Cybersecurity: Securing Vehicle Charging Infrastructure—Consequence Analysis and Threat Assessment

Rick Pratt, Principal Investigator

Pacific Northwest National Laboratory

Project ID#: elt263

This presentation does not contain any proprietary, confidential, or otherwise restricted information.

Overview

Timeline:

- FY19 (10/1/18-9/30/2019)
- FY20 (10/1/19-9/30/2020)
  - Currently, 50% complete

Barriers

- Strategy—critical infrastructure risk mitigation
- Enabling Technologies—interoperability
- Codes and Standards—lack of security

Budget

- FY19 $325k
- FY20 $325k

Partners

- Argonne National Laboratory, Sandia National Laboratories
- Florida Power & Light—in progress

Relevance: Cyber-Physical Security of Electric Vehicles and Extreme Fast Charging while Protecting Our Critical Infrastructure

The PNNL team is investigating how the power system, vehicles, and other services are affected by cybersecurity vulnerabilities introduced by charging systems, communications to, from, or through charging stations, while considering specific barriers and challenges:

- Strategy: Determine the impact of vulnerabilities on power system operations, transportation systems, original equipment manufacturers, and vehicle owners and how these entities can work together to mitigate cyber risk to critical infrastructure
- Enabling Technologies: Communication and control interface to the electric vehicles' (EVs') charging infrastructure
- Codes and Standards: SAE J1772, NISTR 7628, ISO/IEC 15118-2 are some of the standards that were included in this work

This project is:

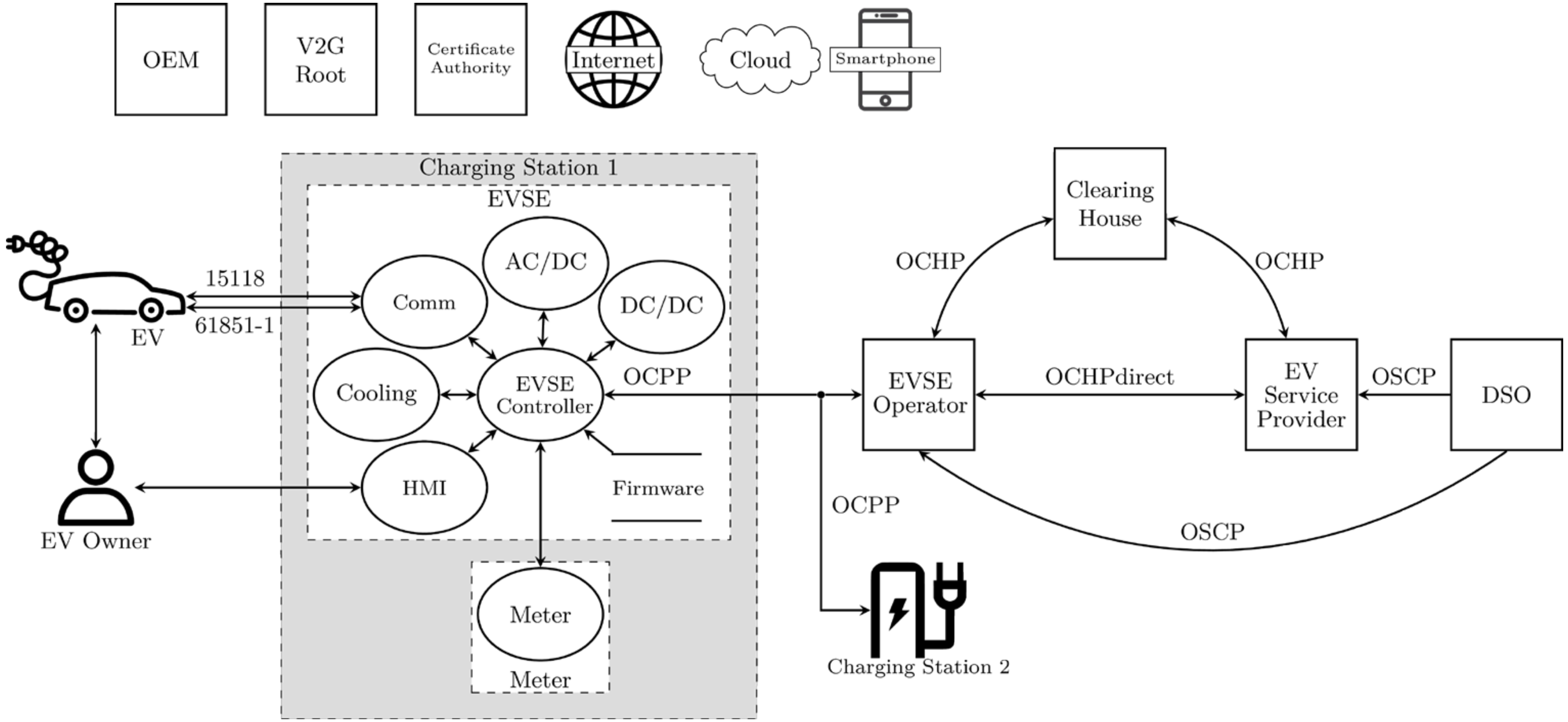
- Assessing the consequences of charging infrastructure on transmission systems
- Creating a threat assessment model
- Determining how vulnerabilities map to grid security

