Cybersecurity Platform and Certification Framework Development for eXtreme Fast Charging (XFC) Infrastructure Ecosystem

DoE Vehicle Technologies Office Annual Merit Review Presentation, ELT206

Principal Investigator: Sunil Chhaya, PhD
Technical Manager: Rish Ghatikar

June 24, 2021

Agenda

- **Overview, Approach, and Milestones**
- **Technical Accomplishments** (2019-Q1 2020)
- **Details for 2020 research** (Q2 2020-Q1 2021)
  - **Key Findings**
  - **Recommendations**
- **Future Research**
- **Technical Back-up Slides**

Project Overview

Timeline

- October 2018 - June 2021
- 95% complete

Barriers

- Lack of integrated security awareness of standards and requirements
- Limited stakeholder engagement process & cybersecurity priorities
- No central location of security risks and requirements

Budget

- $2.2M Total project funding
  - $1.7M DOE funding
  - $0.5M Cost share

Partners

- EPRI (Prime)
- Kitu Systems
- Automation Research Group
- Greenlots
- Argonne National Laboratory
- National Renewable Energy Laboratory

Project Objectives and Features

Objectives

Phase 1 (2018-20)

- Evaluate and assess cybersecurity risks to develop a reference network architecture of connected systems, sub-systems, and communications for an XFC ecosystem – *working together with the industry!*
- Conduct cybersecurity threat and vulnerability assessment to identify and classify assets for XFC sub-systems.
- Recommend controls, system architecture, and a reference design for a *Secure Network Interface Card* (S-NIC) for XFCs – *qualitative and quantitative assessment for field application readiness.*

Phase 2 (2020-21)

- Develop test plans, conduct combined laboratory tests, verify results, and develop an *Integrated Grid Security Risk Management* (IGSRM) tool.

Features

- Uniform electric system-wide requirements
- Active, broad stakeholder team engagement
- System Component testing for requirement verification
- Secure Network Interface Card Open-sourcing of hardware and software design
- Technology transfer through EV Infrastructure Cybersecurity Working Group (EVICWG)
- Coordinated effort with wider Federal, State, standards organizations, and utility industry coalitions with EPRI, as the forum for collaboration

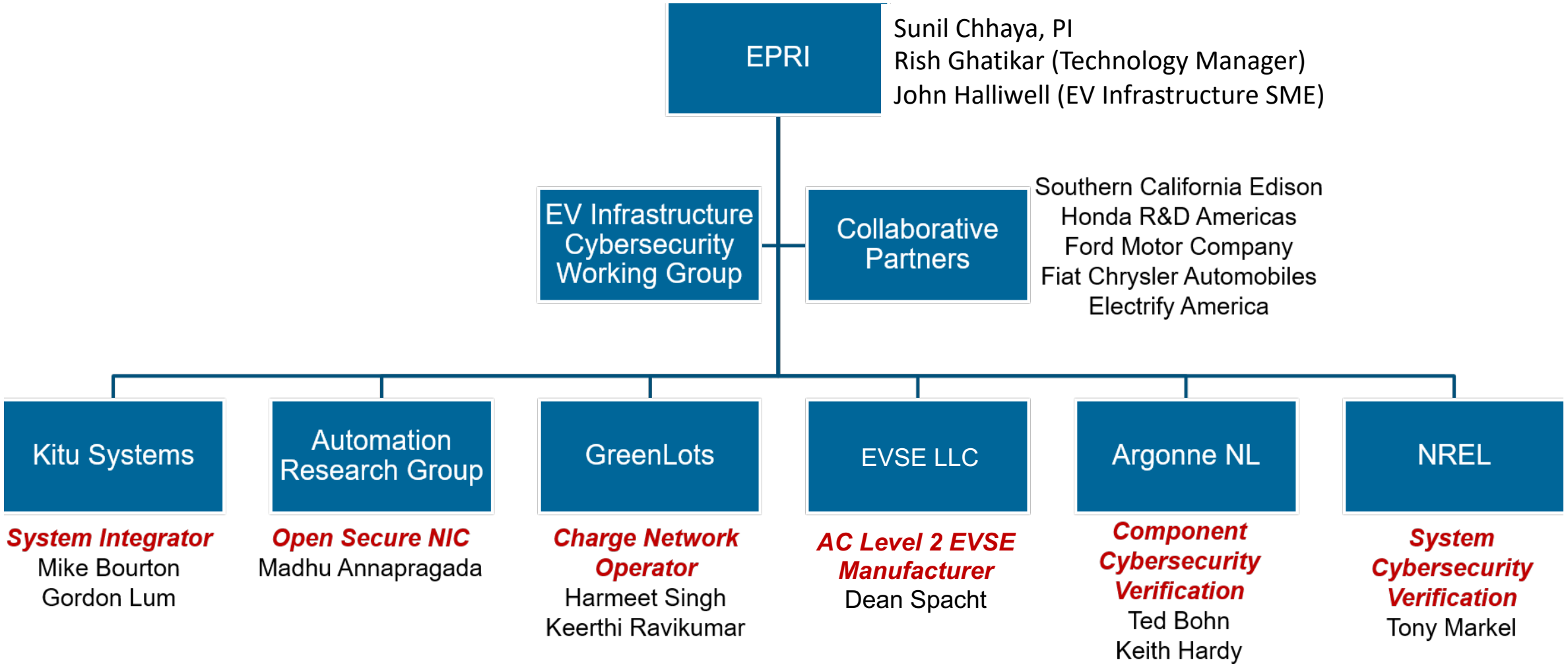
Focus for 2020-21

Approach: PEV Infrastructure Cybersecurity Requirements, Tool Design, Assessment, Mainstreaming

Assess	Define & Design	Build	Test & Validate	Mainstream
• Architectures • Attack pathways • Vulnerabilities • EV Infra. Cybersecurity Working Group (EVICWG)	• System and Component • Test requirements • Test harness requirements + design • Test harness design	• Integrated Grid System Risk Management Tool (IGSRM) • Secure Network Interface Card • Software in the Loop verification	• Test components per test plans, refine requirements • Test system per test plans, refine system-level cybersecurity requirements	• EVICWG – stakeholder consensus, standards • Publication and public dissemination

10/2018 → **06/2021**

Collaboration and Coordination



Engaged EV Infrastructure Industry Ecosystem through EV Infrastructure Cybersecurity Working Group (EVICWG)

SOPO Timeline and Key Milestones – 2020-21 (Revised)

