Pacific Northwest
NATIONAL LABORATORY

Resilient Electric Vehicle Charging Infrastructure

June 29, 2022

Thomas E. Carroll
Pacific Northwest National Laboratory

U.S. DEPARTMENT OF ENERGY BATTELLE

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

AV Perspective

- On-road autonomous vehicles are electrified platforms…
- And will require reliable charging infrastructure

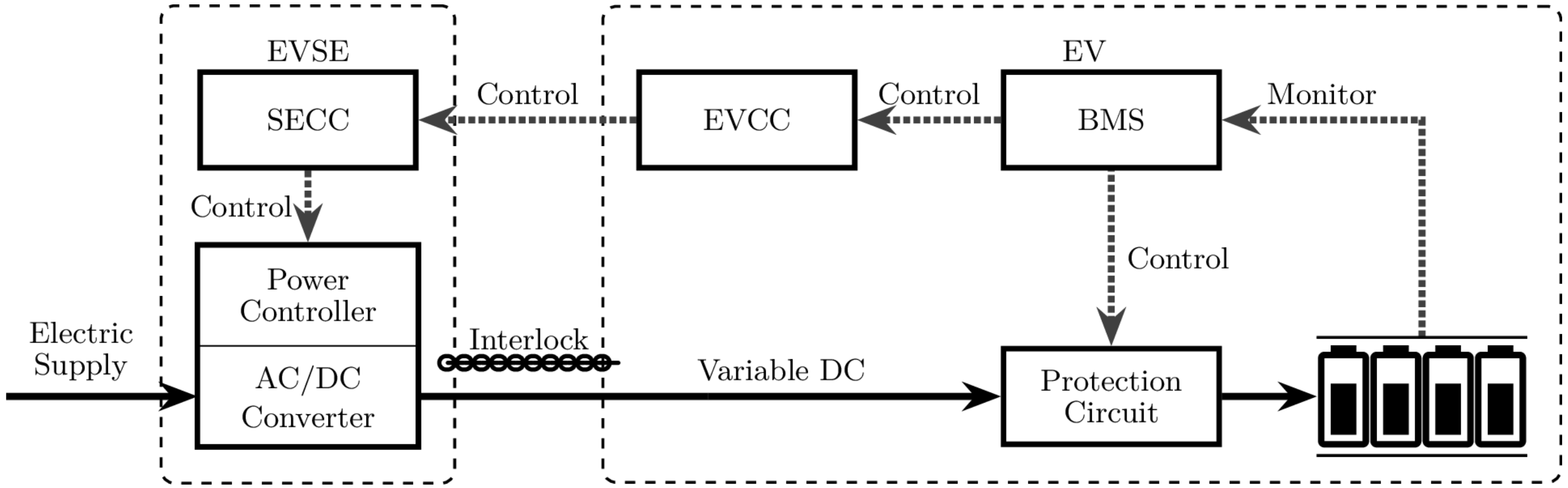
Pacific Northwest
NATIONAL LABORATORY

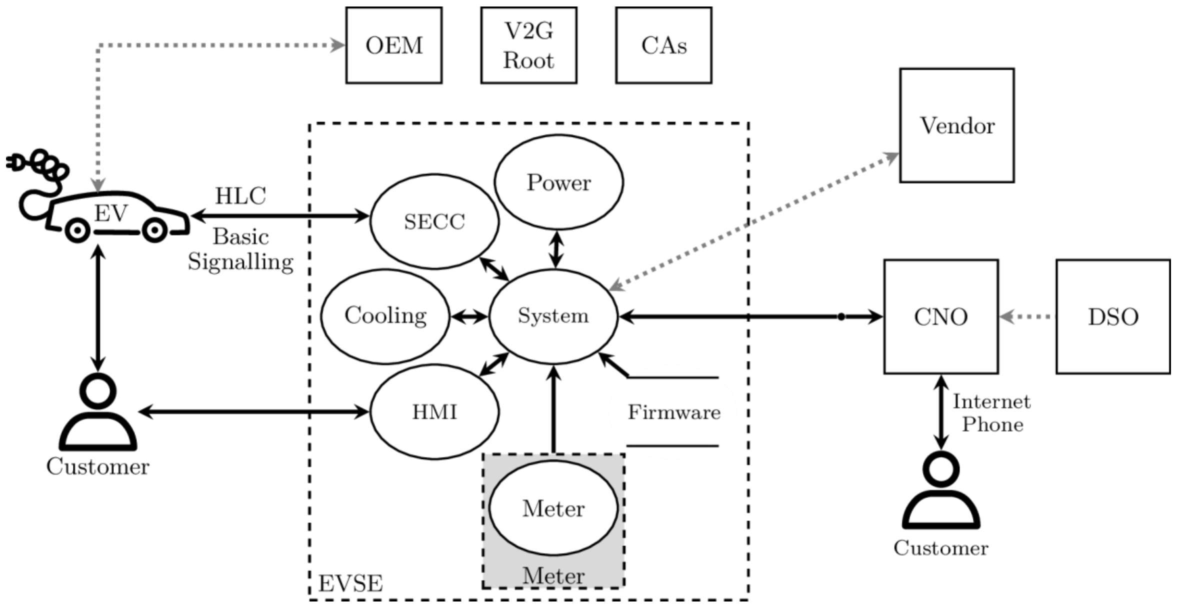
Backdrop

- States mandating zero emission transportation
- The White House is leading the development of a national charging network of along highways and in communities
- DOE is investing to decarbonify transportation and remove barriers to ZEV/EV adoption
  - hydrogen production & distribution; powertrains, batteries & materials; power electronics & chargers; grid integration, architecture, site selection & deployments

- Vehicles with ranges of 250mi → 500mi
- High power charging closing the refueling time gap, <20min → <10min
- Wireless power transfer becoming practical, >90percent efficient

