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

Presenters: Sunil Chhaya – Sr. Technical Executive, Electric Transportation**, Rish Ghatikar – Sr. Program Manager –** Information, Communications, and Cybersecurity

06/04/2020

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

Outline

- Overview
- Relevance
- Milestones
- Approach
- Technical Accomplishments and Progress
- Responses to Previous Year Reviewers' Comments
- Collaboration and Coordination with other Institutions
- Remaining Challenges and Barriers
- Proposed Future Research
- Summary Slide
- Technical Back-up Slides
- Critical Assumptions/Issues

Overview

Timeline

- October 2018 - December 2020
- 60% complete

Barriers

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

Budget

- $2.2M Total project funding
  - $1.7M DOE Share
  - $.5M Cost share

Partners

- EPRI (Prime)
- Kitu Systems
- Automation Research Group
- GreenLots
- Argonne NL
- NREL

Objectives

- 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 utility industry coalitions with EPRI as the forum for collaboration

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

10/2018 → **12/2020**

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

Project Objectives and Features

Objectives

Phase 1

- 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

- 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

Project Approach: Budget Period 1

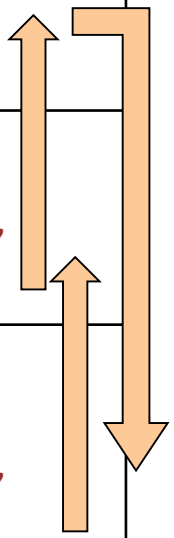
Milestone	Type	Description and Status	Due Date
Risk Matrix Completed	Technical	Risk matrix for each ecosystem subfunction completed.	Q1 2019 → 3/29/19
Working Group Created	Technical	EV Infrastructure Cybersecurity WG (EVICWG) created.	Q1 2019 → 3/29/19
Vulnerabilities and Threats Identified	Technical	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

Planned additional public-report of 2019 activities

Project Approach: Budget Period 2

Milestone	Type	Description and Status	Delivery Date
End-to-End Security Test Plan	Technical	Cybersecurity testing plans.	Q1 2020 → **Draft submitted to DOE, 3/31/20.**
Cybersecurity Testing	Technical	Testing complete with results documented.	Q2 2020 → Due to COVID-19 challenges, planned completion by **Q4 2020.**
Integrated Grid Security Risk Management (IGSRM) Tool Finalized	Technical	Tool developed and updated based on testing results.	Q3 2020 → Due to rescheduling of testing, planned completion by **Q2 2020.**
Integrated Grid Security Risk Management Tool Published	Technical	Reference architecture is market-ready for implementation through industry deployments and regulatory framework.	Q4 2020 → Due to rescheduling of testing, planned completion by **Q3 2020.**



Completed Tasks **Pending Tasks**

Plan to publish public document with best practices with collaboration from the project team, national laboratories, and the industry

Responses to Reviewer Comments

Engagement of existing work and other standards agencies?

- EV Charging Infrastructure Cybersecurity Working Group is *the* central body primarily set up for external engagement and coordination
- Participated in VTO-led cross-industry collaboration involving DoT, DoE, DoC, DoD, labs, universities, FOA 1919 awardees for building on common tools
- Specifically, leveraging INL and Sandia work on detailed subsystem analysis and frameworks
- Contributing to DoT MD/HD infrastructure cybersecurity work

What are the steps taken to ensure efficient engagement of the industry members within and outside the project?

