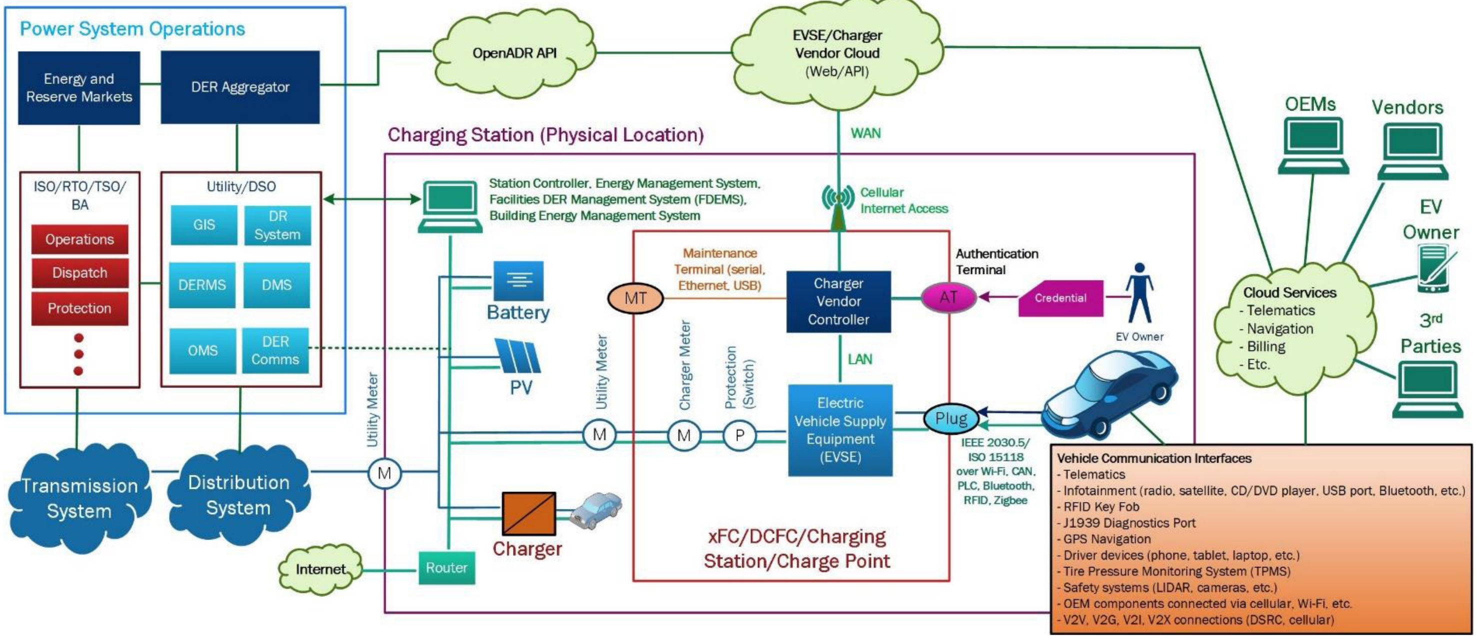
As electric vehicles (EVs) become more prominent on our roads and communities, the risk for cyber-attacks through vehicle charging stations rises too. These attacks threaten not only the electric grid, but personal privacy as well. Sandia National Laboratories is working with academia, government, and the EV and utility industries to better understand these risks and effective security solutions.

WHAT'S THE RISK?

Vehicle charging stations are convenient and affordable for drivers. Many businesses now offer employees free hook ups for their EVs. However, researchers have found that these stations can be a target for cyberattack because they lack proper security measures—physical security, EV owner and maintenance work authentication, and backhaul encryption—which could allow an adversary to steal personal information, change vehicle or charger firmware, or control a fleet's charging rates. Any malware or ransomware could attack the computer systems of vehicles, rendering them inoperable and even allowing access to drivers' personal and financial information. The graphic below shows how vehicles communicate with charging systems and third-party applications, and grid operators.

FRAMEWORKS

Sandia—in partnership with Pacific Northwest National Laboratory, Argonne National Laboratory, the US Department of Transportation, BTCPower and National Motor Freight Traffic Association—is working to address electric vehicle supply equipment (EVSE) cybersecurity by creating a cybersecurity threat model, and performing risk assessments of existing EVSE, so that automotive, charging and utility stakeholders can better protect their customers, vehicles and power systems. The result of this project will provide stakeholders with a strong, technological basis for securing vehicle charging infrastructure from cyber threats.