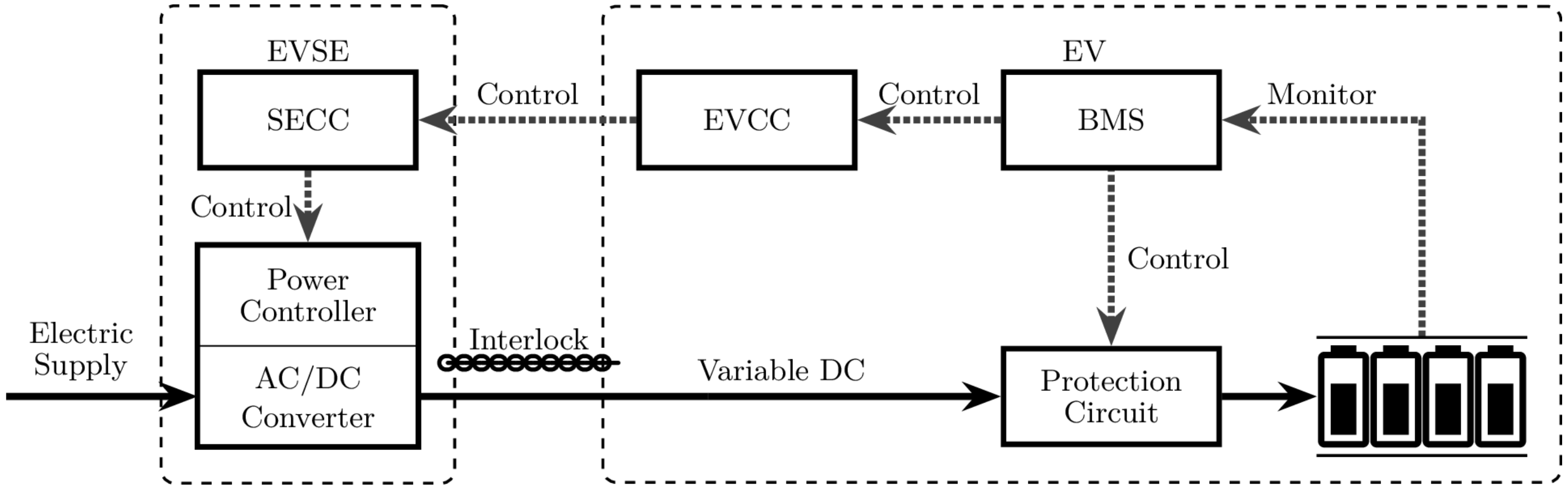
Charging Basics

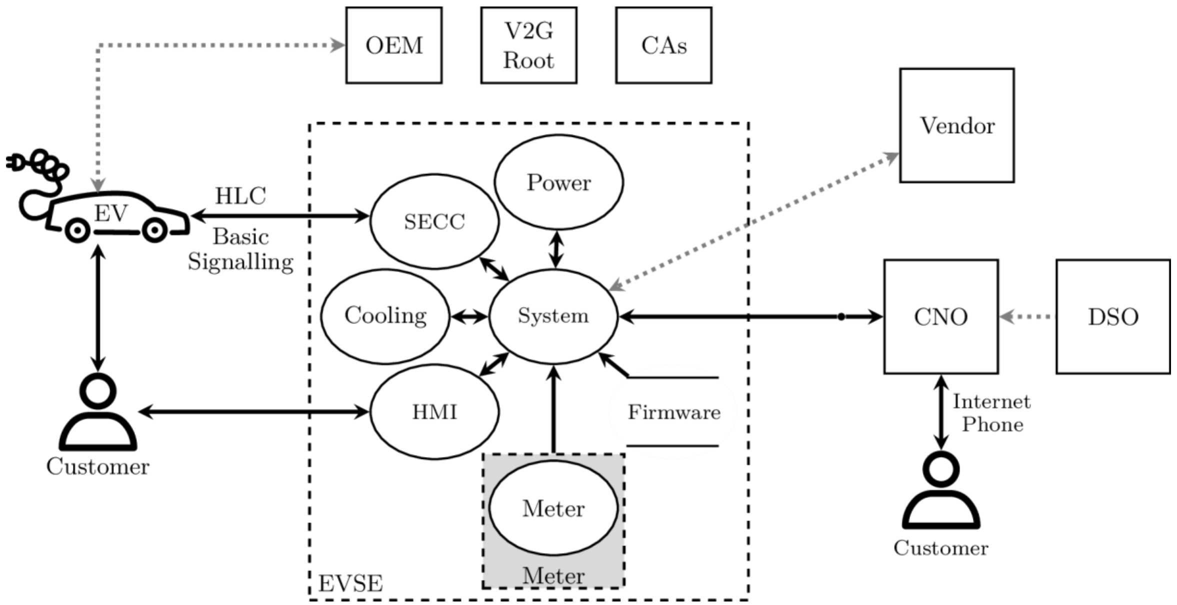




- High-power devices utilizing digital communications
- Local control, may operate offline for seven days
- Consumer facing, poor physical security
- Open components architectures
- Limited capacity for crypto agility
- ISO 15118-2 ⟶ ISO 15118-20
  - TLS 1.2 // verify SECC // optional ⟶ TLS 1.3 // mTLS // mandatory
  - AES 128 ⟶ AES-256
  - NIST P-256 ⟶ NIST P-521
  - 2x publicly-trusted PKI certificate hierarchies