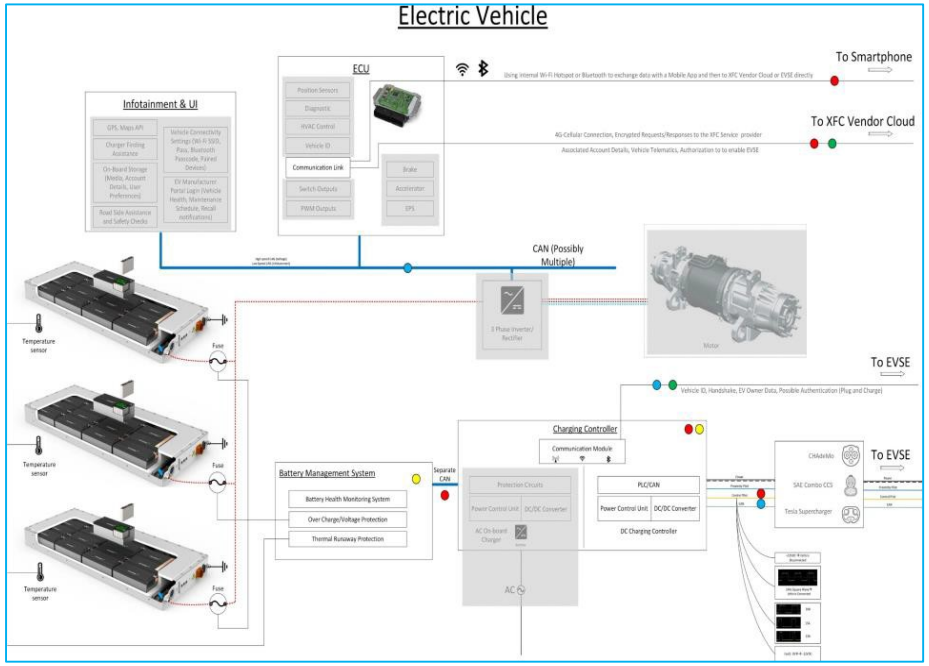
- Biweekly reviews with EVICWG
- Deliverable discussion and reviews / comments sought for the project
- Project team involves industry leaders and standards representatives directly taking learnings back to their respective activities

How will the qualitative assessments from the project be assessed against real-world scenarios or productization?

- Project involves both requirements and test plans (theory) and their implementation on SecureNIC as well as functional testing at ANL and NREL.
- Additional technology transfer through active engagement of equipment providers and EVSPs

Technical Status: Component or Asset-Level Threat & Vulnerability Assessment

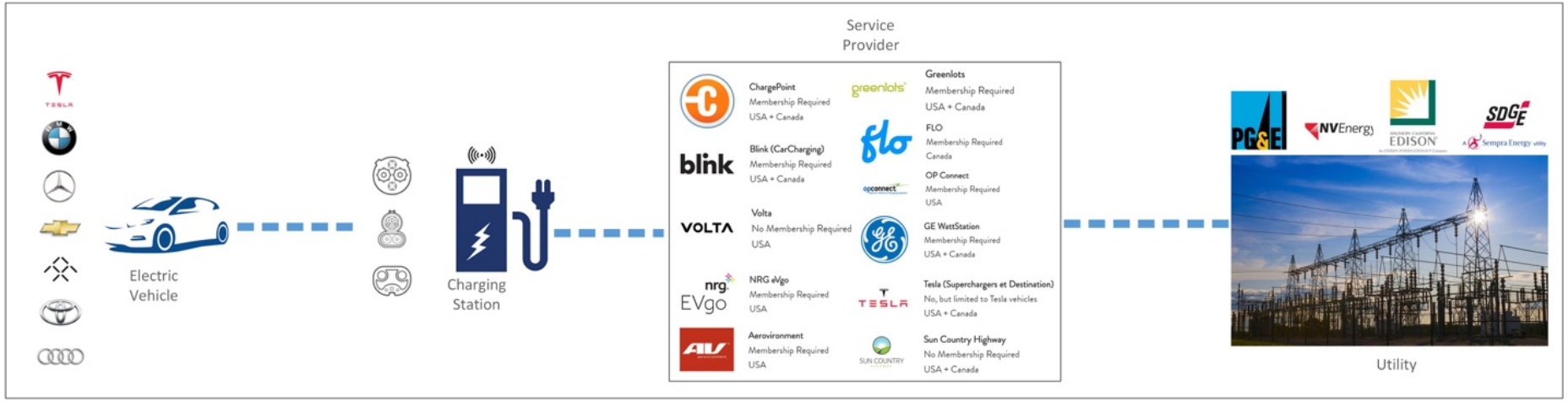
- Each sub-system assessment includes matrix that elaborates threat & vulnerability for each component and their assets.
- Results used recommend cybersecure architecture and controls.