Milestone	Type	Description and Status	Delivery Date
End-to-End Security Test Plan	Technical	Cybersecurity testing plans.	Q1 2020 → **Draft submitted to DOE.**
Integrated Grid Security Risk Management (IGSRM) Tool Finalized	Technical	Tool prototype developed and updated based on testing results.	Q2-Q3 2020 → **Due to rescheduling of testing, recommend completion by Q2 2020.**
Cybersecurity Testing	Technical	Testing complete with results documented.	~~Q3 2020~~ Q1 2021 → **Due to COVID-19 Challenges, recommend completion by Q2 2021.**
Integrated Grid Security Risk Management Tool Published	Technical	Reference architecture is market-ready for implementation through industry deployments and regulatory framework.	~~Q3 2020~~ Q1 2021 → **Due to rescheduling of testing and process, completed by Q1 2021.**

Completed Tasks

Pending Tasks

Even with COVID-19 Delays, the Project Team is on Track to Meet the Project Objectives

Responses to Reviewer Comments

Approach to performing the work—

- The project has managed to adapt and revise the deliverable schedule to meet the project objectives with no cost over-runs.
- The innovation of the project lies in reviewing the cybersecurity requirement for the entire EV ecosystem, as an integrated and connected ecosystem where the attack on one subsystem (e.g., EV) can expose the risks in the other (e.g., EVSE).
- Additionally, the project implemented a critical analysis of the as-is EV charging ecosystem, allowing for the identification of cybersecurity requirements and the addressing of gaps through the EV cybersecurity platform reference architecture and design implementation

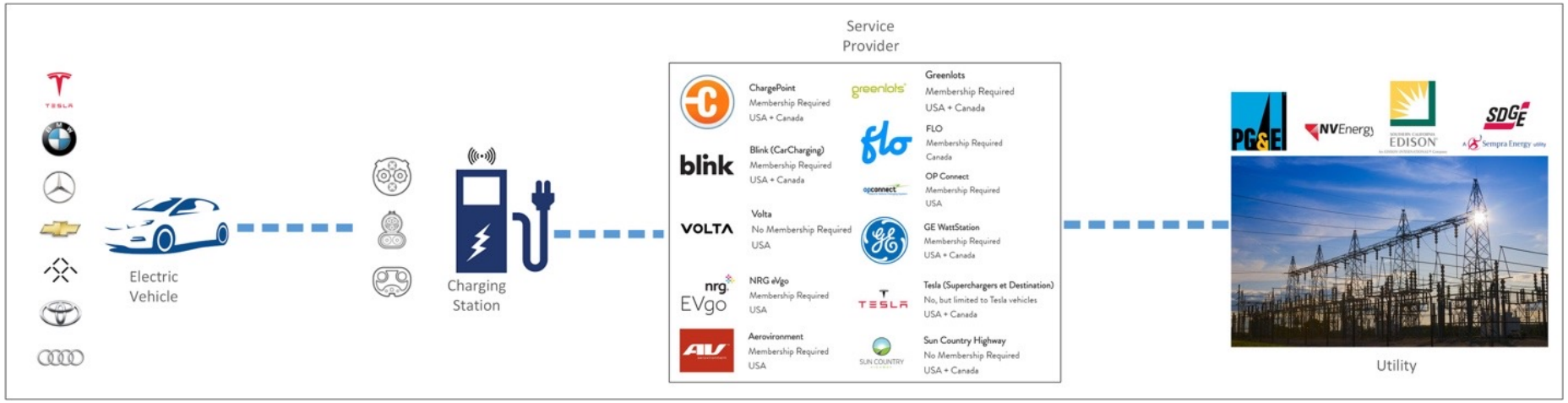
Technical Accomplishments and Progress toward overall project goals—

- The EV ecosystem sub-system is categorized under EV, EVSE, network operator, and utility/building subsystems to review component-level requirements for data-at-rest and data-in-motion. The model can be expanded to support a diversity of EVSEs.
- Industry acceptance by EV Infrastructure Working Group (EVICWG) that comprises of >100 members across the entire EV sector.
- Project team has validated qualitative cybersecurity risk assessment and recommendations through laboratory tests.

Proposed Future Research—

- The methodology and tools provides a platform to disseminate cybersecurity risks and recommended controls to the EV stakeholders; project is modular to scale to meet the evolving future cybersecurity and EVSE infrastructure needs.
- Laboratory testing has provided initial validation of cybersecurity risks; Field application will help understand real-world issues.
- Aligning the project findings and recommendations with national level XFC cybersecurity profile to industry adoption (e.g., NIST).

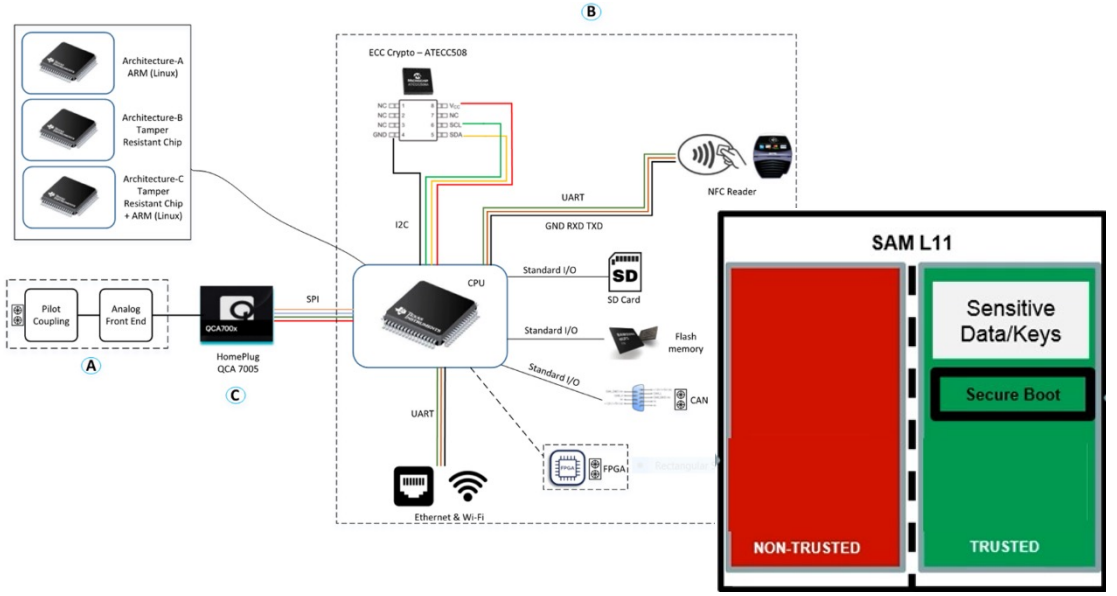
2019 Research Outcomes: System Architecture, Cybersecurity Controls



Controls for each sub-system (e.g., EV)

#	Components	Summary of Security Controls
1	Smartphone-Vehicle Communications, Android/IOS application, Bluetooth, Wi-Fi Hotspot, Smartphone memory (internal/external)	• Careful use of memory and sandboxed design. • Avoid using external memory or media on a smartphone. • Encrypt and Anonymize data between smartphone and an EV.
…	…	• …
9	CAN bus/OBD Port, EV Charging Controller and communications	• Communications originating and ending at charge controller must be secured, on a private network or control bus (e.g., CAN). • For charge controller connected to CAN gateway, implement data and control security at the gateway or the ECU level.