Challenges



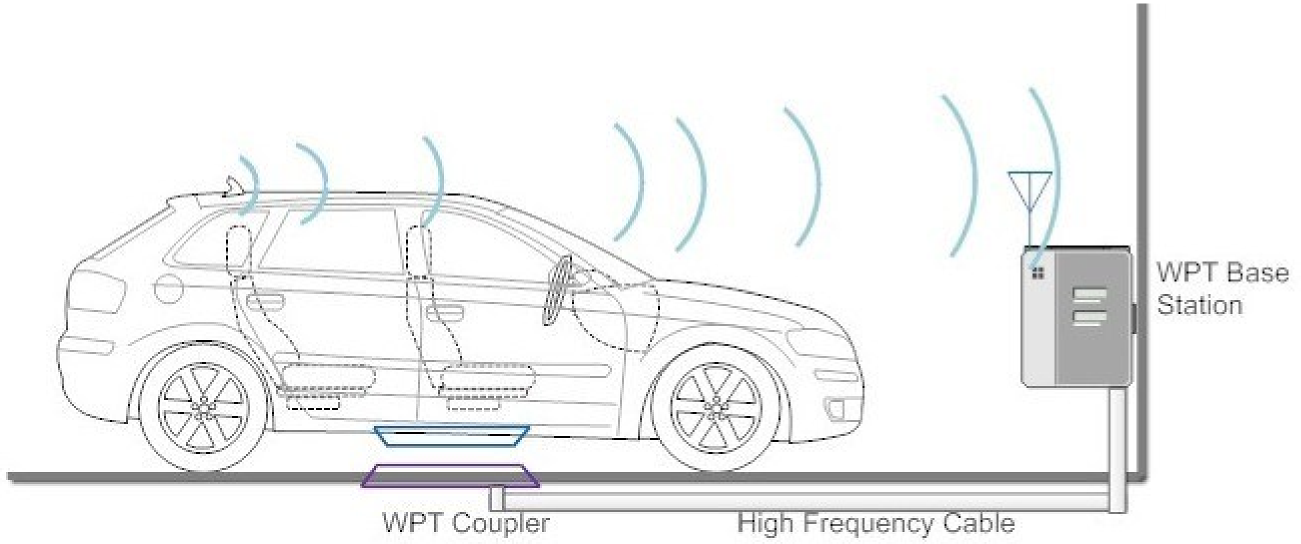


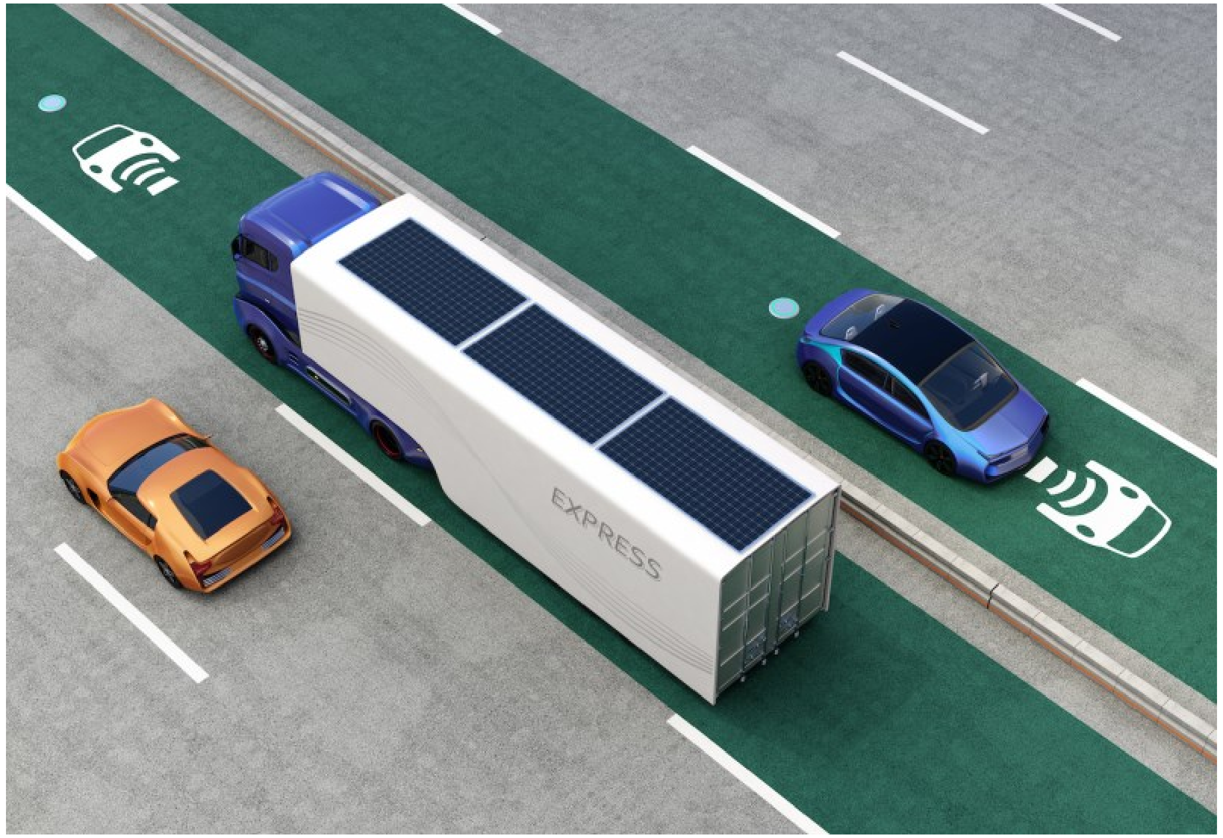
- Couples traditionally disparate transportation and electric sectors
- Non-traditional third parties involved in electric supply and network stability, who are operating across/above utilities and balancing authorities
  - EVs provide ancillary grid services, such as frequency regulation
- Information exchanges to locate, authenticate, authorize, meter, bill, and pay
- Largely unregulated by government… and want to keep it that way
  - Some industry-based cybersecurity best practices