Threat and Vulnerability Assessment for XFC Sub-Systems

No.	Components	Assets
1	Smartphone-Vehicle Communications, Android/IOS application, Bluetooth, Wi-Fi Hotspot, Smartphone memory (internal/external)	Customer PII, Payment information saved in the application, user credentials.
2	XFC Vendor Cloud - Vehicle Communications, vehicle cell modem, vehicle telematics.	Vehicle PII, XFC Vendor Cloud, Decisions made by the cloud.
3	Smartphone, EV and the XFC Vendor cloud, Apple Car-play and Android Auto.	User contacts, PII, Payment information saved in the application and user credentials for the cloud.
4	EV Charging Controller, EVSE, Wired Communication, RF/Wi-Fi.	Financial details, payment information and identity.
5	EV Charging Controller, EVSE, Wired Communication, RF/Wi-Fi.	User and EV privacy, EV-Charging profile.
6	EV Charging connector-female, EVSE	EV side controller, Charging connector and the charging service
7	EV Charging connector-female, EVSE	Handshake details, charging protocol, detailed signal data
8	EV Charging controller, Firmware	Charging service, EV controller, EV charging functionality
9	CAN bus/OBD Port, EV Charging Controller and communications	Charging service, EV controller, EV charging functionality

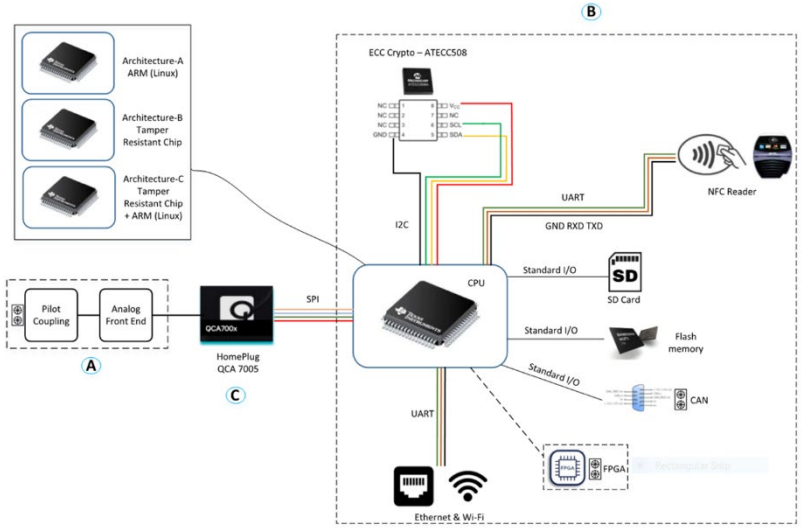
Technical Status: Recommendations: System Architecture, Cybersecurity Controls



