Electric Vehicle Supply Equipment (EVSE) Security

SOUTHWEST RESEARCH INSTITUTE®

Katherine Kozan

March 26, 2026

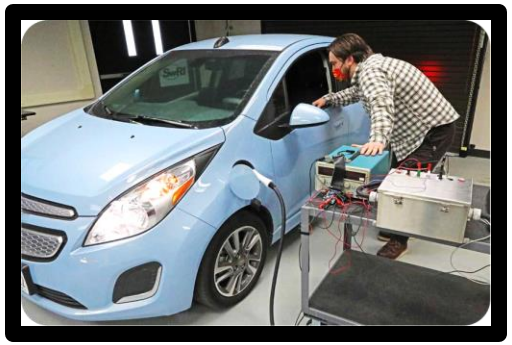
Concerns

- Battery Management System Exploits
  - Spoof
  - Denial of Service
- J1772 L2 Charger
  - Machine-in-the-middle
    - Overcharging
    - DoS
    - Limit charging
- DCFC Charger Vulnerabilities (PLC)
  - System access
- Plug-n-Charge
  - MitM with Signal Level Attenuation Characterization (SLAC)
- PKI for EVSE
- Key Management

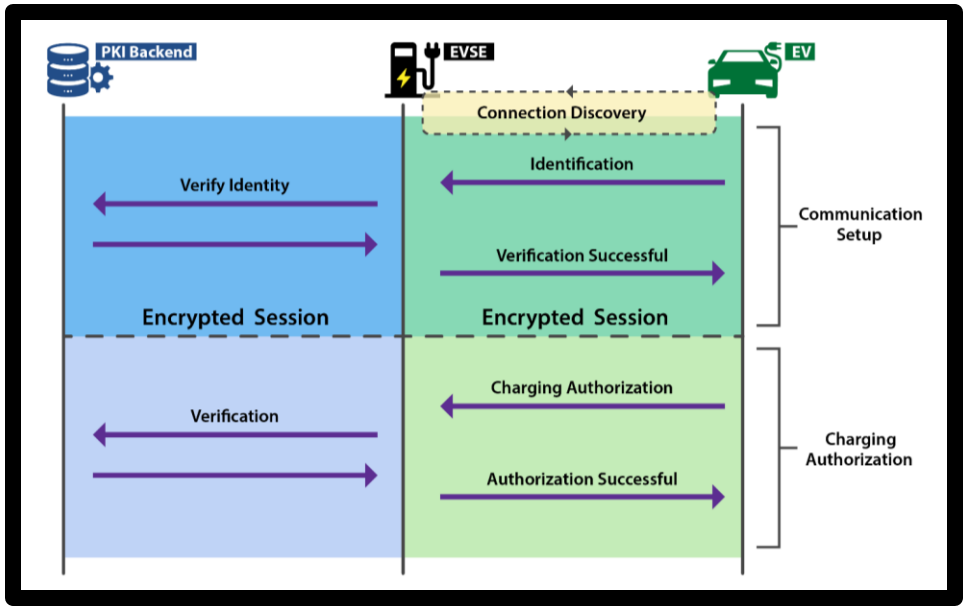
BMS
J1772 L2
PLC
PnC
PKI
KM

The Evolution of EV/EVSE Comm Security

- **DIN 70121**
  - No TLS, request & response
  - Signal Level Attenuation Characterization (SLAC)
  - Basic Communication & Authentication for DC charging
  - Limited Encryption
- **ISO15118-2**
  - TLS Encryption Introduced
  - PKI and Digital Certificates
  - Plug & Charge
- **ISO 15118-20**
  - Enhanced TLS (1.3) and Mutual TLS (mTLS)
  - Bidirectional Charging Security
  - Regular Security Updates