Pacific Northwest
NATIONAL LABORATORY

Conductive Charging

Wireless Charging

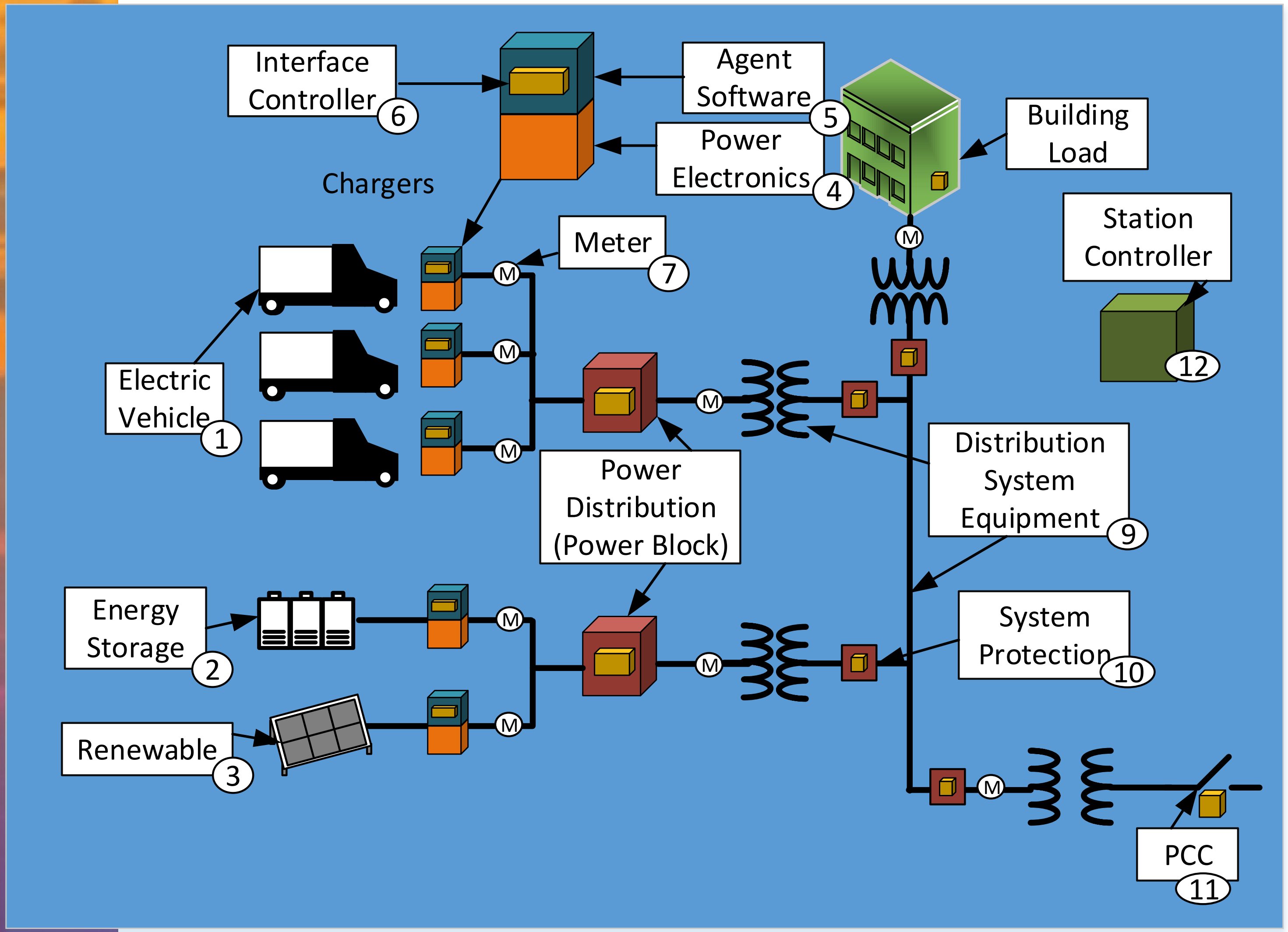




Assurances, Resiliency, and Cybersecurity Challenges

- Want assurances:
  - Safe
  - Availability and integrity of charging operations
  - Availability and integrity of electric supplies and networks
  - Limit energy, PII, and financial theft
  - Continued correct operation of vehicle
- EV charging infrastructure has numerous security & resiliency challenges
  - Confluence of environment, physical, cyber & cyberphysical security
  - Unclear which stakeholder has what responsibility
  - Stakeholders prefer self-governance over government regulation
- Attackers can use AV controllable to their advantage:
  - Demand-side attacks that impose grid stress that can lead to cascading faults
  - Impose financial harm