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



Technical Status: Mapping 2019 Recommendations to Q1 2020 Test Plan

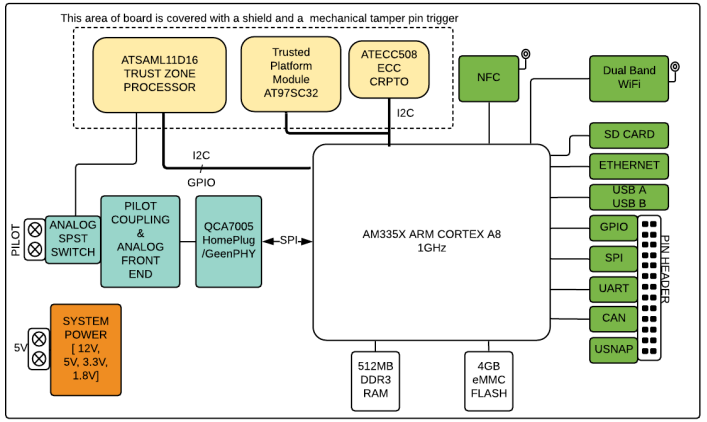
Laboratories and Test Cases	Relation to Key Recommendations
EPRI Cybersecurity Research Laboratory (CSRL) 1. Spoof Payment / Authentication System – SNIC 2. Evaluation of attack surface of UI 3. Evaluating functional behavior of EVSE in absence of network or un-responsive Charging service provider 4. 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.

Technical Status: EPRI Open-Sourced Secure Network Interface Card

Open Grid Interface API,
Local EMS + OCPP,
EPRI IEEE 2030.5 server;
IEC/ ISO 15118 Server

SAE J1772 PWM
Pilot w/ IEEE
2030.5 or IEC/ISO
15118 /PLC

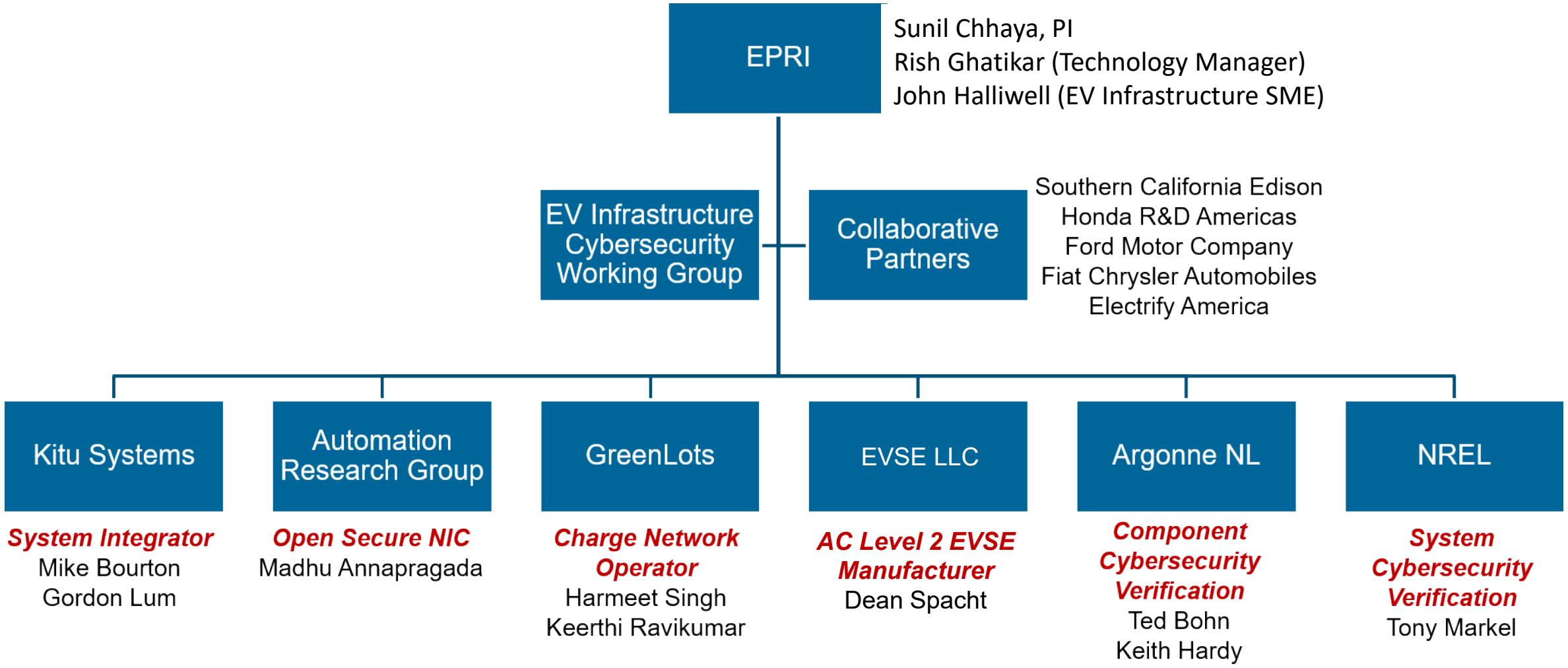
Open-Sourced Secure Network Interface Module for EVSE and XFC