Schematic Design of Secure NIC



2020-21 Research Priorities

Efforts focused on using the earlier findings and recommendations to:

1. **Conduct Combined Test and Verify Results:** The study conducted experiments and assessed results to create cybersecurity requirements, test protocols, results, vulnerabilities and mitigation schemes or strategies in close association with the cybersecurity reference architecture.
2. **Develop an Integrated Grid Security Risk Management (IGSRM) Tool:** The IGSRM design was used to develop a web evaluation tool prototype to help vendors, service providers and utilities to navigate through the various cybersecurity standards.
3. **Mainstream and Standardize Interoperable Cyber-Secure Ecosystem**: Continuing from the earlier efforts, the project engaged the EV Infrastructure Cybersecurity Working Group (EVICWG) to review project outcomes and obtain feedback to engage the industry in the market transformation of cybersecure XFC infrastructure.

Summary of Test Set-up

CSRL

A 7.2 KW Level 2 charger was installed and comprised of two primary components:

1. EVSE Payment Module: payment processing, C&C, network routing
2. EVSE Charging Module: power electronics for the charging system

An engineering workstation hosting a virtual instance of Kali Linux was used to facilitate the regular operation, profiling, and attempted exploitation of the charger.

NREL

Focus on communication between the EVSE and a network operator or the charging service provider backend.

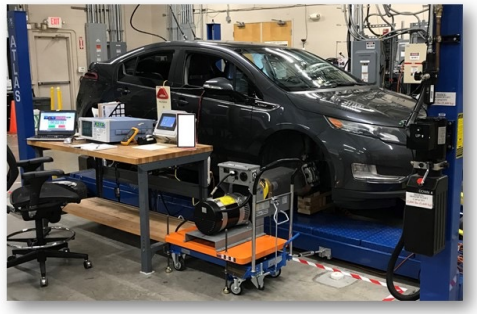
1. Identify potential vulnerabilities associated with the use of Open Charge Point Protocol (OCPP), which is an open standard protocol supporting EVSE interoperability
2. primary components of interest were categorized into Vehicle, EVSE, and Systems Control/Backend.

ANL

Focus is on EVSE communication pathways with

1. Evaluate Network Level Site Controller
2. Communications between EVSEs in a facility
3. Integrated energy storage, as a service, to EVSEs
4. Evaluate security for communication between cloud/back-end and the EVSE.

The EVSE test articles represent very latest models (2021 practices and a variety of ZigBee, Ethernet, Wi-Fi, Modbus connected EVSEs.



Summary of Test Results

CSRL

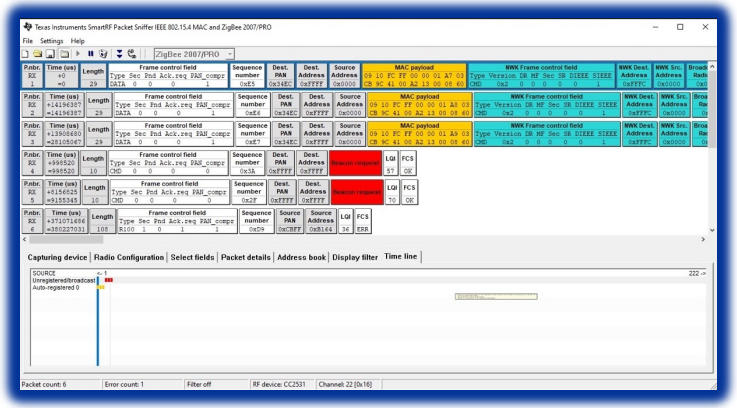
Focus primarily being the data flows into and out of the EVSE that could be exploited for theft of theft of credentials, theft of service, or other malicious exploitation of the system via MITM, replay attacks or DOS.

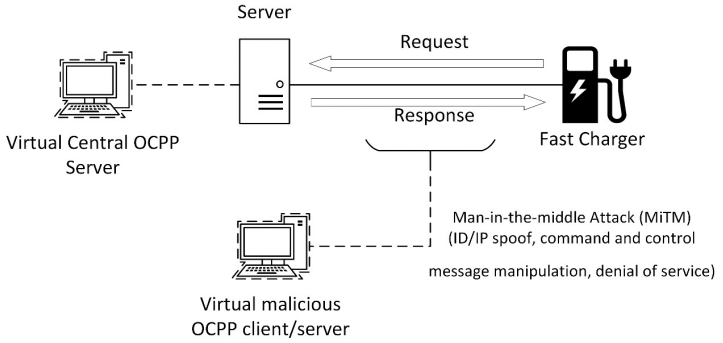
- Use of standard controls could benefit in mitigating the associated risks.
- Encrypted channels for communication, message authentication methodologies, along with intrusion detection technologies would all aid in creating a secure, layered defense against a multitude of threats

NREL

Testing of several cybersecurity aspects of the EV charging ecosystem using hardware, software emulation, and cloud interfaces.

- Outcomes contribute to improving our understanding of the tools and test methods available for security testing of EVSE infrastructure in addition to identifying potential gaps and enhancements to the cybersecurity posture.
- Use of encryption and authentication methods in current and future standardized OCPP implementations is highly recommended.

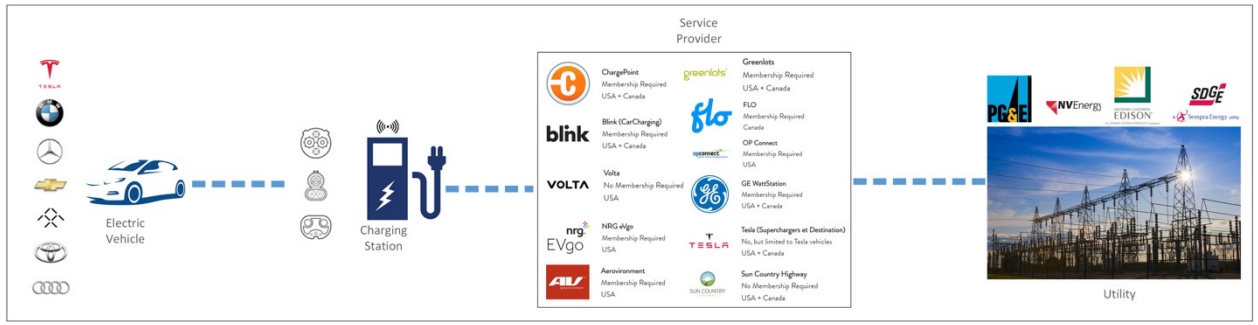




Overarching solutions (e.g., S-NIC) handling all communications with encryption can be developed and deployed broadly.