Resilient High Power Charging Facility

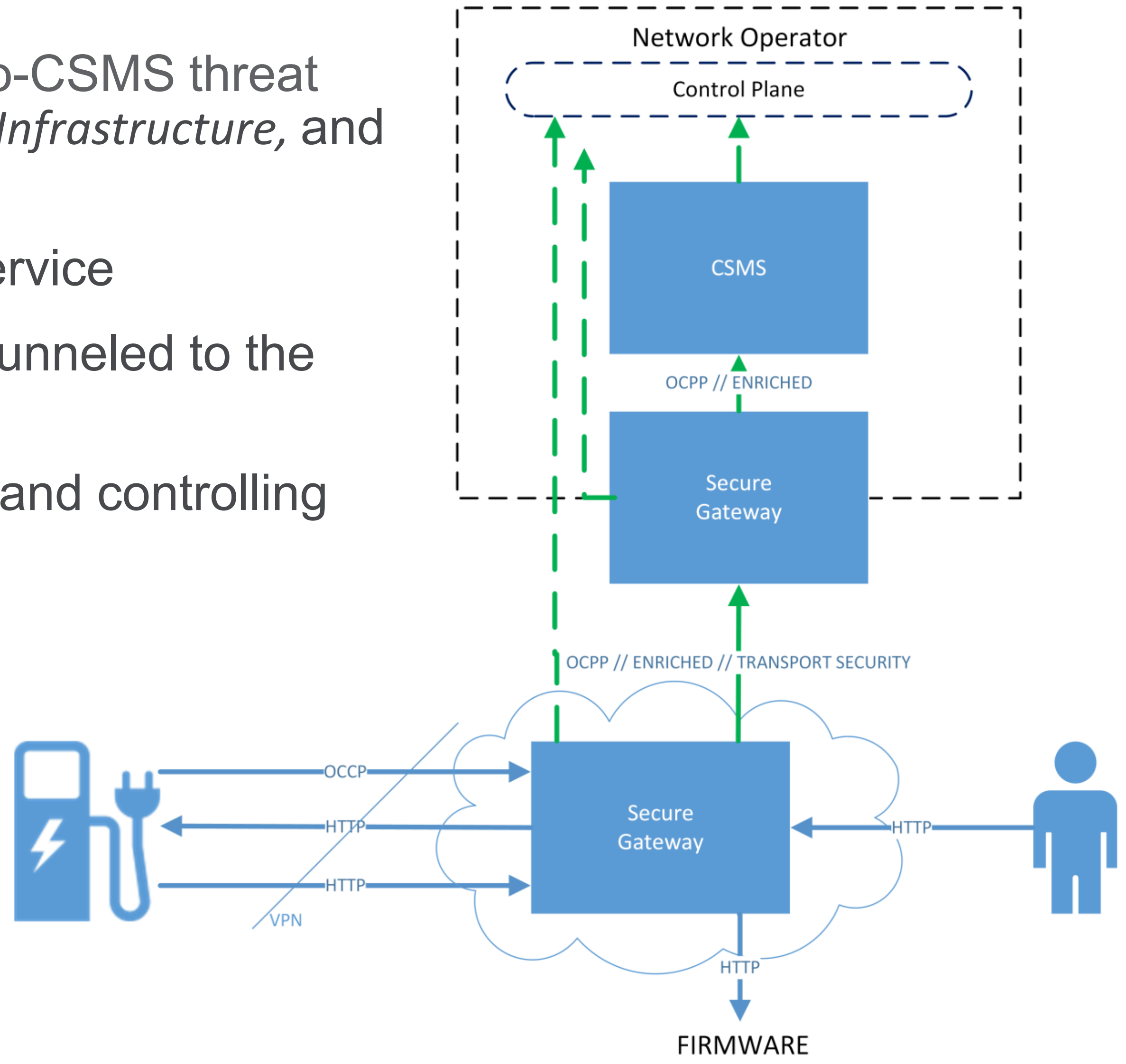


Use Cases Mapping to Sections of the Station

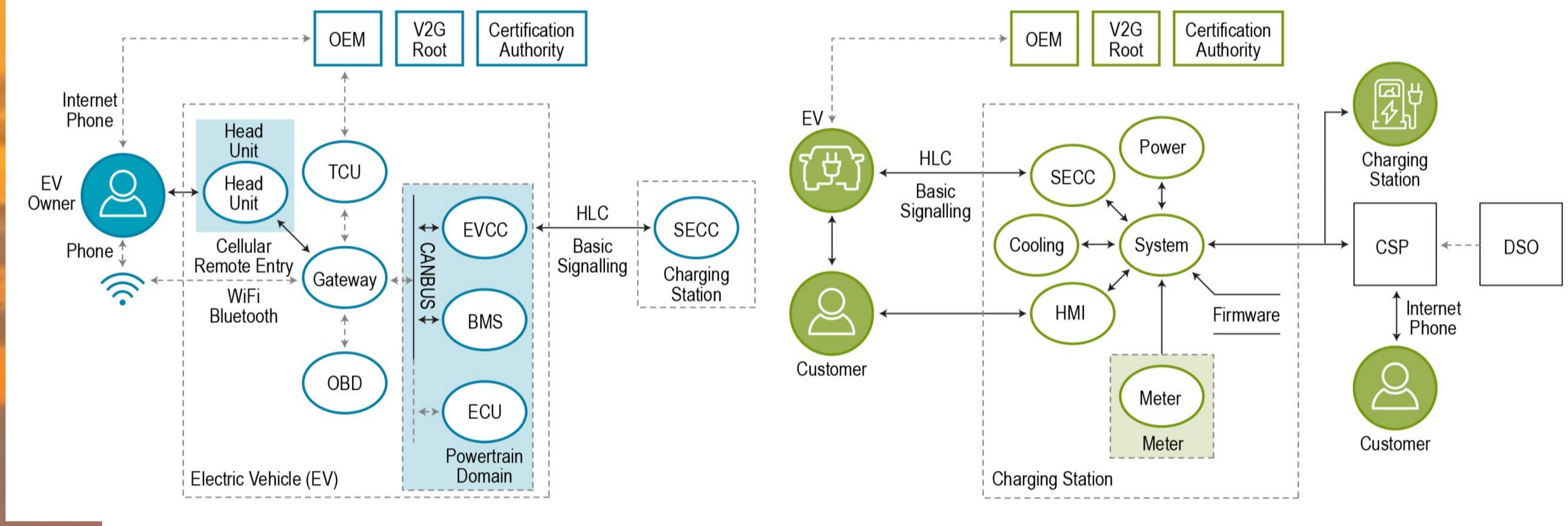
- National laboratory collaboration, lead by ORNL
- Include station response as a major focus including the potential for multi-phase isolation (**with a microgrid/nanogrid strategy) in a step-by-step fashion**.
- Station response may include several aspects such as **shedding loads, isolating chargers, ramping up energy storage, and/or isolation from the grid**.
- **Soft drop-off strategies** should be explored including leveraging stationary energy storage (including secondary use battery packs and ultracapacitors).
- Methodologies and tools to accurately and reliably **detect abnormal behavior of individual chargers and the charging station.**
- R&D focused on charging control **technologies, processes, and protocols**.
- **Exploration of open architectures** should also be pursued, identification of power electronics needs therein, and integration of station and smart charge management.