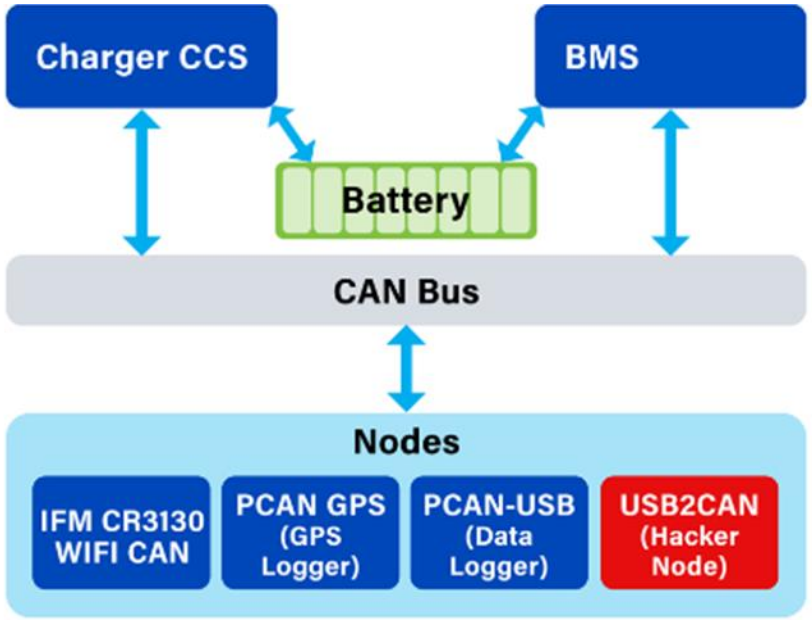
SwRI's EV & EVSE Cybersecurity Research



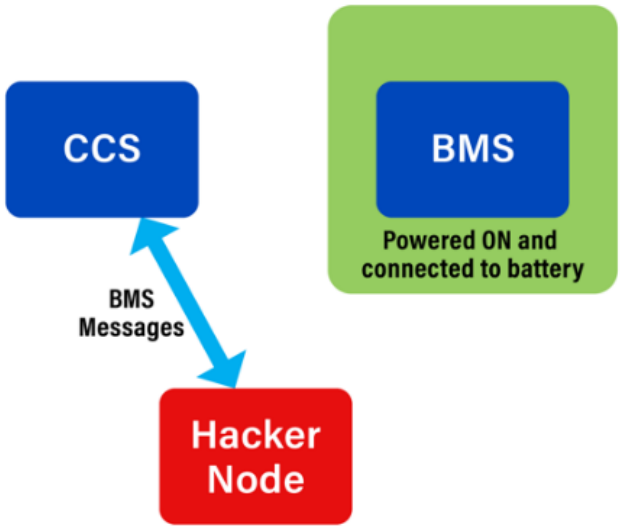
TLS in PnC: Authorization Sequence

BMS Background

- **Combined Charging System:**
  - Provides and regulates battery's charging current
  - Monitor voltage of battery
- **Battery Management System:**
  - Manages and evaluates overall battery function and health
  - Monitors each battery cell
  - Commands CCS for charging

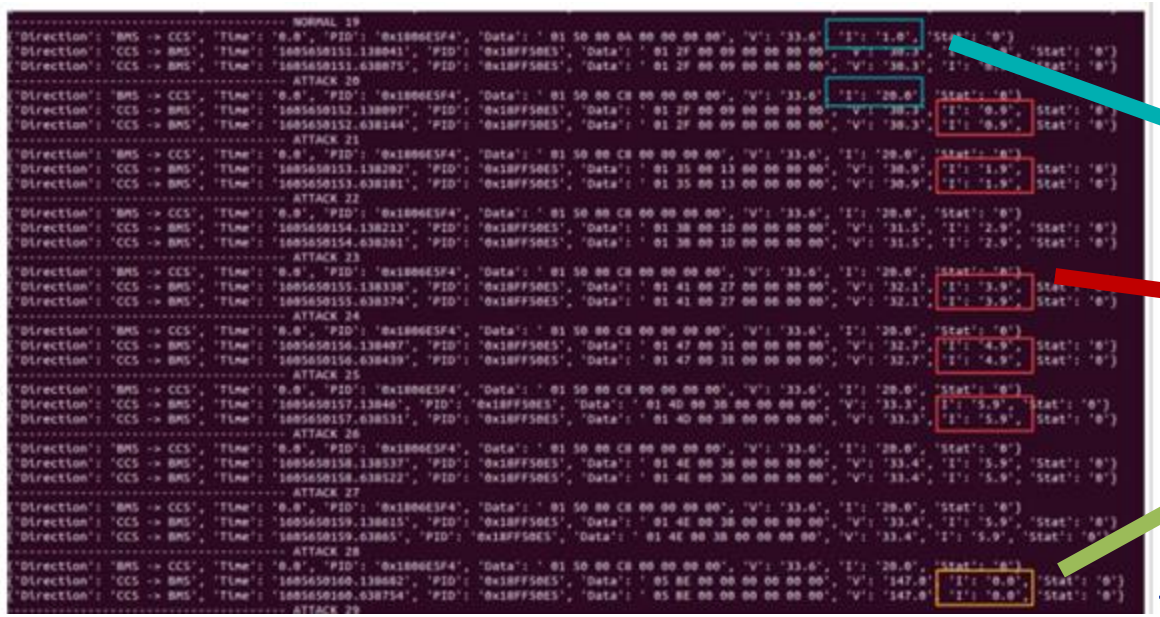


BMS Spoof CCS Current



- Hacker node sends messages as BMS to CCS
- Using BMS to CSS ID
- Hacker gradually sends messages to CCS
- Increase Current to unsafe levels