Tool Architecture Illustration: OSA Cloud Computing Pattern

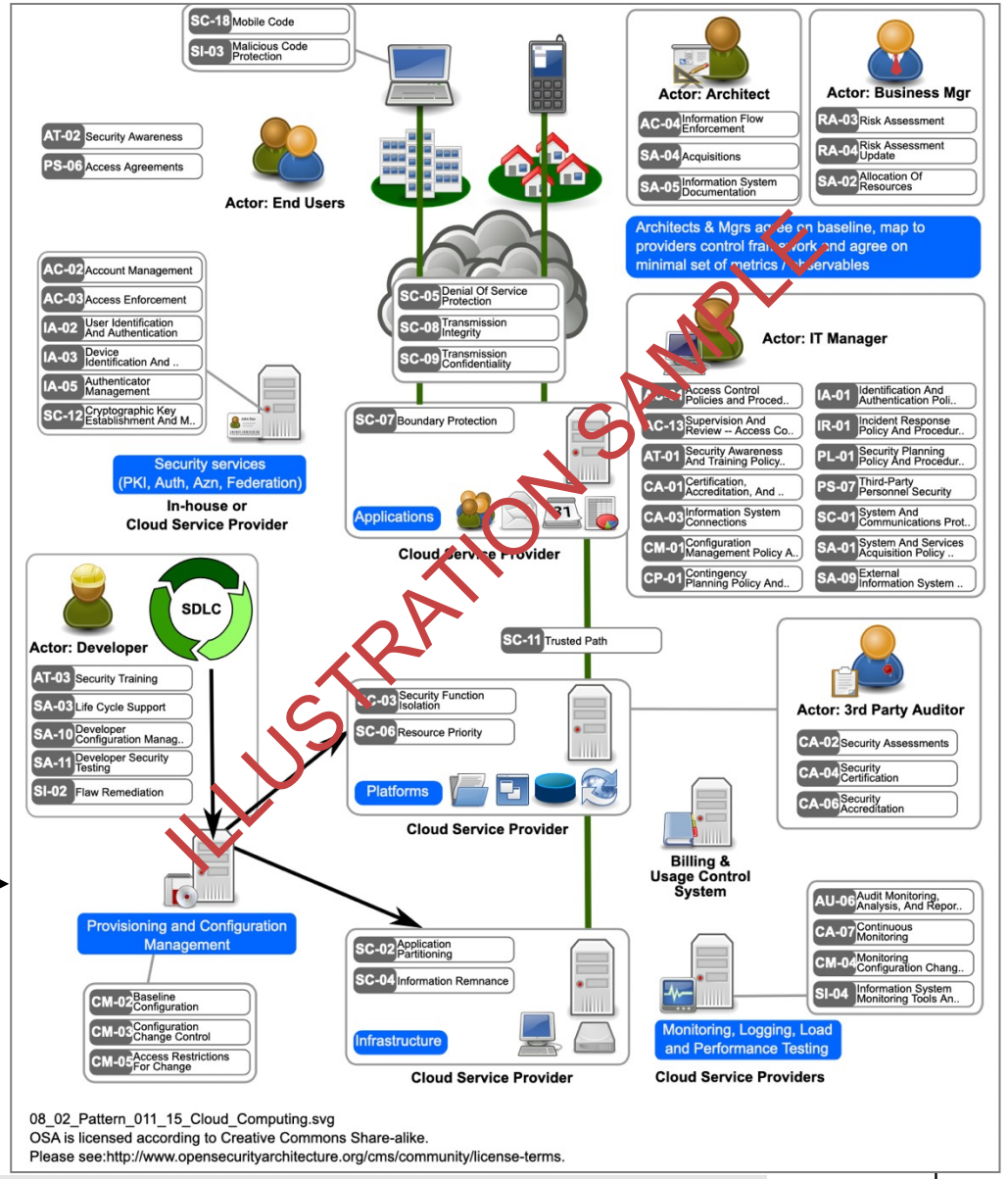
XFC Ecosystem



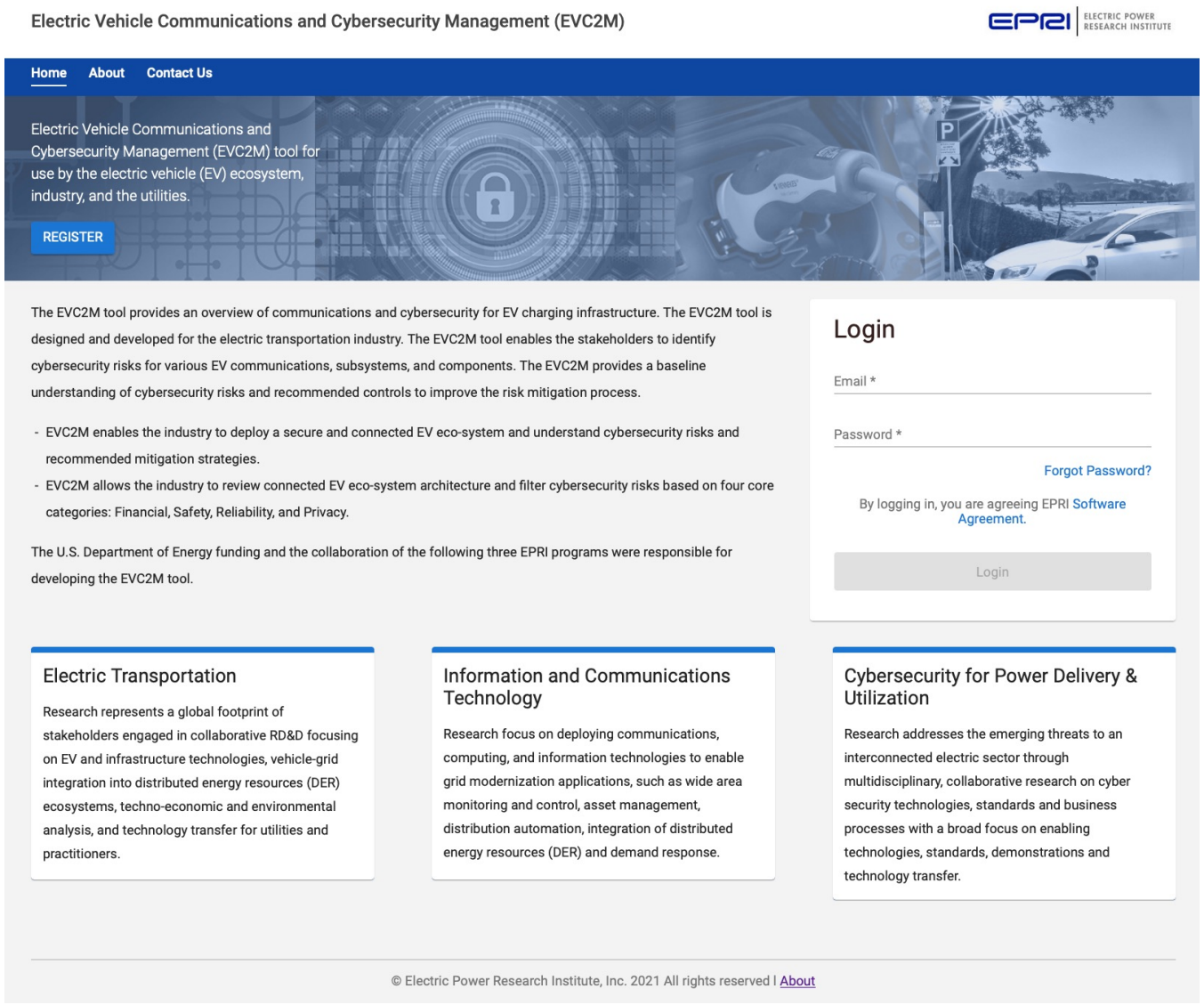
Sub-system | Sub-system | Sub-system | Sub-system