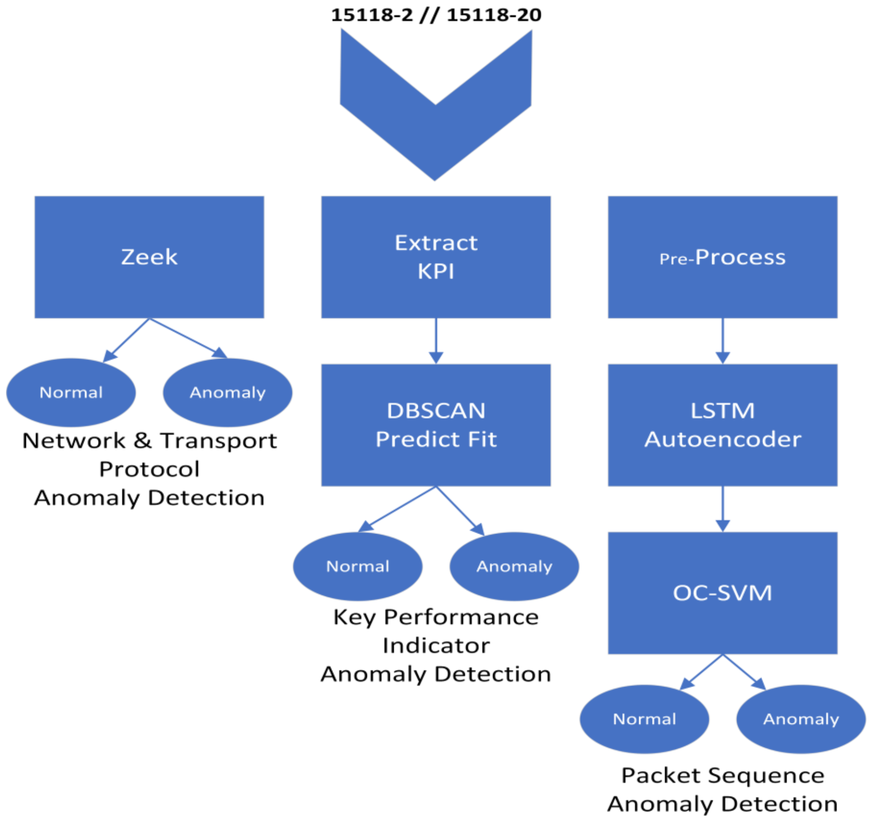
Zero Trust
EV @ Scale

- Distributed zero trust architecture intended to prevent/reduce intensity & scale of cyber attacks & breaches
- Addresses internet-to-charger, charger-to-internet & charger-to-CSMS threat vectors observed in *Power jacking*, *Securing the Vehicle Charging Infrastructure,* and *High Consequence Events*
- Chargers are cryptographically bound to a *Secure Gateway* service
- Charger management network interface communications are funneled to the Gateway
- The Gateway is a policy enforcement point, enforcing policies and controlling access
- The charger is separated from Gateway because:
  - Consistent application of access controls
  - Charger is not physically secure; has unmanaged interfaces
  - More capacity; easier updates
- Zero trust objectives are achieved:
  - Every request is authenticated & authorized
  - Identity-based access controls
  - Observability & continuous monitoring
  - Reduced third-party observability



Threat Model of EV Charging – Grid Impacts





Performed first of its kind EV Charging Infrastructure Threat Analysis (Figure 1):

1. Identify consequences to energy and transportation sectors
2. Define XFC security objectives: privacy, power system, transportation system, financial transactions, etc.
3. Model systems, identifying information and electric power flows
4. Examine flows for vulnerabilities
5. Identify controls and mitigations to address threats

Investigated cryptosystems and Public Key Infrastructure (PKI) as employed in ISO/IEC 15118-2//15118-20 ecosystems.

Findings:

- Consequences helped identify power/transportation threats.
- Energy sector cannot mitigate XFC alone; ecosystem parties need strong coordinated cyber practices.

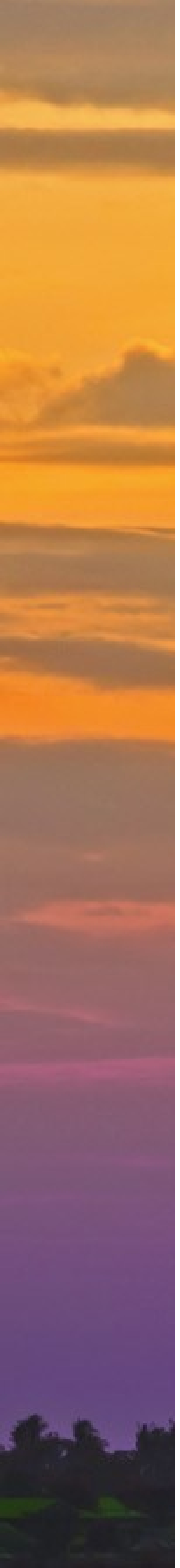
Deliverable:

- Threat consequence report published 9/2020

15118-20 anomaly detection (Figure 2):

- 15118-20 mandates TLS for all use cases
- Develop analysis techniques to detect anomalies patterns of encrypted network traffic.

Pacific Northwest
NATIONAL LABORATORY



Thank you