PNNL's Research Focuses on a Two-Pronged Approach

1. Threat Assessment: Develop and refine a characterization of electrical vehicles, charging systems, and supporting protocols and processes to identify areas of undesirable operation (e.g., modify extreme fast charging [xFC] charging ramp rate or EV-initiated disconnect) to enhance threat modeling and consequence analyses efforts.
   - To understand communications, develop flow diagrams from a charging infrastructure-grid perspective
   - Identify threats and their consequences to xFC infrastructure, grid, and transportation
2. Consequence Analysis: Develop and refine US power grid Consequence Analysis models and simulations focusing on Transmission System impacts of EVs' xFC. In particular:
   - Assess load drop at single and multiple locations
   - Investigate oscillating load at single and multiple locations

Threat Assessment: Document Communication Flow to Grid

15118-Centric Infrastructure Model



Developing first of its kind 15118 EV Threat model:

1. Identify consequences to energy and transportation sectors
2. Define xFC security objectives: privacy, power system, transportation system, financial transactions, etc.
3. Revise communication and energy flow diagrams
4. Identify vulnerabilities and threats using a modified STRIDE methodology
5. Identify controls and mitigations to address threats

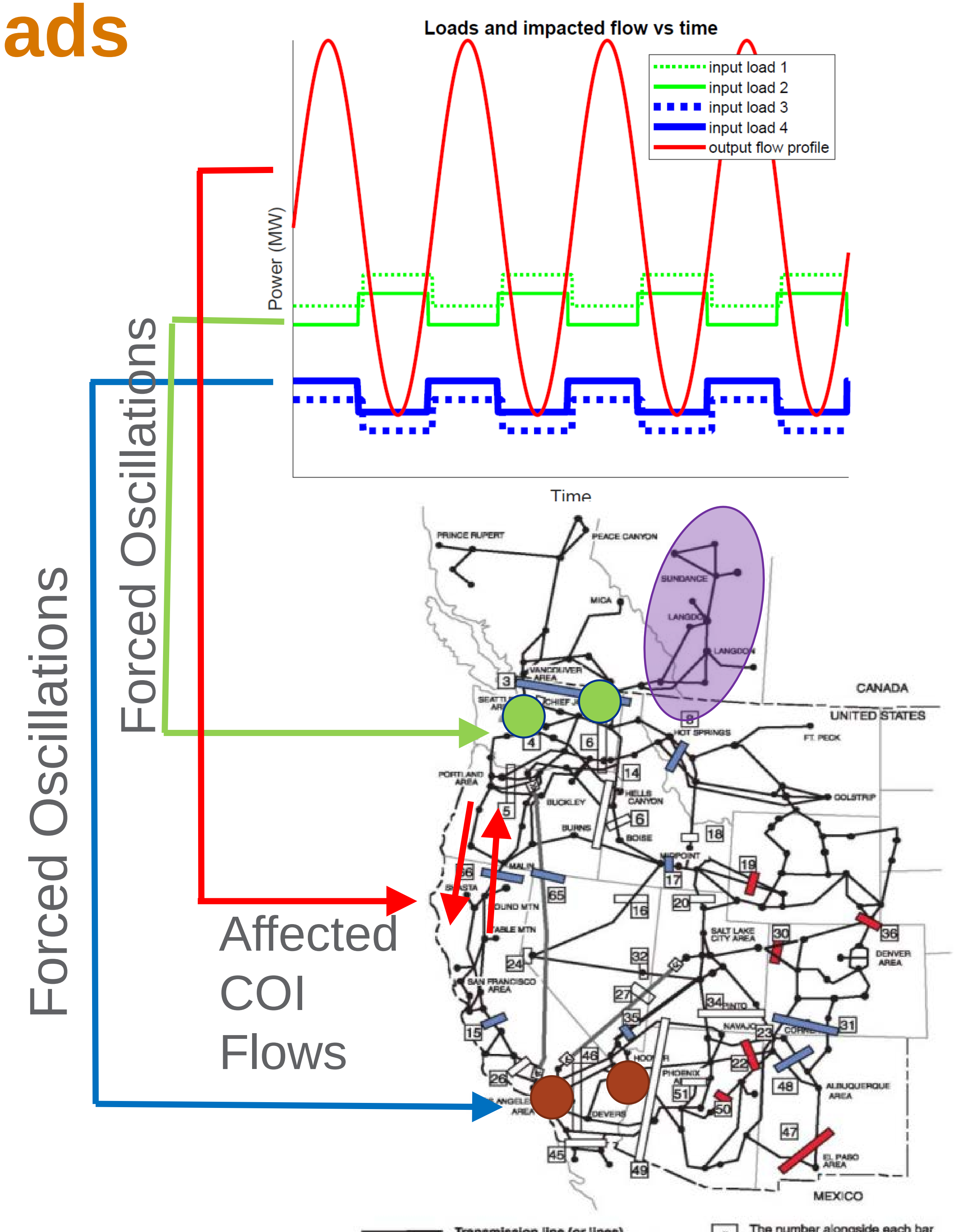
Consequence Analysis: Loads and Impacts over Time