- Component
- Component
- Component

- Safety
- Reliability
- Financial
- Privacy



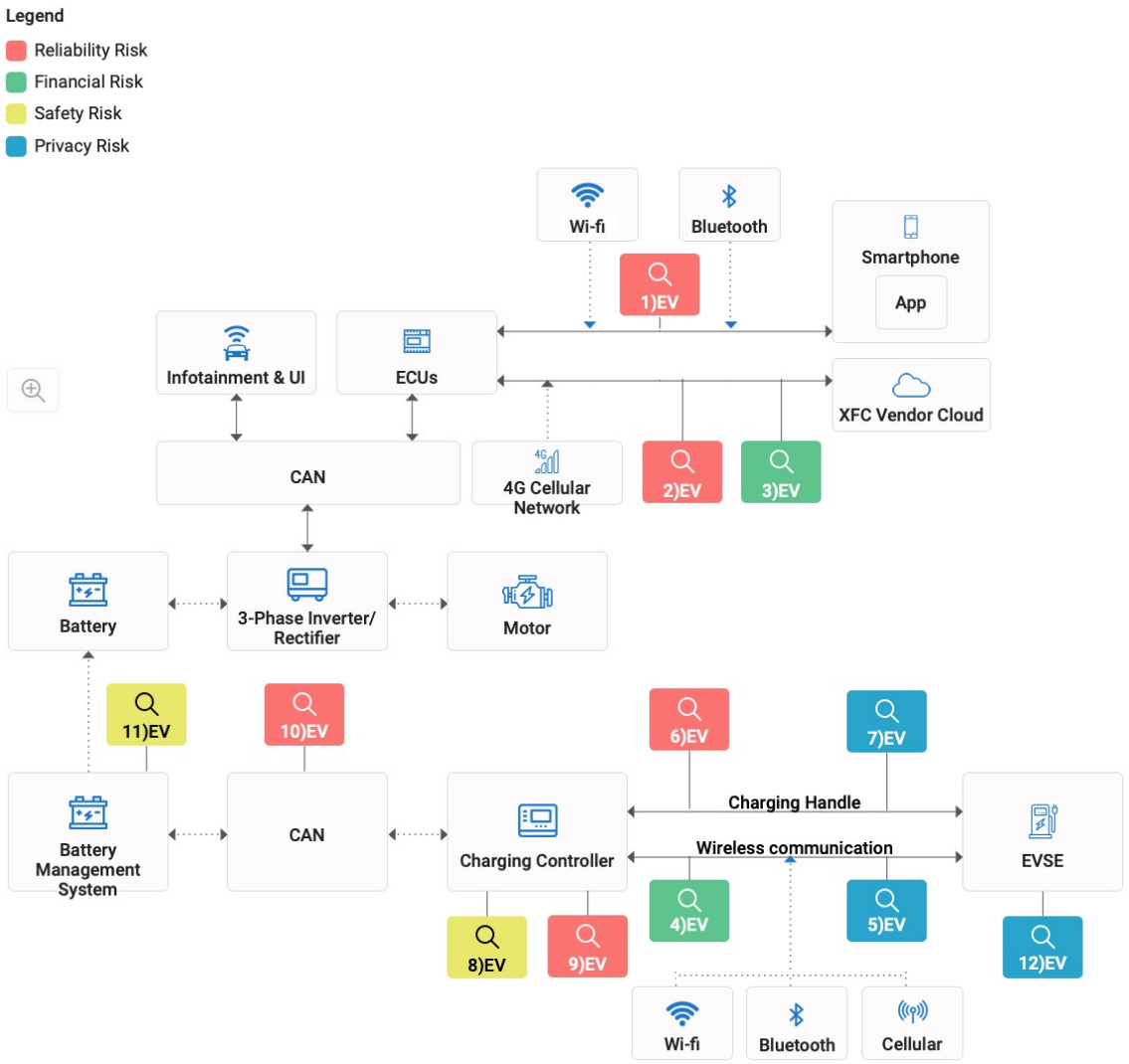
EVC2M Tools for Integrated Grid Security Risk Management