Result: Charging Halted

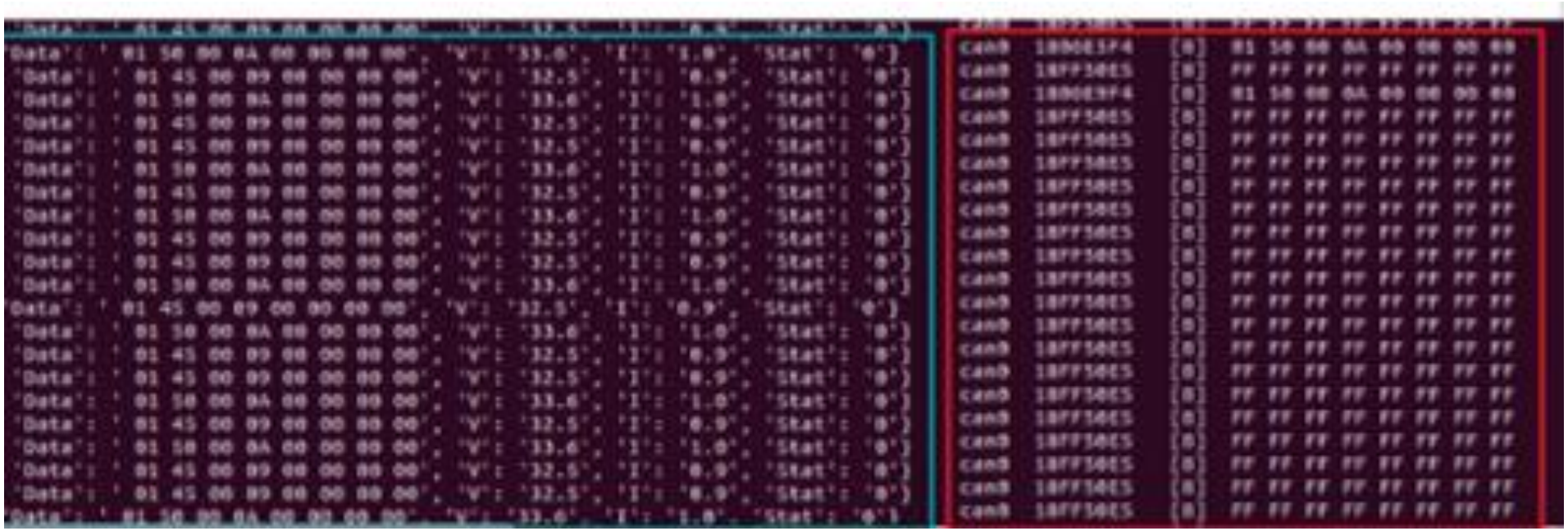


BMS->CCS, Current increase

CCS->BMS, Current increasing

CCS->BMS, Current stop

Denial of Service



- Hacker node sends messages and floods CAN Bus
- Real BMS & CCS disconnected

Result: DoS Attack Successful

BMS

Electric Vehicle Charging Networks: Technology Advancements Outpace Necessary Cybersecurity

- Increased reliance on electronic communication and charging systems have created opportunities for novel cyberattacks.
- SwRI research demonstrated cyberattacks are possible on current networks.

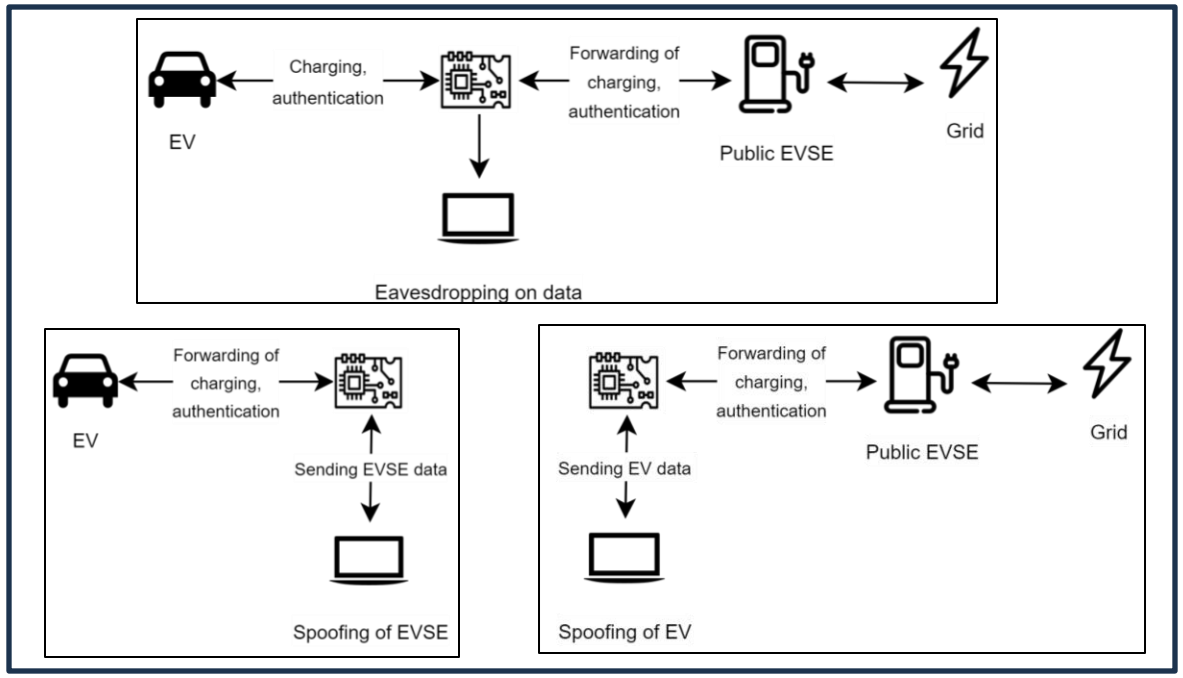
SwRI Project: Electric Vehicle Charging Station Cyber Security Vulnerabilities
https://www.swri.org/press-release/electric-vehicle-charging-cybersecurity-vulnerabilities

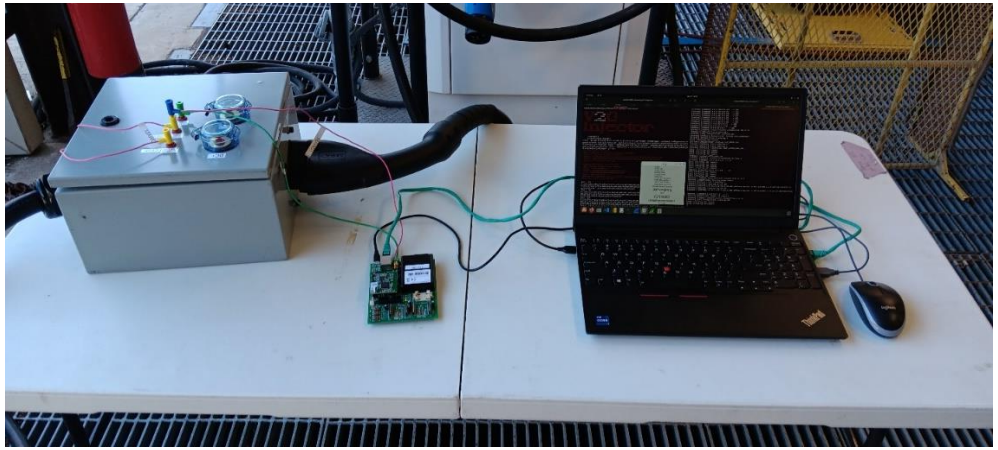
SwRI Project: Electric Vehicle Cybersecurity
https://www.swri.org/work-us/internal-rd/2020/automotive-transportation/10-r6022