Source: Automation Research Group

Secure Open Standards Network Interfaces, for built-in Cybersecurity Compliance

Collaboration and Coordination



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

Impacts

The project has:

1. Defined and validated uniform cyber-security technologies and engaged the industry
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.

Future Research

1. Publicize the assessment and recommendations to the XFC ecosystem
2. Develop a reference Secure NIC prototype and IGSRM tool
3. Test security controls to real-world applications

Testing Capabilities

EPRI Cybersecurity Research Lab (CSRL)

- Utility-focused cybersecurity testbed
- Specialized equipment to provide penetration testing
- Developing Integrated Grid Security Risk Management Tool (IGSRM)

Argonne National Lab

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

NREL Energy System Integration Facility (ESIF)

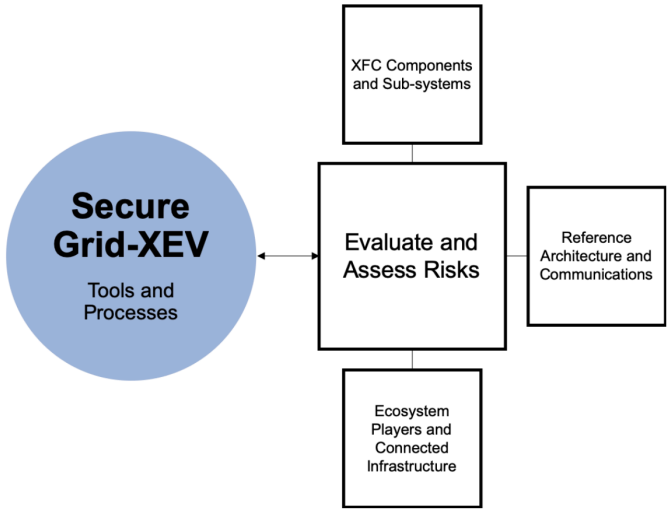
- System level testbed including distribution system simulation
- Isolated circuits to provide visibility into individual test cases and consequences

Summary

- The project focus is on creating uniform, system-wide and balanced EV XFC Infrastructure cybersecurity best practices for the practitioners to implement
- The best practices are being vetted through the engagement of all the stakeholders of the ecosystem as well as through the physical testing and application of the techniques on actual infrastructure representations
- BP1 covered the first phase of this work defining the ecosystem actors, analyzing of the entire ecosystem, identifying risk areas and creating applying the methods for assessing the risk
- BP2 will focus on physical testing of cybersecurity requirements on physical infrastructure, testing and application of Secure NIC and public dissemination of the test results
- Future goal would be to incorporate the best practices within a standards construct with SAE, IEEE or NIST collaboration