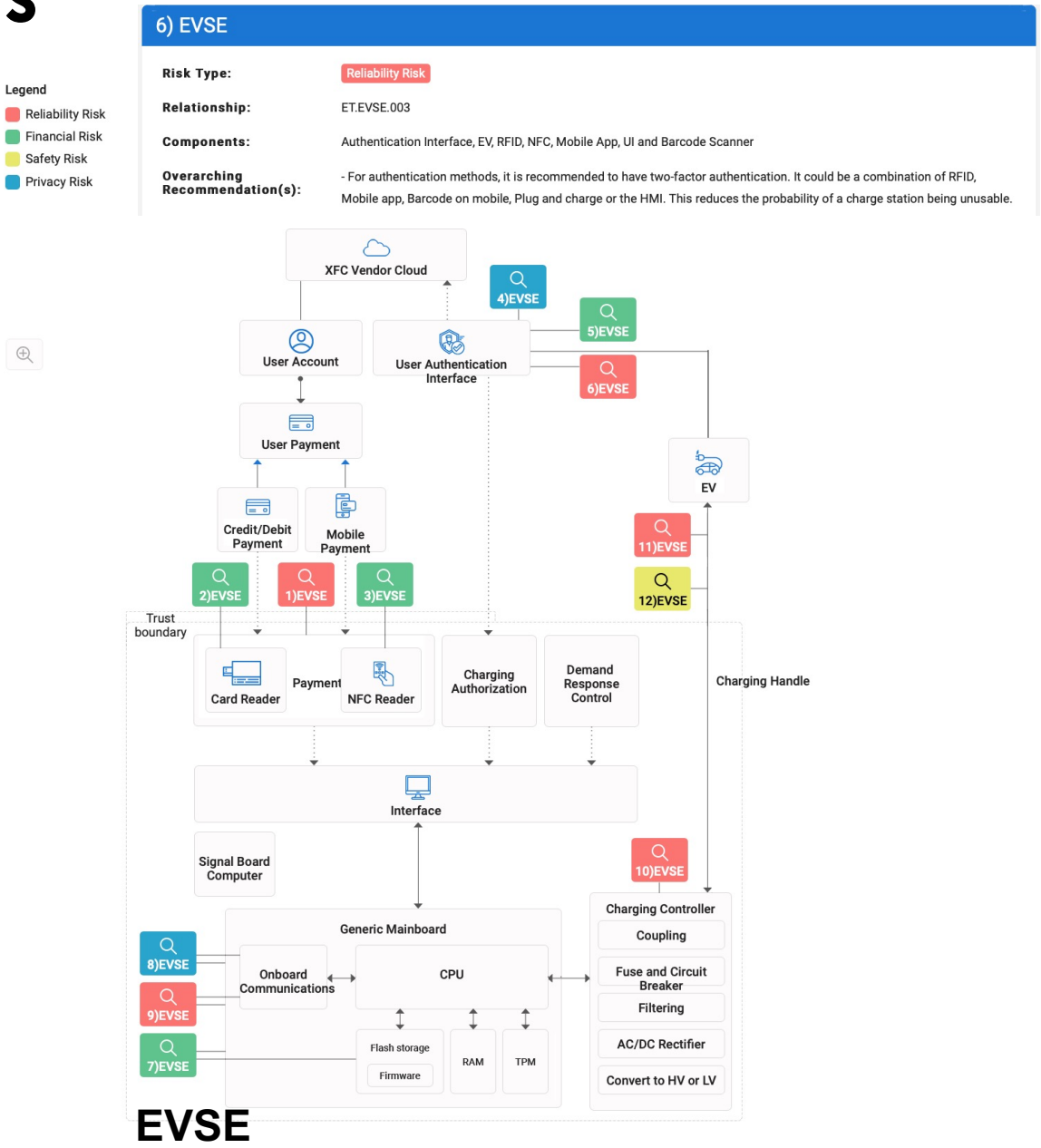
- Ability to scope stakeholder, risk type, sub-system, components.
- Allow free navigation to quickly scale from overall XFC-infrastructure to sub-system level.
- Ability to review reference architecture along with detailed risks, assets and security control information.

Front End	Angular 10
Backend	Java 11
Database	PostgreSQL12.3
Operating System	CentOS 8
Browsers	Firefox 68+ Google Chrome 72+ Internet Explorer 11 Safari 13+

EVC2M: EV and EVSE Subsystems



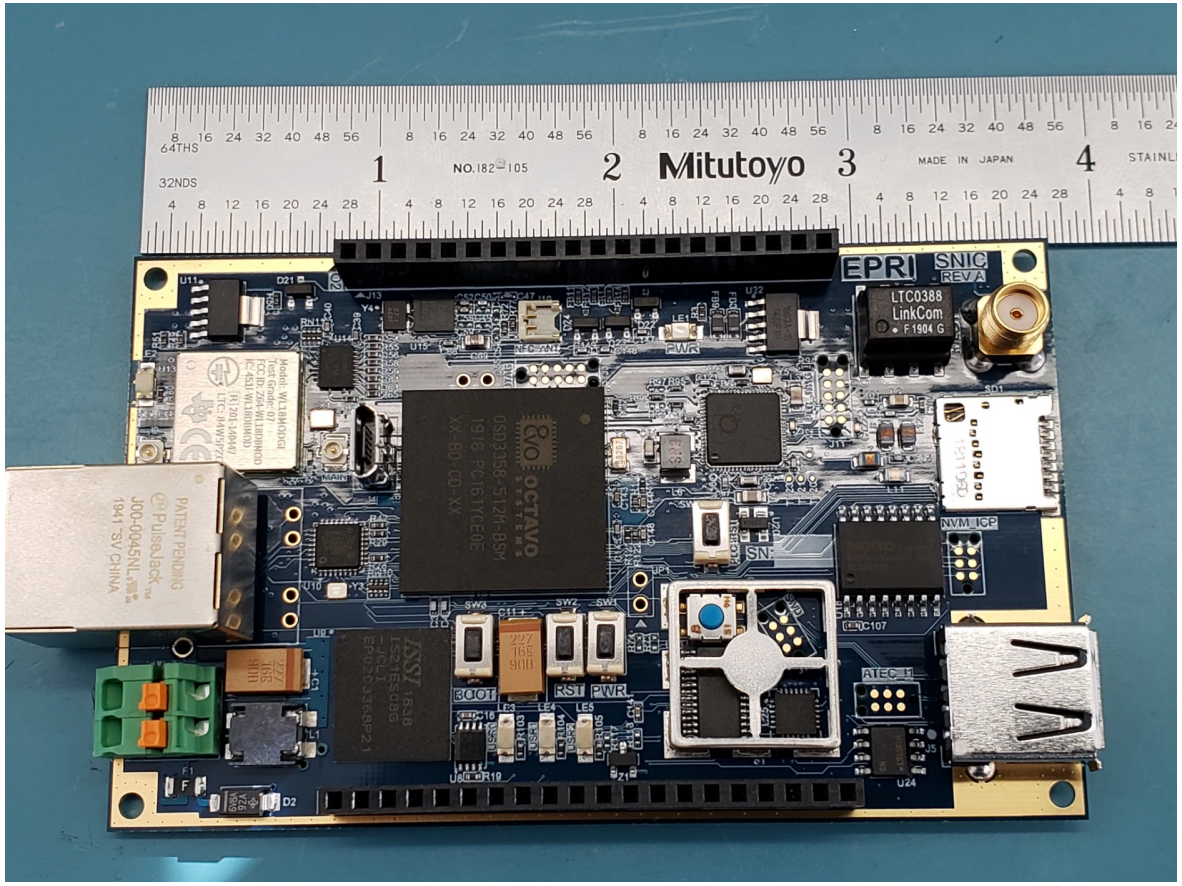
EV



EVSE

Secure Network Interface Card (S-NIC)

- The SNIC will play a key role in testing communication security.
- The SNIC will act as a wrapper to all communications originating from any of the subsystems
- The SNIC will provide protection to hardware from tampering and verify changes to firmware and boot operations.
- The major components of the system:
  1. Central Processing Unit/System
  2. Vehicle Communication
  3. Cloud Communication