Research Question: Can manipulating EV load induce inter-area oscillations in the full Western Interconnection (WECC) model?

Approach using multiple models:

- Used Modal/Eigen analysis to determine resonant frequencies
- Conducted frequency response to select most affected locations
- (For comparison, also assessed synthetic ERCOT model)

Results: Loads of 500 MW intelligently distributed across WECC causing >1500 MW of power fluctuations on California Oregon Intertie (COI).



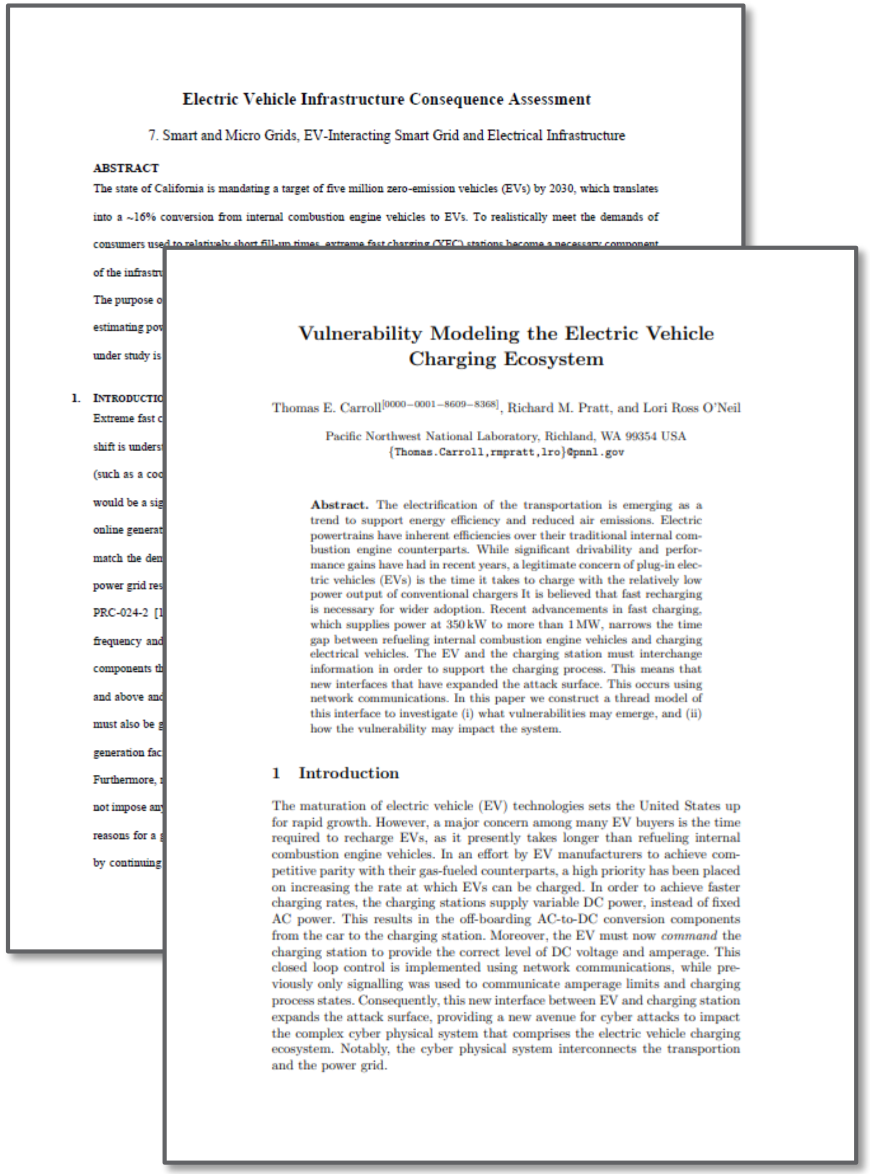
Forced Oscillations

Forced Oscillations

Affected COI Flows

Technical Accomplishments and Progress to Date

- Our novel modeling and simulation work showed that current controls of the US electric grid prevent adverse effects due to xFC oscillatory load manipulations.
- No prior load drop studies have addressed xFC's effect to the US grid.
- Submitted abstract titled "Electric Vehicle Infrastructure Consequence Assessment" to 2020 IEEE Transportation Electrification Conference.
- Preparing abstract for 2020 ES-CAR (Embedded Security in Cars).
- Developed new WECC and ERCOT model simulations, not previously related to xFC charging to calculate effects on the grid through automation of contingency generation.
- Developed new cyber threat models to xFC communications pathways and infrastructure to identify vulnerabilities and consequences.
- Work has been peer reviewed by experienced PNNL staff. Next reviews will be with industry and other labs.



Electric Vehicle Infrastructure Consequence Assessment

7. Smart and Micro Grids, EV-Interacting Smart Grid and Electrical Infrastructure

ABSTRACT

The state of California is mandating a target of five million zero-emission vehicles (EVs) by 2030, which translates
into a ~16% conversion from internal combustion engine vehicles to EVs. To realistically meet the demands of