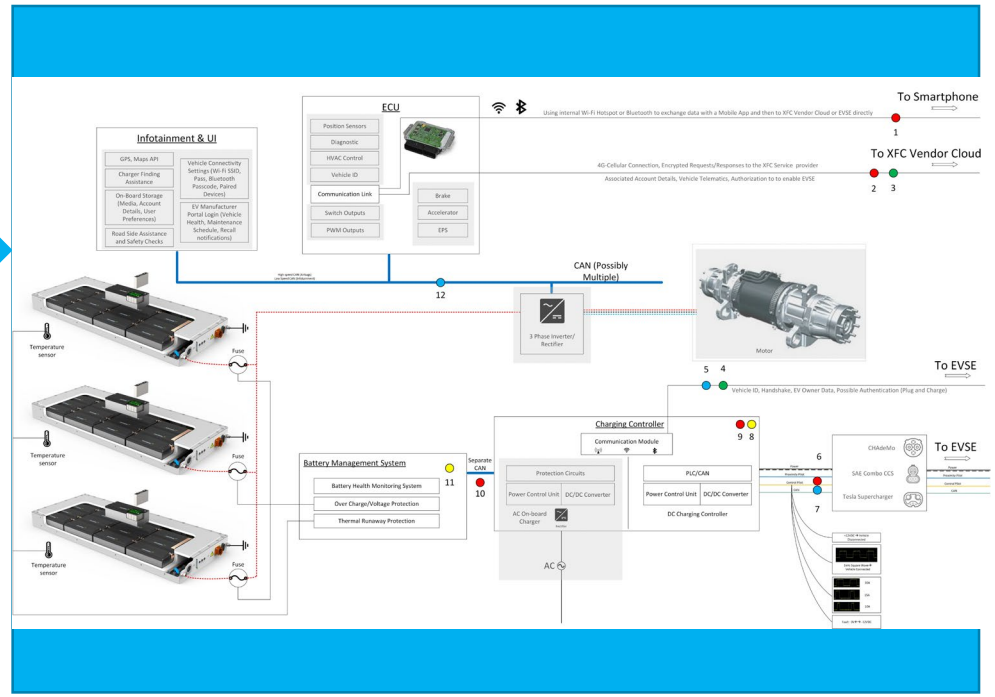
Technical Backup Slides

Technical Status: Component or Interface-Level Risk Assessment



- Each ecosystem component & system interface evaluated
- A risk type was assigned for each component / interface:
  1. Reliability
  2. Privacy
  3. Financial
  4. Safety

- Sub-systems assessment:
  1. EVSE/XFC
  2. Electric Vehicle
  3. XFC Third-Party Network (Cloud)
  4. XFC and Facility, Utility Interfaces.