J1772 L2

DC Fast Charging (DCFC) EV Supply Equipment (EVSE) Security IR

Objective: Analyze the EV DC Fast Charging (DCFC) charging process and the power-line communication (PLC) used



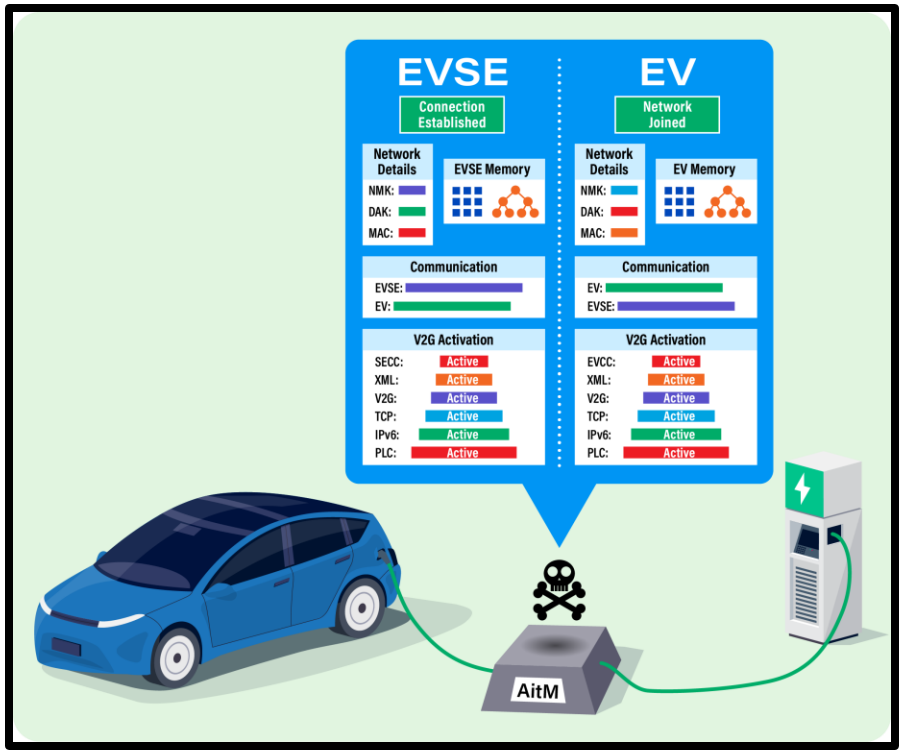


PLC

Press Release: https://www.swri.org/press-release/swri-evaluates-cybersecurity-risks-associated-ev-fast-charging-equipment

Power Line Communication DCFC

- Determine whether DCFC chargers are secure
- Conversion from PLC to Ethernet
- Dumped config files
- Modify & Reuploaded config files



This diagram demonstrates an SwRI-developed adversary-in-the-middle (AitM) attack and its capability to emulate both an electric vehicle and EV supply equipment (EVSE), as well as monitor their defined attributes.

Result: Open Ports

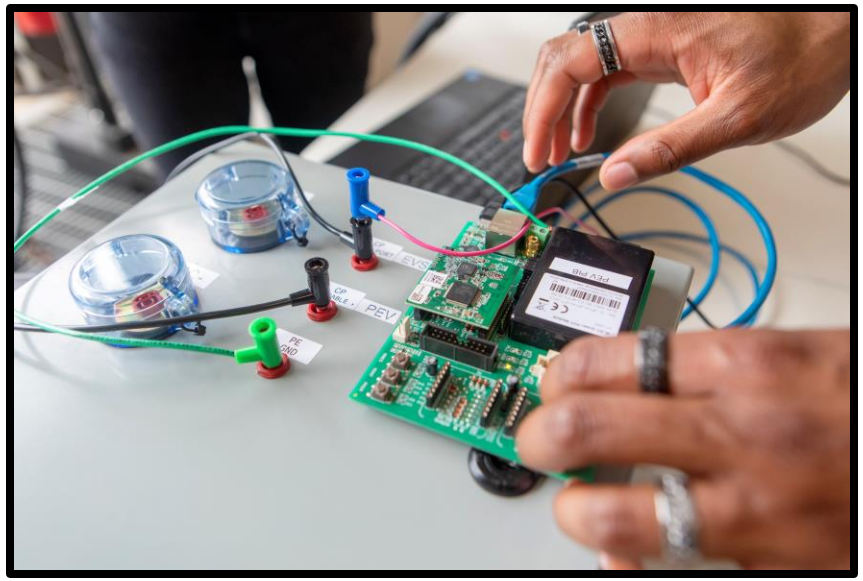
Press Release: https://www.swri.org/press-release/swri-evaluates-cybersecurity-risks-associated-ev-fast-charging-equipment

P
L
C

Interception of Plug-n-Charge Comms

Objective: Establish a MitM by leveraging weaknesses in the Signal Level Attenuation Characterization (SLAC) process.