consumers used to relatively short fill-up times, extreme fast charging (XFC) stations become a necessary component
of the infrastru
The purpose o
estimating pow
under study is

1. INTRODUCTIO
Extreme fast c
shift is underst
(such as a coo
would be a sig
online generat
match the dem
power grid res
PRC-024-2 [1
frequency and
components th
and above and
must also be g
generation fac
Furthermore, r
not impose any
reasons for a g
by continuing

Vulnerability Modeling the Electric Vehicle Charging Ecosystem

Thomas E. Carroll[0000−0001−8609−8368], Richard M. Pratt, and Lori Ross O'Neil

Pacific Northwest National Laboratory, Richland, WA 99354 USA
{Thomas.Carroll,rmpratt,lro}@pnnl.gov

Abstract. The electrification of the transportation is emerging as a trend to support energy efficiency and reduced air emissions. Electric powertrains have inherent efficiencies over their traditional internal combustion engine counterparts. While significant drivability and performance gains have had in recent years, a legitimate concern of plug-in electric vehicles (EVs) is the time it takes to charge with the relatively low power output of conventional chargers It is believed that fast recharging is necessary for wider adoption. Recent advancements in fast charging, which supplies power at 350 kW to more than 1 MW, narrows the time gap between refueling internal combustion engine vehicles and charging electrical vehicles. The EV and the charging station must interchange information in order to support the charging process. This means that new interfaces that have expanded the attack surface. This occurs using network communications. In this paper we construct a thread model of this interface to investigate (i) what vulnerabilities may emerge, and (ii) how the vulnerability may impact the system.