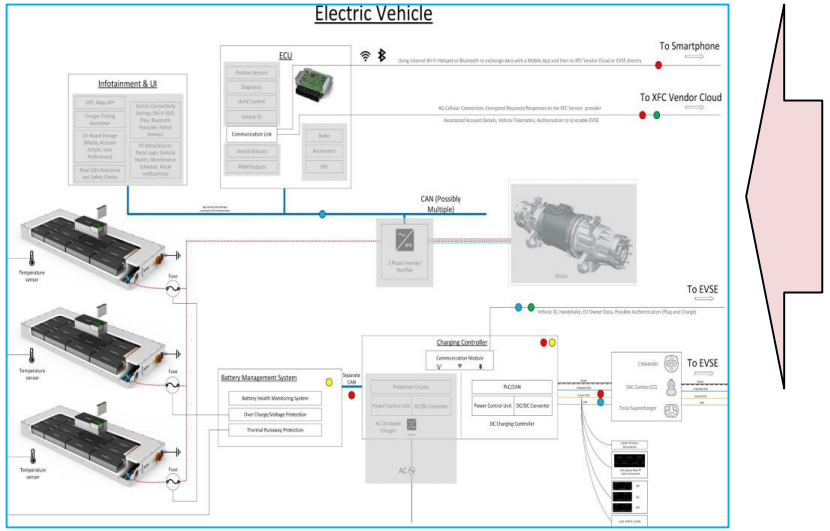


Generic Architecture for Components and Communications for an EV Sub-System

Technical Status: Risk Assessment and Description

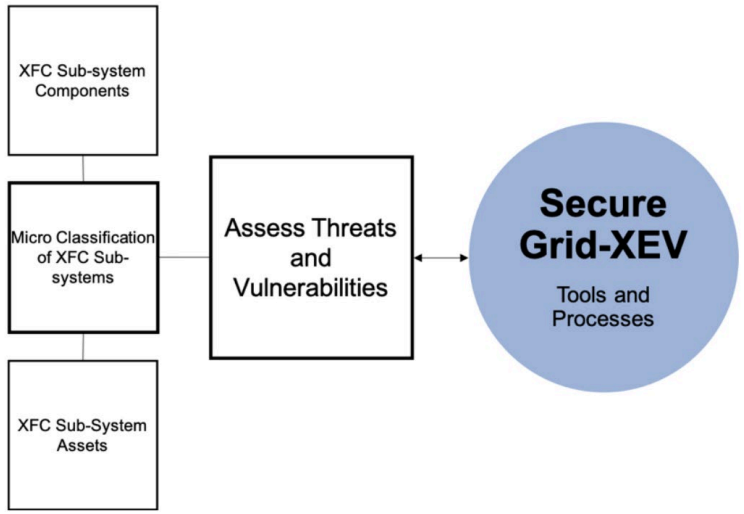
- Each sub-system assessment included a risk matrix that elaborated the risks.
- Results used to prioritize threats and vulnerabilities
- Controls and communications requirements are derived form risks.

- Similar exercise for threat and vulnerability assessments



#	Components	Category	Risk Description	Consequences
1	Communication between Smartphone and EV via Wi-Fi	Reliability Risk	Data/Control flowing between the mobile application and EV is through cellular/Wi-Fi or Bluetooth which can be intercepted.	This can bring in reliability issues for the user and his interaction with the EV.
2	Communication between EV and XFC Vendor Cloud	Reliability Risk	Possible modification of data/request being sent to XFC Vendor Cloud to trigger/stop charging when not desired.	Attack on this pathway can allow the attacker to control/see what is being sent to the cloud.
3	EV, smartphone and XFC Vendor Cloud, 4g-Cellular communication	Financial Risk	Account credentials, Vehicle Telematics and payment information are vulnerable to theft during exchange between cloud, EV and smartphone.	Payment details/Account Details breach can pose heavy financial risk to the users and cloud service providers.
4	EV Charging Controller, EVSE, Wired comm., RF/Wi-Fi	Financial Risk	Data theft when EV is directly communicating with the EVSE to handshake, authenticate, authorize. This could be over the wire (Connector) or Wireless.	The bad actor can get lot of details, probably impersonate/replicate the actual vehicle's presence to get free charge.
5	EV Charging Controller, EVSE, Wired comm., RF/Wi-Fi	Privacy Risk	If the EVSE and EV talk on Wi-Fi or RF, there is a risk of anyone intercepting/capturing packets and spy on sensitive information	Lot of PII regarding the user/EV can be captured.
6	EV and EVSE charging connector plug	Reliability Risk	Modification of the connector plug or replacing with a 3rd party plug can cause reliability issues.	Possibly irregular current flowing through the harness, power directed elsewhere.
7	EV and EVSE charging connector plug	Privacy Risk	Risk of identifying charging patterns, vehicle data, protocols etc. by modifying the charging connector/adding a spy chip/hardware to it.	Tiny wireless chips when planted can provide valuable insights to the attacker.
8	Charging Controller	Safety Risk	Risk of firmware/Hardware modification. Protection envelopes being disabled, wrong charge parameters being communicated etc.	This can pose a safety risk because now the vehicles charge controller is being tricked. Over charge, discharge, missing alerts etc.
9	Charging Controller, Communication Module	Reliability Risk	Modified firmware of charging controller can refuse to charge a battery, over charge or discharge at the attacker's will.	Possible DOS, the user will be uncertain about the charging behavior of the EV; unless firmware is fixed
10	CAN Bus for Charging Controller, Communications	Reliability Risk	Manipulation of vehicle's CAN bus specific to charge controller can hand complete control of charge system to attacker	This would be dangerous since vehicles integrity is still intact, yet the bad packets on CAN pretend to be authentic.
11	Battery Management System CAN connected to it and Charging Controller.	Safety Risk	Gaining access on the CAN bus specific to Charging and BMS can potentially disable safety systems in place for the battery packs.	Possible thermal runaway, undesired behavior of the EV anywhere within the charging cycle/process.
12	CAN, OBD-II and PLC	Privacy Risk	Setting up a clone EVSE can allow Sensitive Data going out of these ports to be captured.	Sensitive data related to vehicle is captured by malicious EVSE.