- **Modify existing traffic in transit between the systems**
- **Compromise certificate exchange during connection setup**
- **Downgrade the security of the connection**



PnC

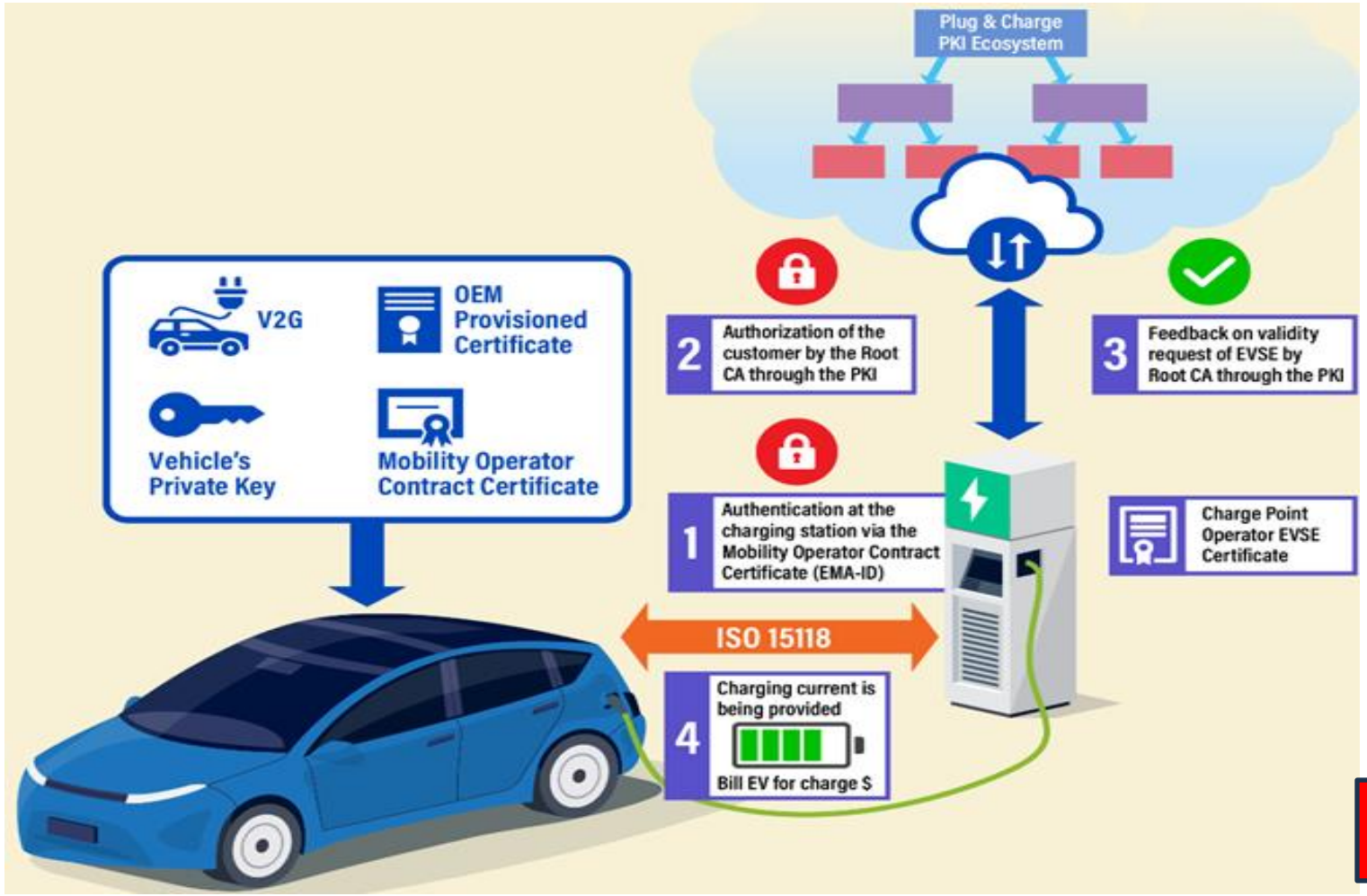
EVSE Public Key Infrastructure (PKI) Research

- **Investigating**
  - Security of PKI communication in EV charging networks
  - Feasibility of attacks against communication protocols/PKI certificates
- **Analyzing communication protocols in EVSE environment**
  - Identifying vulnerabilities
  - Developing mitigation strategies

P
K
I

PKI for an EVSE

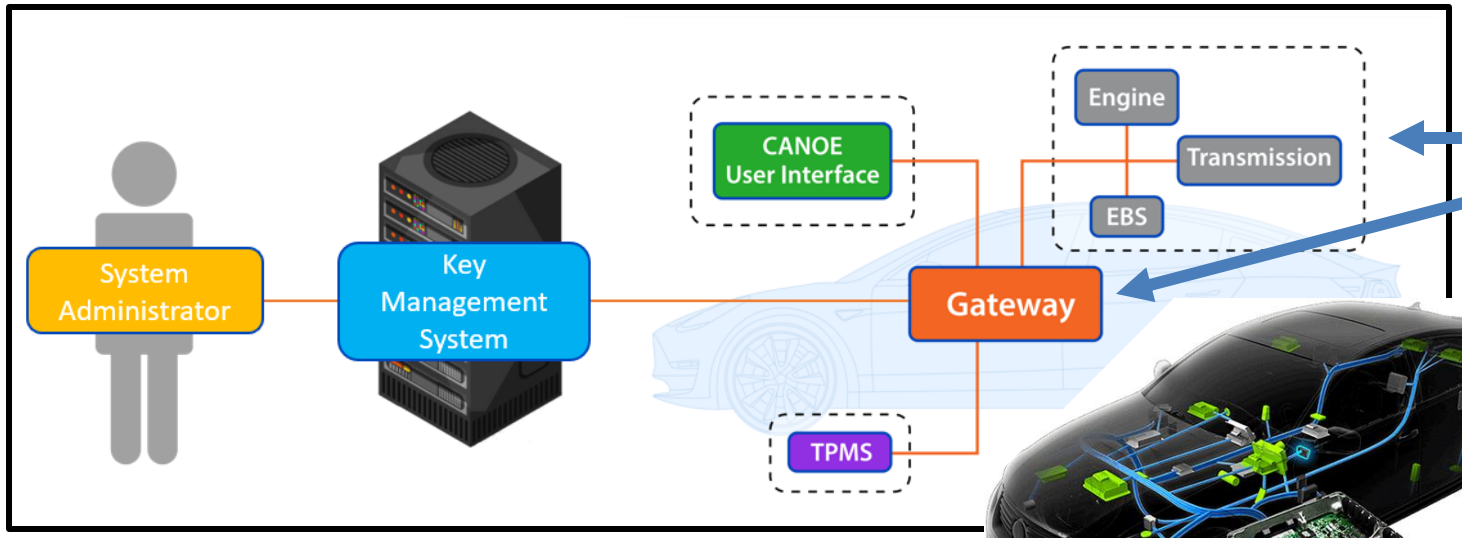
- SwRI will be establishing an EVSE simulation with PKI capabilities and utilizing a vehicle with an active PKI
- Create a baseline reference architecture of backend communications
- Focus on authentication and authorization