1 Introduction

The maturation of electric vehicle (EV) technologies sets the United States up for rapid growth. However, a major concern among many EV buyers is the time required to recharge EVs, as it presently takes longer than refueling internal combustion engine vehicles. In an effort by EV manufacturers to achieve competitive parity with their gas-fueled counterparts, a high priority has been placed on increasing the rate at which EVs can be charged. In order to achieve faster charging rates, the charging stations supply variable DC power, instead of fixed AC power. This results in the off-boarding AC-to-DC conversion components from the car to the charging station. Moreover, the EV must now *command* the charging station to provide the correct level of DC voltage and amperage. This closed loop control is implemented using network communications, while previously only signalling was used to communicate amperage limits and charging process states. Consequently, this new interface between EV and charging station expands the attack surface, providing a new avenue for cyber attacks to impact the complex cyber physical system that comprises the electric vehicle charging ecosystem. Notably, the cyber physical system interconnects the transportion and the power grid.

Intra-Lab and Industry Collaboration

- Working closely with national labs (SNL and ANL) as part of the Securing Vehicle Charging Infrastructure project
- Presented EV Flow diagram work at 2019 Cyber-Security of On-Road Transportation for peer review and comment, which was used in this project
- Work presented to Grid Interaction Tech Team
- Regular member and contributor to EPRI (nonprofit organization) working group
- Leveraging GMLC 62 efforts and related prior VTO work for this project
- Scheduled presenter at EVS33 World Electric Vehicle Symposium & Expo June 2020
- Florida Power & Light (industry—NDA in process)

Next Steps for FY20 and Beyond

Threat Assessment:

- (FY20) Develop and apply mitigation strategies to identified threats
- (FY21) Verification and validation of approaches by peers and industry

Consequence Analysis:

- (FY20) Investigate sensitivity of response to:
  - Forced oscillation noise (phase and frequency of load oscillations)
  - Load distribution
- (FY20) Investigate where load models and charging profile modifications may be made to better represent EVs
- (FY21) Integrate Threat Assessment and Consequence Analysis approaches into a high-fidelity, grid-scale analysis for system-level protection of charging
- (Beyond) Greater integration with transportation sector to help it understand effects on grid infrastructure capacity, planning, and security

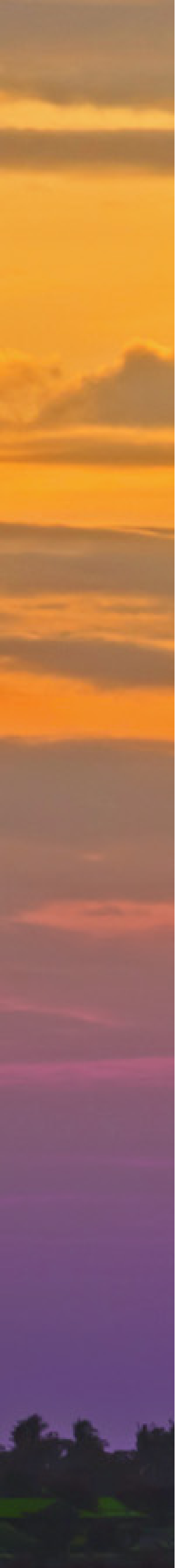
Any proposed work is subject to change based on funding levels.

Summary

FY	Research Area	Impact
2019	Load drop studies	Quantifies grid frequency impact due to potential simultaneous EV load disconnection events.
2019	STRIDE Threat Modeling	STRIDE analysis of processes revealed significant numbers of interconnected cyber-physical systems.
2020	Oscillatory Load Studies	Identifies critical scenarios and effects for advanced EV load control.
2020	Consequence Threat Modeling	Threat modeling using consequences enabled STRIDE analysis of threats and effective mitigation approaches.
2021	Verify and Validate Threat models with industry partners	Expert review improves/enhances models/methods.