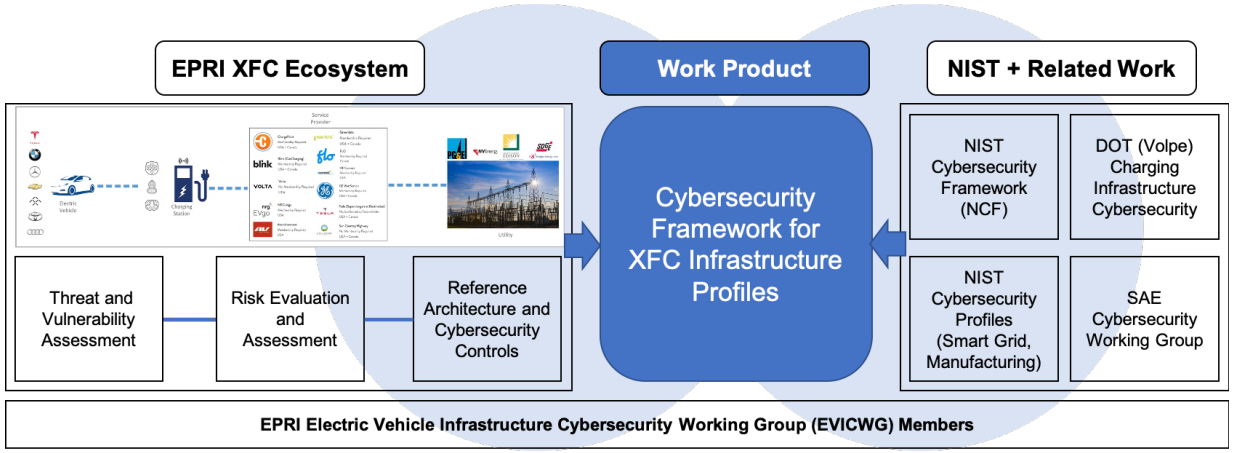


Impacts (2020)

1. Recommendations to be transferred to a standard enforcement or interoperability certification process to ensure that the reference architecture is effectively applied to all XFC stakeholders and is industry-approved for secure implementation through deployments and regulatory.
2. Industry can review the EV ecosystem subsystems, components, communications, to identify risks and review recommended controls.
3. Industry-facing EVC2M tool can be used for baseline security assessment and implementing recommended controls.

Future Research

1. Continued evolution with assessment capabilities and diversity of charging infrastructure & EVC2M tool.
2. Develop tools and processes for compliant implementation of real-world cybersecure practices & scaling.
3. Develop national-level cybersecurity profile for XFC infrastructure that aligns with NIST framework.



Summary

The project focuses is on creating uniform, system-wide and balanced EV XFC Infrastructure cybersecurity best practices for the practitioners to implement.

1. The 2019 research defined the ecosystem actors, analyzing of the entire ecosystem, identifying risk areas and creating applying the methods for assessing the risk
2. The 2020 research focused on on physical testing of cybersecurity requirements on physical infrastructure, testing and application of Secure NIC and public dissemination of the test results.
3. Future goal would be to incorporate the best practices within a standards construct with SAE, IEEE or NIST collaborative activities.

Project Goals

- Uniform system-wide requirements
- Active, broad stakeholder team
- Component → System test for requirement verification
- Secure Network Interface Card Open-sourcing of hardware and software design
- Technology transfer through EV Infrastructure Cybersecurity Working Group
- Coordinated effort with wider Federal, State and utilities
- Industry coalitions with EPRI, as the forum for collaboration and adoption

SOPO Timeline and Key Milestones – 2018-19

Milestone	Type	Description and Status	Delivery Date
Risk Matrix Completed	Technical	Risk matrix for each ecosystem subfunction completed.	Q1 2019 → 3/29/19
Working Group Created	Technical	EV Infrastructure Cybersecurity WG (EVICWG) created.	Q1 2019 → 3/29/19
Vulnerabilities and Threats Identified	Technical	Security vulnerabilities and threats for each subsystem identified.	Q2 2019 → 6/28/19
Secure Network Interface Card	Technical	Network interface card open source retrofit	Q2 2019 → 6/28/19
Subsystem Security Requirement Complete	Technical	Subsystem security requirements.	Q3 2019 → 9/30/19
Draft Reference Cybersecurity Architecture Completed	Go/No Go	Draft reference cybersecurity architecture.	Q4 2019 → 12/20/19