Key Management System

- Demonstration of a comprehensive KMS for embedded systems based on adapting open-source software in an embedded automotive environment

Demonstratable proof of concept for other applications



Work with multiple device types

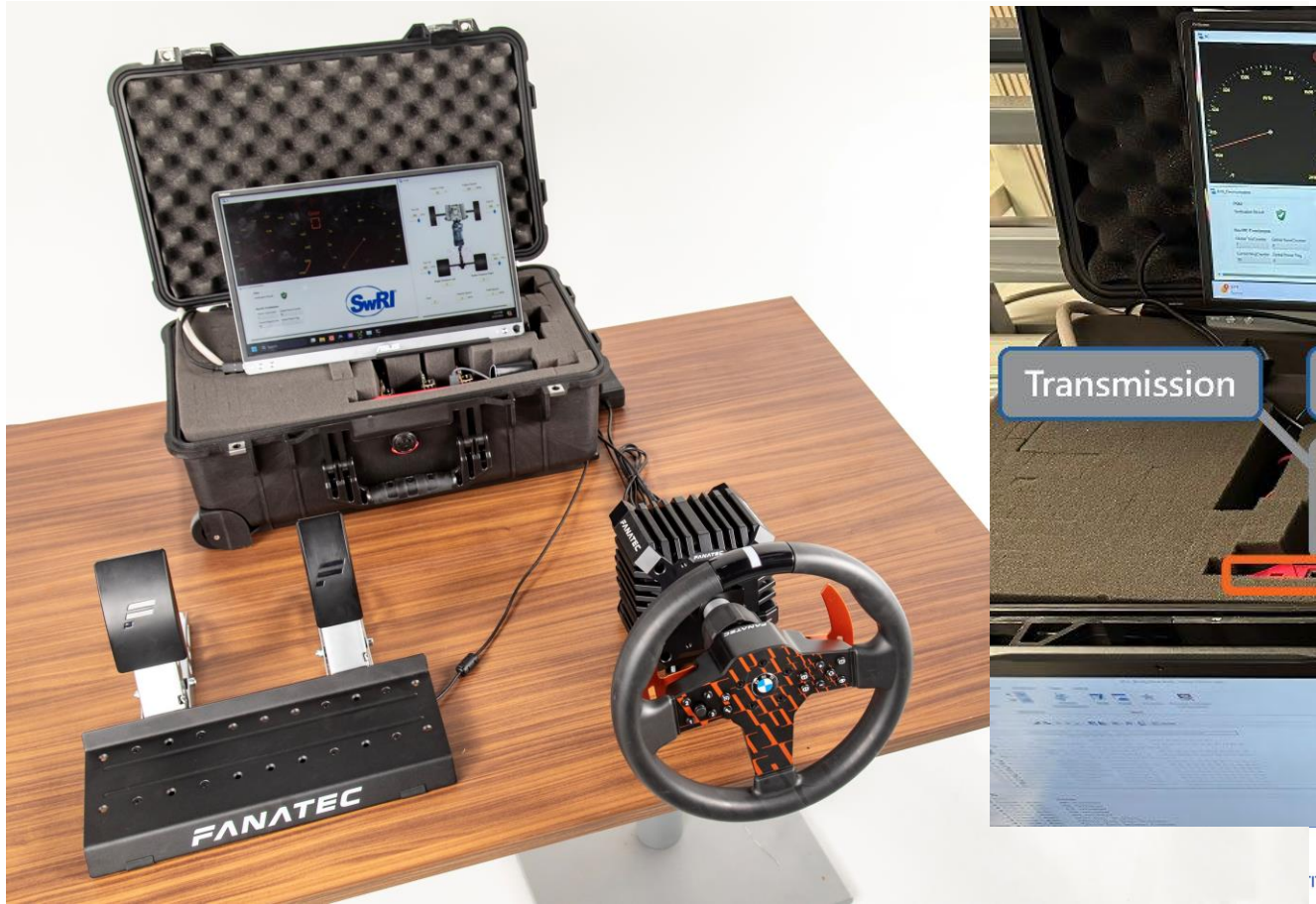
Work with existing SwRI cyber applications