Backup Slides

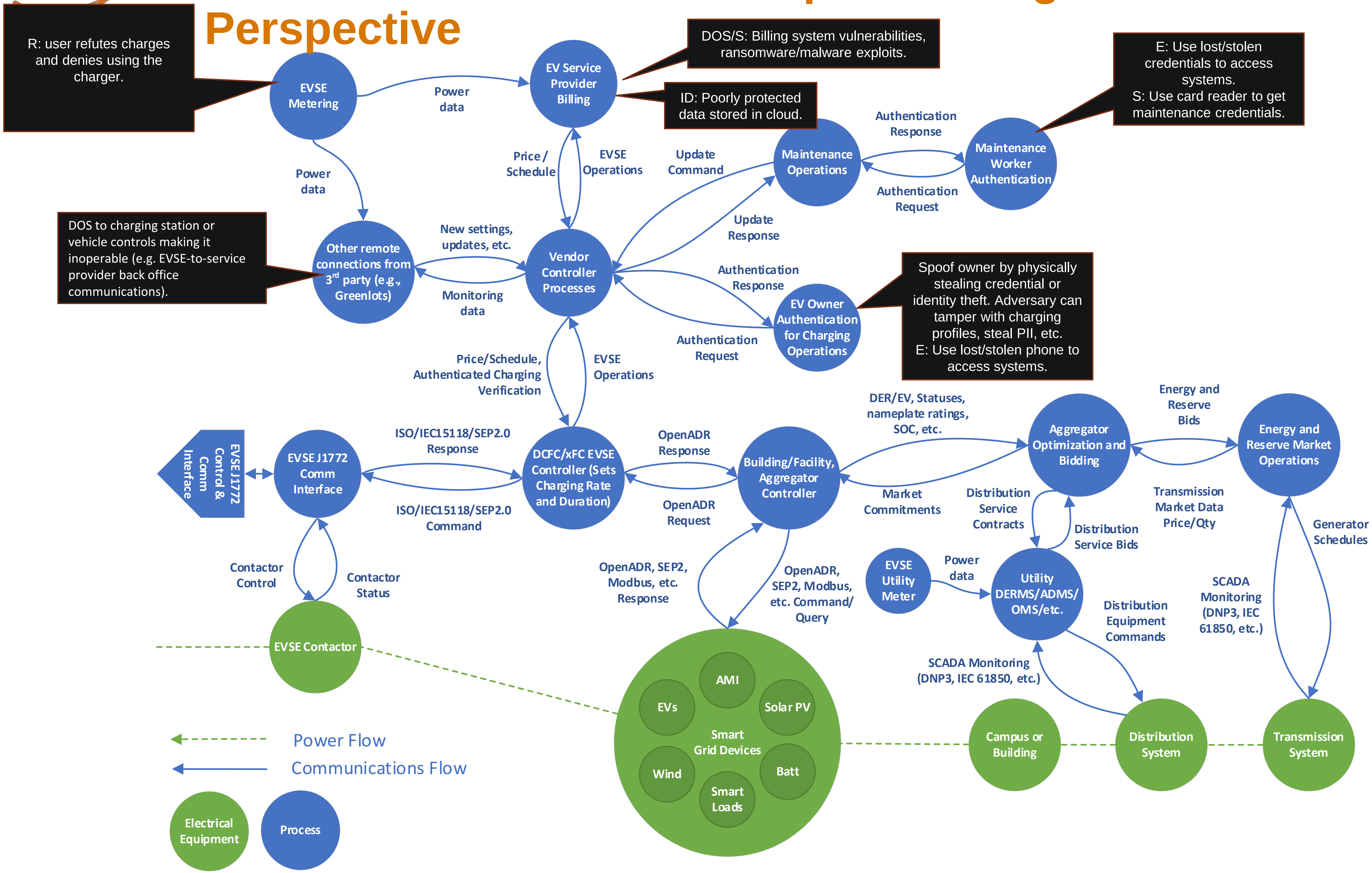
PNNL is operated by Battelle for the U.S. Department of Energy



FY20 Milestones

Milestone Name/Description	Criteria	End Date	Type
1. EV Cyber-Physical Weakness Characterization Approach - Characterize EVs, charging systems, and supporting protocols to identify cyber-physical weaknesses that may lead to adverse conditions (e.g., modify xFC charging ramp rate, initiate coordinated plug-in EV disconnects, etc.). The results will inform threat and consequence analysis.	Develop EV Cyber-Physical Weakness Characterization Approach, vet the approach with industry, and deliver white paper describing approach and outcomes.	9/30/2020	Annual Milestone (Regular)
1. EV Consequence Analysis - Extend EV xFC of US power grid Consequence Analysis to incorporate microgrid, coordinated charging changes, and network communications.	Project report and a publicly disseminated paper documenting a detailed analysis of consequences to power systems, transportation, and other related critical infrastructure.	9/30/2020	Annual Milestone (Regular)

Threat Assessment: Develop Flow Diagram from Grid Perspective



R: user refutes charges and denies using the charger.