Completed Tasks

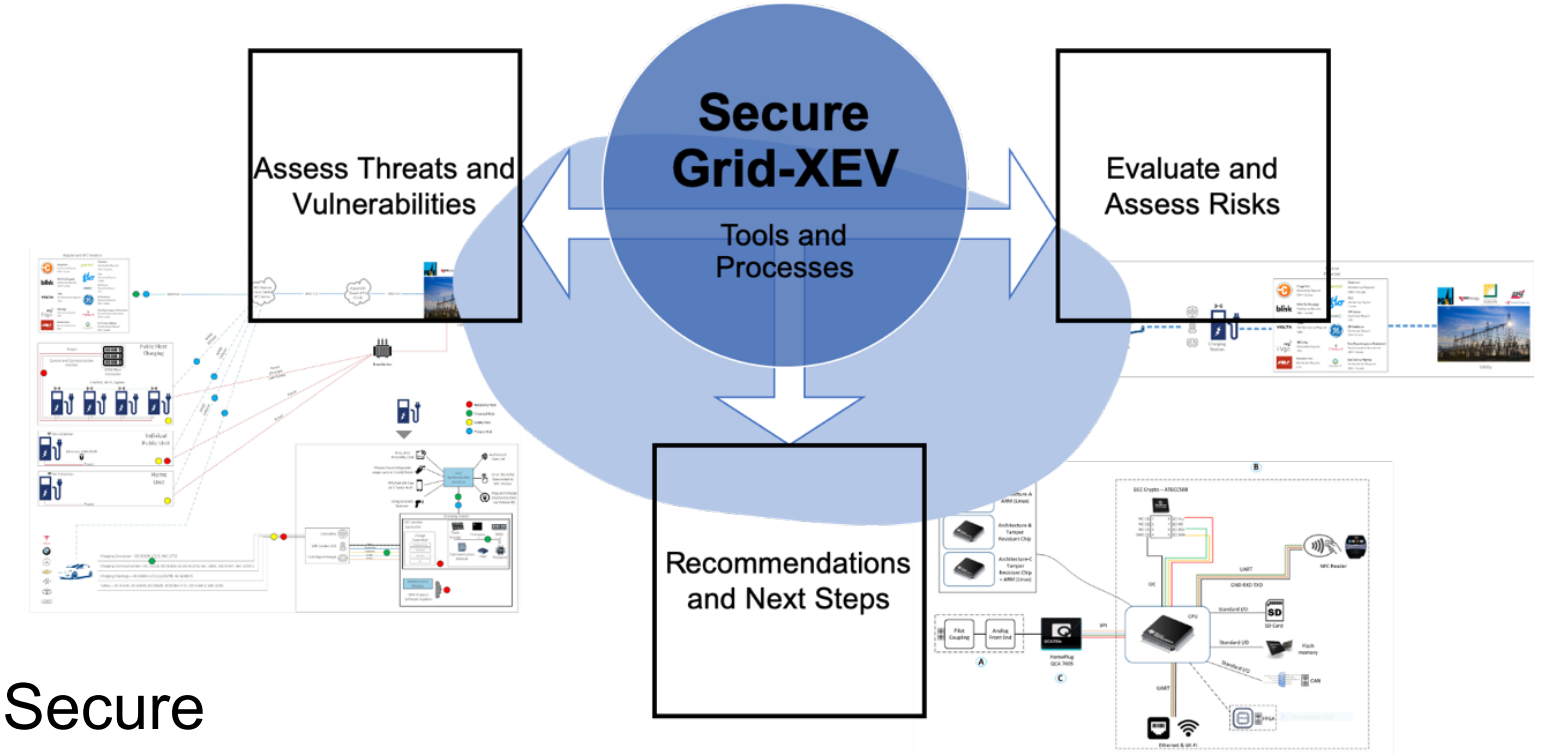
Pending Tasks

EPRI completed the draft public-report of 2019 activities
(DOE review in process)

2019 Research Summary

- Activities focused on the four core areas:

1. Assess cybersecurity requirements;
2. Conduct risk, threat, and vulnerability assessment;
3. Mainstream research;
4. Recommend cybersecurity controls, XFC ecosystem reference architecture, and Secure Network Interface Card (S-NIC) reference design.



Technical Status: Mapping Outcomes to 2020 Test Plans and Testing

Laboratories and Test Cases	Relation to Key Recommendations
EPRI Cybersecurity Research Laboratory (CSRL) 1. Spoof Payment / Authentication System – SNIC 2. Evaluation of attack surface of UI 3. Evaluating functional behavior of EVSE in absence of network or un-responsive Charging service provider 4. EVSE Communications channel vulnerability assessment 5. Maliciously exploit EVSE API 6. Theft of Credentials or Keys	• PKI for end devices and their clouds. • Encryption of PII, data at rest and in motion • Secure NIC • 2-way communication between EVSE and cloud (Bi-directional) with defined alert stack.
National Renewable Energy Laboratory (NREL) 1. Man in the middle attack 2. Denial of Service attack 3. Communication chain EVSE to Cloud	• PKI for end devices and their clouds. • Encryption of PII, data at rest and in motion • Secure NIC
Argonne National Laboratory (ANL) 1. Network Level Site Controller: Evaluate dependencies of EVSE-EVSE interactions in clusters and the site controller. 2. Evaluate security of EVSE communications within a facility. 3. Test integrated energy storage, DC as a service with an EVSE. 4. Evaluate Confidentiality, Integrity and Availability (CIA) for communication between cloud/back-end and the EVSE.	• PKI for end devices and their clouds. • Encryption of PII, data at rest and in motion • Secure NIC • Load Smoothening by deploying power dense storage solutions.

Cybersecurity Testing Capabilities

EPRI Cybersecurity Research Lab (CSRL)

- Utility-system focused cybersecurity testbed
- Specialized EVSE equipment and tools for cybersecurity penetration testing

National Renewable Energy Laboratory (NREL)

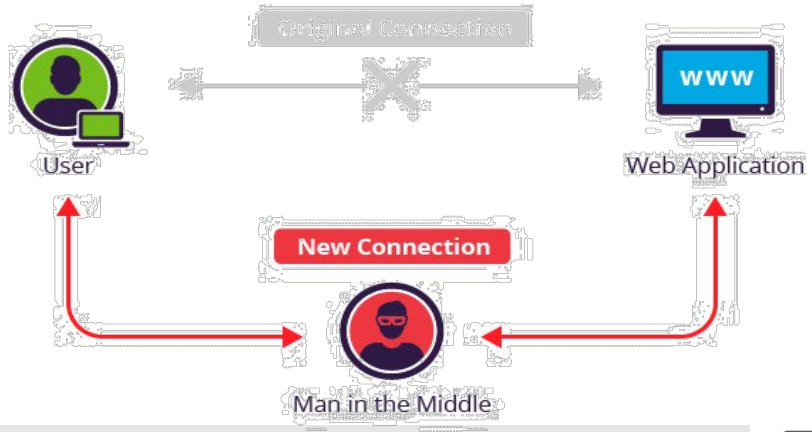
- System level testbed including distribution system simulation
- Isolated circuits to provide visibility into individual test cases and consequences

Argonne National Laboratory (ANL)

- Responsible for testing Subsystem-level cybersecurity
- Access to flexible XFC and other charging equipment as well as EVs

Testing Capabilities

- **The CSRL has a library of utility focused cyber security use cases that can be run against test beds to demonstrate the effectiveness of architectural changes or the introduction of new technologies.**
- **Specialized Exploits Available**
  - Advanced Man-in-the-middle (MITM) attacks utilizing ARP spoofing and IP hijacking
  - IEC/ISO 15118-2 and SAE J2847/2 and other protocols
  - CrashOverride / Industroyer, Havex, Black Energy and DragonFly malware
- **Penetration Testing**
  - Fuzzing
  - Vulnerability Scanning
  - Attack Surface Evaluation



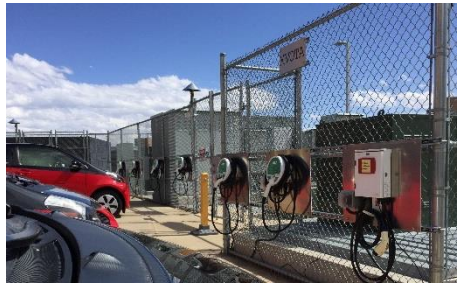
Argonne National Lab Test Setup for Component Level Cybersecurity Verification

26

NREL ESIF Test Setup for EV Infrastructure System Level Cybersecurity Verification

Facility Smart Charge Management

Energy Security and Resilience



Distribution Vehicle to Grid Impacts

DCFC Systems Integration

27

Impacts (2019)

1. Defined and validated uniform cyber-security technologies and engaged a diversity of industry stakeholders
2. Developed architecture and system-specific modular security controls
3. Developed recommended controls across the EV XFC Charging Infrastructure and electric grid ecosystem to support secure deployment and grid integration of EV charging infrastructure.

28