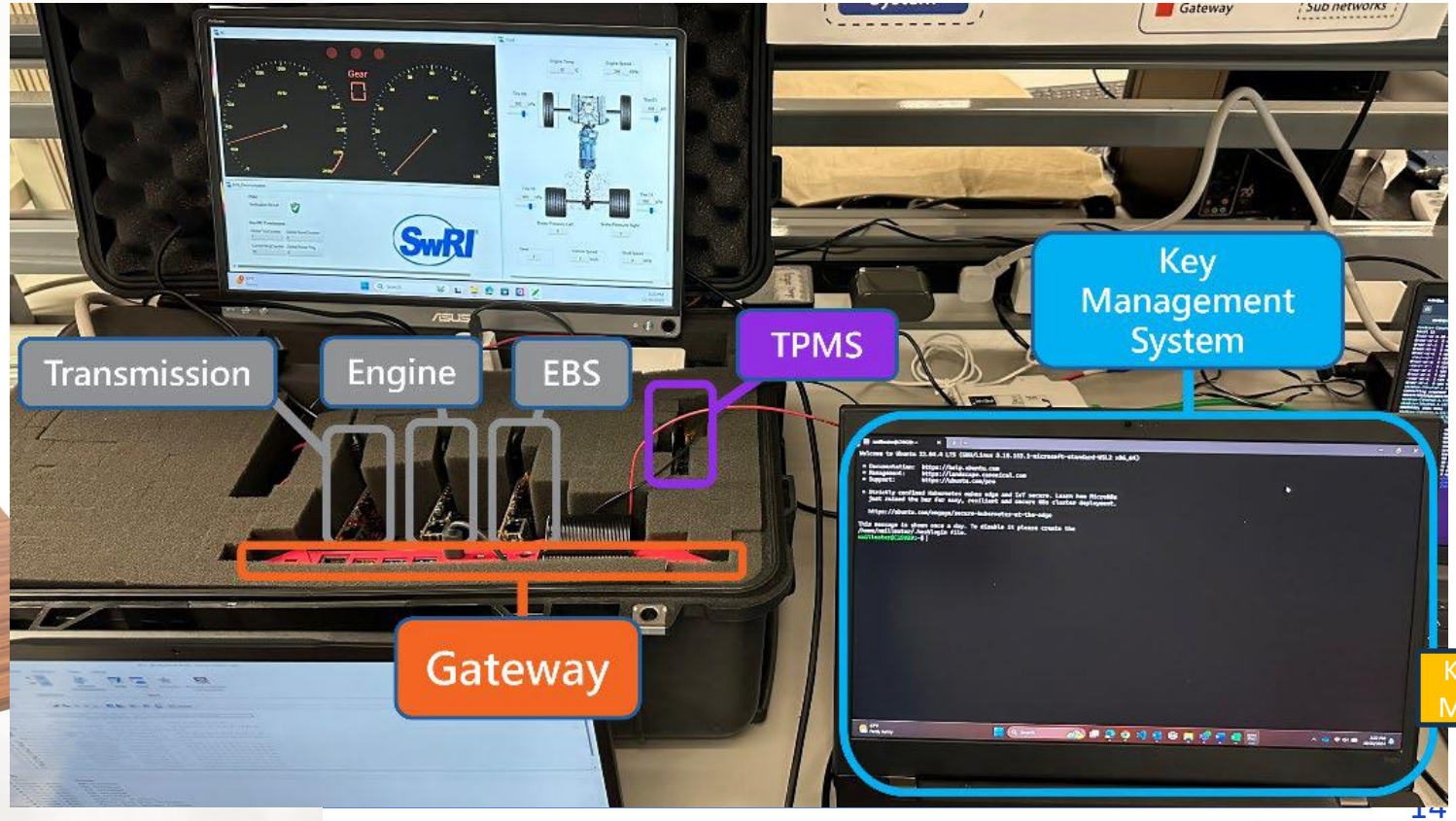
Measure Success with a Test Plan

K M

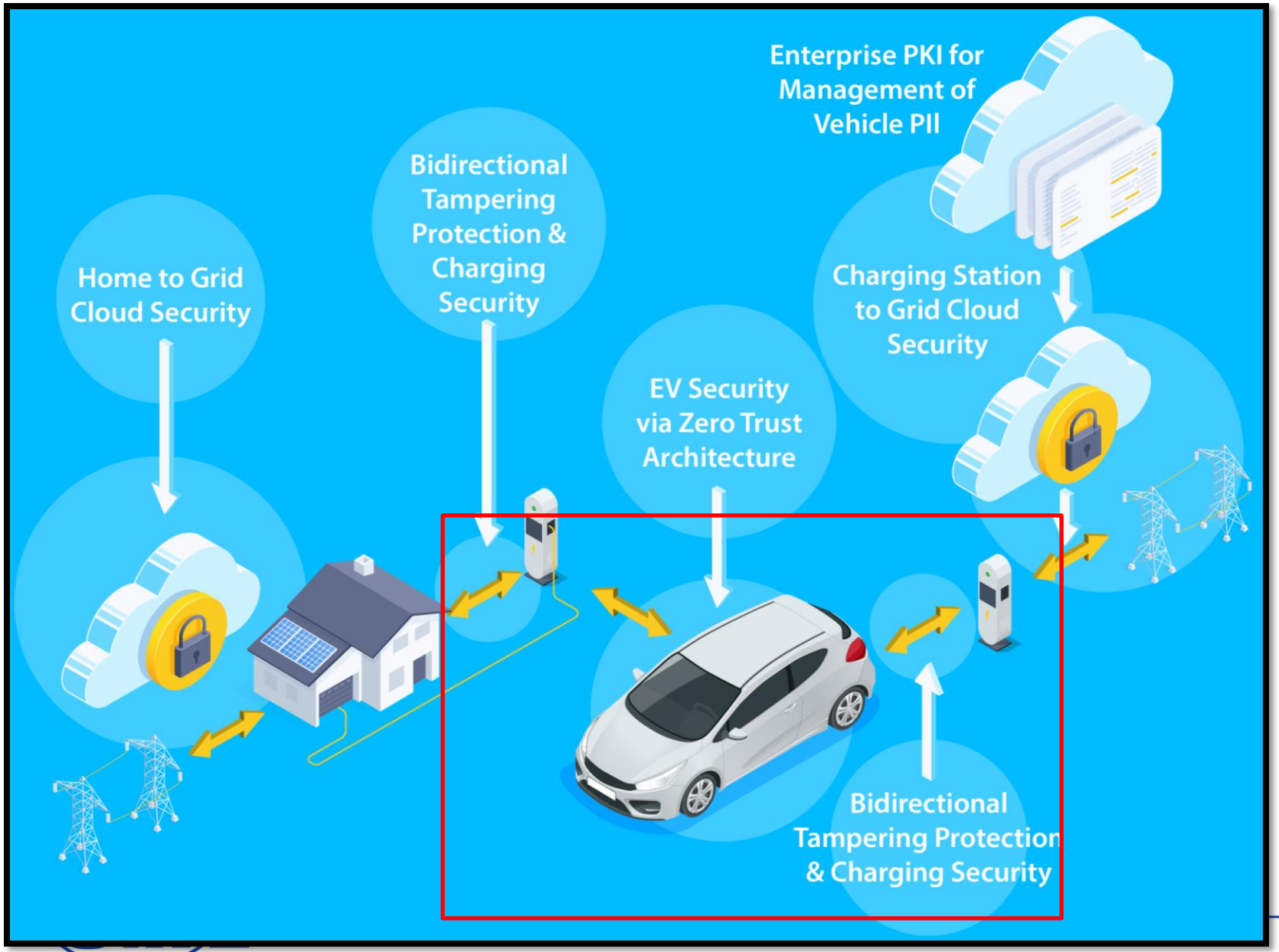
Key Management

- Successfully demonstrated key exchanges on a hardware-in-the-loop vehicle simulator
- Implemented full SecOC and Zero Trust principles





SwRI's V2G Cybersecurity



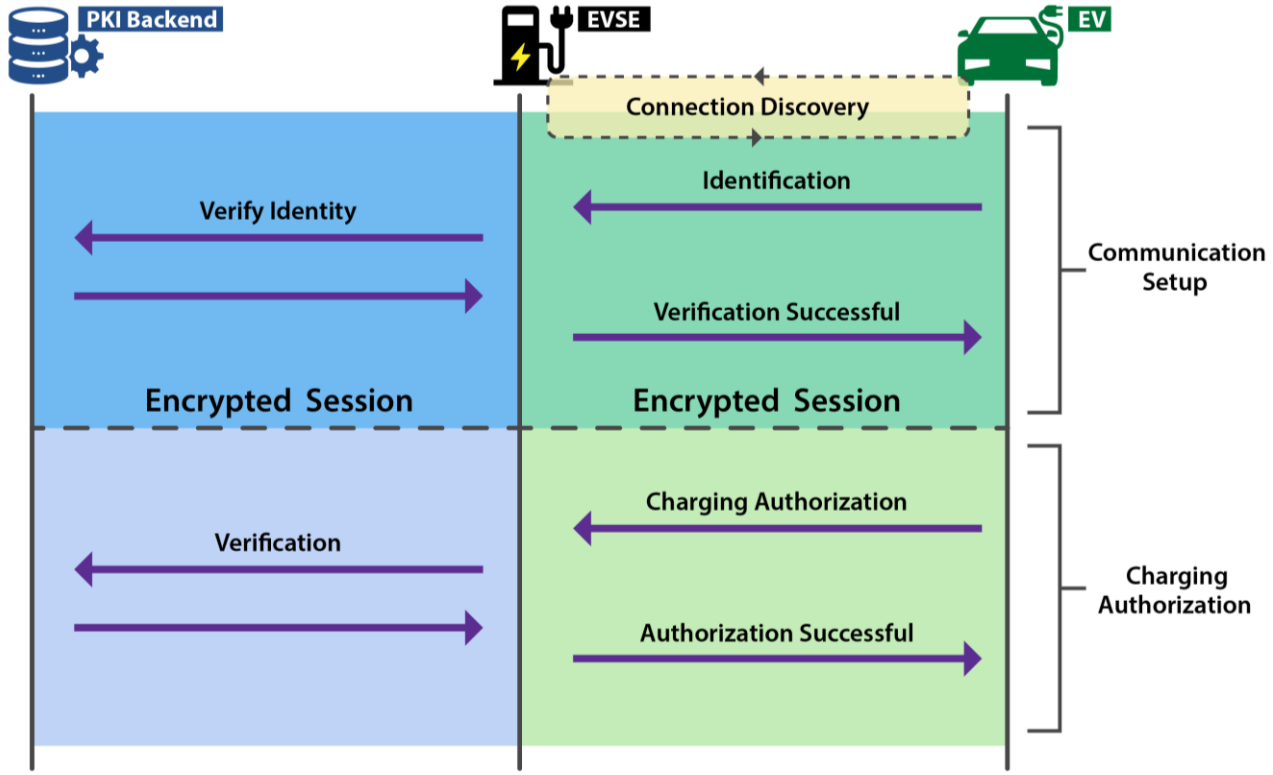
- **Previous research areas**
  - Security
  - Standardization
  - Speed of charging
  - Functionality

We believe that a V2G solution can be designed with security as a foundation, providing robust functionality at scale

- **Next Phase of Research**
  - Distribution (availability)
  - Integration
  - Ease of use

Authentication & Authorization

- Examining certificate exchange and provisioning
- Examine ISO 15118 authentication foundation
- Identify Vulnerabilities and Develop Mitigation Strategies
  - Open network ports
  - Data manipulation
  - Interception attacks



Questions And Further Discussion

Katherine Kozan
Research Engineer
210.522.2541
Katherine.kozan@swri.org