DOS/S: Billing system vulnerabilities, ransomware/malware exploits.

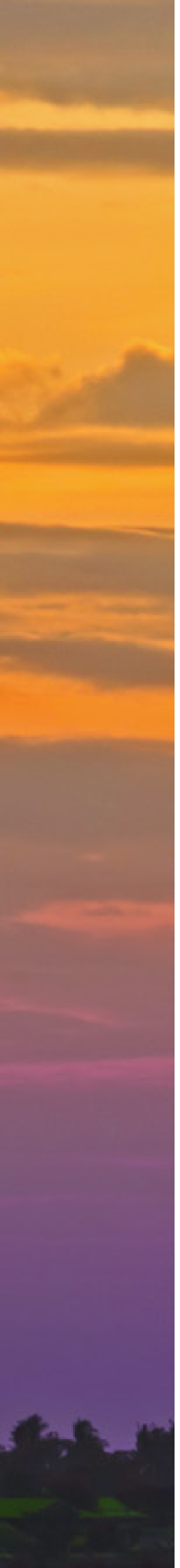
ID: Poorly protected data stored in cloud.

E: Use lost/stolen credentials to access systems.
S: Use card reader to get maintenance credentials.

DOS to charging station or vehicle controls making it inoperable (e.g. EVSE-to-service provider back office communications).

Spoof owner by physically stealing credential or identity theft. Adversary can tamper with charging profiles, steal PII, etc.
E: Use lost/stolen phone to access systems.

EVSE Metering
Power data
EV Service Provider Billing
Power data
Price / Schedule
EVSE Operations
Update Command
Maintenance Operations
Authentication Response
Authentication Request
Maintenance Worker Authentication
Other remote connections from 3rd party (e.g., Greenlots)
New settings, updates, etc.
Monitoring data
Vendor Controller Processes
Update Response
Authentication Response
Authentication Request
EV Owner Authentication for Charging Operations
Price/Schedule, Authenticated Charging Verification
EVSE Operations
EVSE J1772 Control & Comm Interface
EVSE J1772 Comm Interface
ISO/IEC15118/SEP2.0 Response
ISO/IEC15118/SEP2.0 Command
DCFC/xFC EVSE Controller (Sets Charging Rate and Duration)
OpenADR Response
OpenADR Request
Building/Facility, Aggregator Controller
DER/EV, Statuses, nameplate ratings, SOC, etc.
Market Commitments
Aggregator Optimization and Bidding
Energy and Reserve Bids
Energy and Reserve Market Operations
Transmission Market Data Price/Qty
Distribution Service Contracts
Distribution Service Bids
Generator Schedules
Contactor Control
Contactor Status
EVSE Contactor
OpenADR, SEP2, Modbus, etc. Response
OpenADR, SEP2, Modbus, etc. Command/ Query
EVSE Utility Meter
Power data
Utility DERMS/ADMS/ OMS/etc.
Distribution Equipment Commands
SCADA Monitoring (DNP3, IEC 61850, etc.)
SCADA Monitoring (DNP3, IEC 61850, etc.)
AMI
EVs
Solar PV
Smart Grid Devices
Wind
Batt
Smart Loads
Campus or Building
Distribution System
Transmission System
Power Flow
Communications Flow
Electrical Equipment
Process



Pacific Northwest
NATIONAL LABORATORY

Threat Assessment: Model Progress of EV Charging Focusing on Grid Impacts

Findings:

- STRIDE’s narrow focus limits understanding of significant consequences
- Understanding consequences helped us identify relevant threats
- Energy sector cannot mitigate every xFC threat on its own
- All xFC parties need strong, coordinated cyber practices

Work to Date:

- Investigated the PKI and security of ISO/IEC 15118-2
- Developed power and communication flows for 15118-centric infrastructure
- Developed modified STRIDE to accommodate cyber-physical systems

Deliverable:

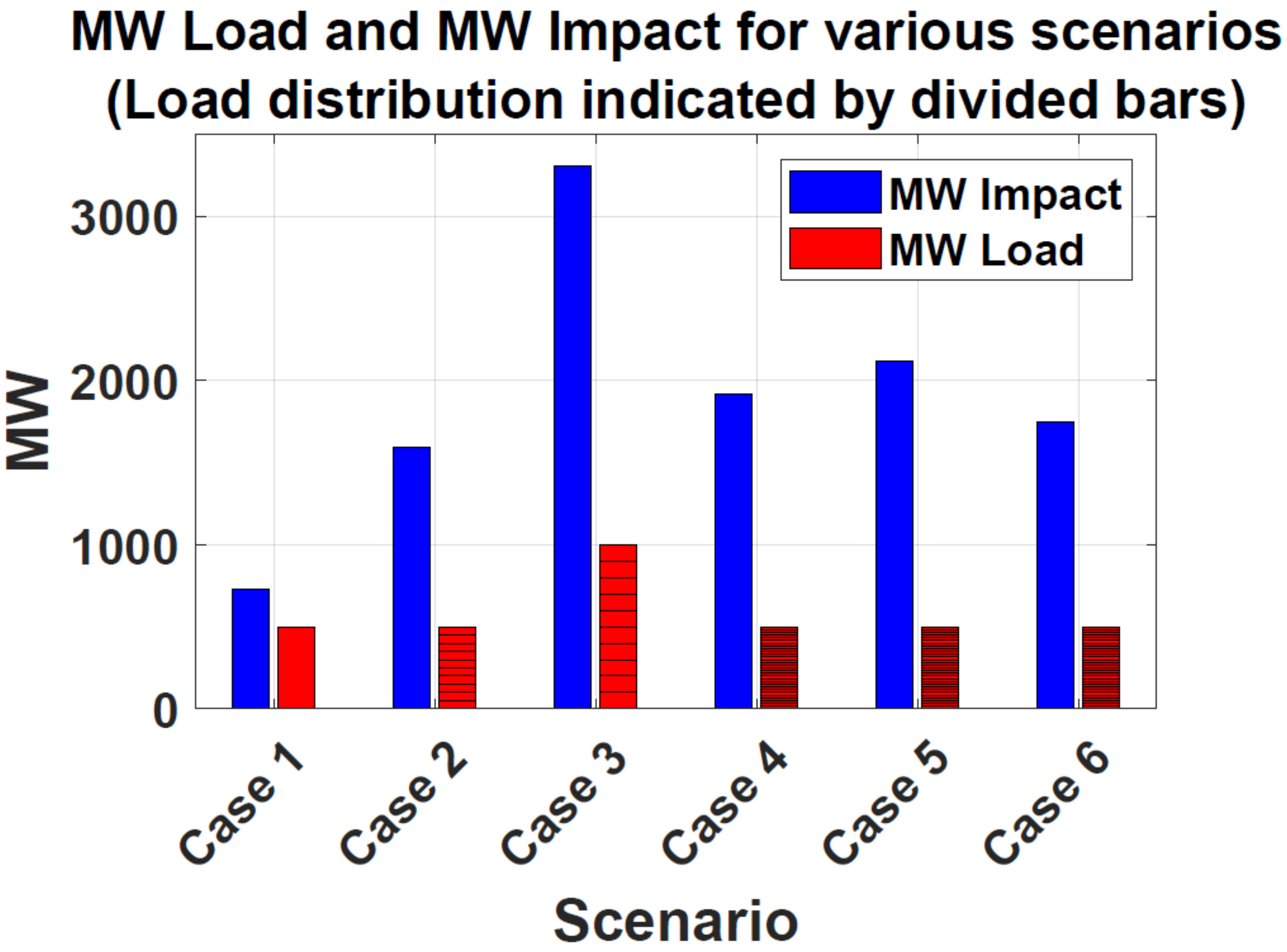
- Threat consequence report publication target date: 9/2020

STRIDE Threat	Desired Property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Consequence Analysis: Results from Load Oscillations

Evaluated 6 scenarios:

- Case I :
  - Single 500 MW controllable load
  - Single location chosen using knowledge of system
- Case 2 :
  - 500 MW controllable load distributed at 10 different buses
  - Location chosen using frequency response methods.
  - Loads are oscillating in phase with the system oscillation
- Cases 3-6 :
  - Additional sensitivities using distributed loads


MW Load and MW Impact for various scenarios
(Load distribution indicated by divided bars)
MW Impact
MW Load
MW
Case 1
Case 2
Case 3
Case 4
Case 5
Case 6
Scenario