Power System Operations
Energy and Reserve Markets
DER Aggregator
ISO/RTO/TSO/BA
Operations
Dispatch
Protection
Utility/DSO
GIS
DR System
DERMS
DMS
OMS
DER Comms
Transmission System
Distribution System
Utility Meter
M
Internet
Router
OpenADR API
EVSE/Charger Vendor Cloud (Web/API)
WAN
Charging Station (Physical Location)
Station Controller, Energy Management System, Facilities DER Management System (FDEMS), Building Energy Management System
Cellular Internet Access
Battery
PV
Charger
Utility Meter
M
Charger Meter
M
Protection (Switch)
P
MT
Maintenance Terminal (serial, Ethernet, USB)
Charger Vendor Controller
LAN
Electric Vehicle Supply Equipment (EVSE)
Authentication Terminal
AT
Credential
EV Owner
Plug
IEEE 2030.5/ ISO 15118 over Wi-Fi, CAN, PLC, Bluetooth, RFID, Zigbee
xFC/DCFC/Charging Station/Charge Point
OEMs
Vendors
EV Owner
3rd Parties
Cloud Services
- Telematics
- Navigation
- Billing
- Etc.
Vehicle Communication Interfaces
- Telematics
- Infotainment (radio, satellite, CD/DVD player, USB port, Bluetooth, etc.)
- RFID Key Fob
- J1939 Diagnostics Port
- GPS Navigation
- Driver devices (phone, tablet, laptop, etc.)
- Tire Pressure Monitoring System (TPMS)
- Safety systems (LIDAR, cameras, etc.)
- OEM components connected via cellular, Wi-Fi, etc.
- V2V, V2G, V2I, V2X connections (DSRC, cellular)

EDUCATION IS KEY

It has been projected that globally, over the course of the next decade, the number of EVs will increase by tens of millions. This means that as the number of vehicles grows, so will the number of available charging stations these vehicles will need to use.

At this time, there is no comprehensive EV cybersecurity approach and the industry has only adopted limited best practices. One of the project's main goals is to educate key industry leaders about the risks posed, and help them understand their role in providing grid security and resilience.

Sustained cybersecurity leadership and stakeholder commitment are necessary to continuously improve EV charging equipment and networks, build effective standards, and support government and commercial R&D efforts.

THREAT MODELING

To enumerate threats in a testing environment, researchers at the national laboratories used the STRIDE threat modeling methodology to determine potential vulnerabilities. This includes: communication and control interface with the EV's battery management system, the controls that manage power flow to vehicle batteries, utility communications and grid operator control, and financial communications. This threat model was further informed by red team assessments of DC fast chargers and extreme fast chargers (xFCs).

The research team also investigated how the power system, vehicles and other services are impacted by coordinated cyberattacks on charging systems at the both the transmission and distribution levels. Based on these consequences, mitigations can be prioritized based on the potential risk to critical US infrastructure. The team expects that the results of the threat model will be the foundation for improvements to cybersecurity of EVs, EVSEs, and other support infrastructure.

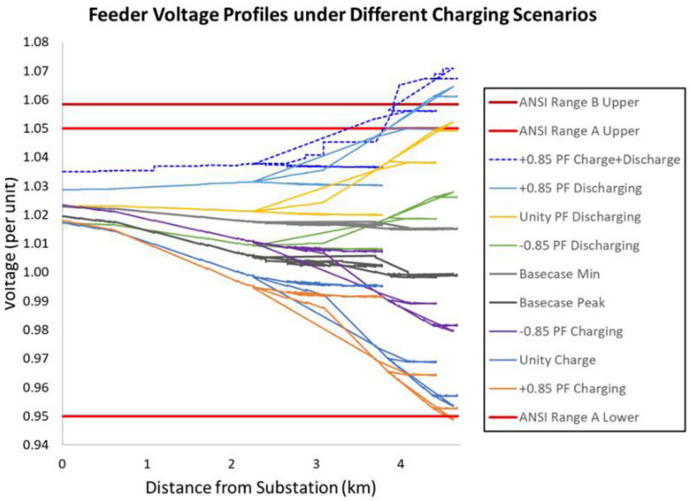


Figure: Distribution system voltage impact from coordinated EV charging and discharging with 2.25 MW EVSEs.

CONTACT:

Jay Johnson
Principal Investigator
jjohns2@sandia.gov
(505) 284-9586

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-13532 O