Component or Interface-Level Threat & Vulnerability Assessment



- Identified asset-specific threat and vulnerability for each of the sub-systems, its potential business impacts, and proposed mitigation strategies

- Classified assets into three groups:
  1. Information
  2. Equipment
  3. Service

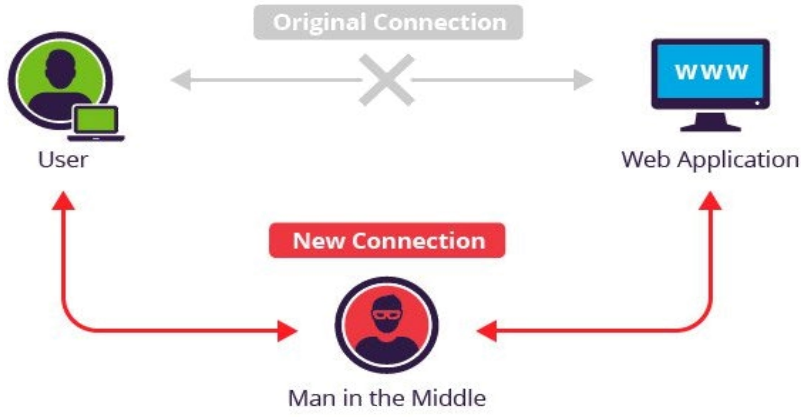
Generic Architecture for Components and Communications for an EV Sub-System

Information	**Refers to customer information, personally-identifiable information (PII), payment information, EVSE firmware, human machine interfaces (HMI) passcodes, network credentials, vehicle location, charging telematics, charge control parameters, vehicle ID, private keys, on-board storage of EVSE data, data exchange between cloud and EVSE.**
Equipment	Includes charging station, power/data connectors, payment modules, EV—EVSE communication, controllers, wireless modules (e.g., Wi-Fi, Bluetooth, RF, cellular,), power electronics, HVDC components, site controller, power cabinets, cooling systems, sensors (e.g., temperature), connected relays, fuses, emergency disconnect, circuit breakers.
Service	Charger availability, payment process, authentication, start charging, end charging, handshake , plug and charge, cloud-based communications, over-the-air or connected software update for EVSE, charging schedule, smartphone communications with EVSE.

Asset	Description

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

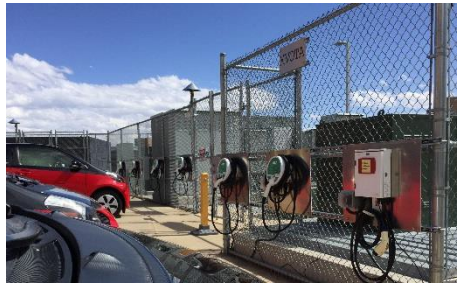


Argonne National Lab Test Setup for Component Level Cybersecurity Verification

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

Critical Assumptions / Issues

- A 100% cybersecure system is beyond the scope of this project
- The challenge is where to draw the line as to defining the breadth and depth of the work on this project
- The goal is to apply the industry best practices to design-in multiple layers of cybersecurity protection mechanisms through hardware, software and system design, for EV XFC Infrastructure, and avoid reinventing the wheel
- Goal is also to apply standards where necessary, and identify gaps to create new standards as appropriate
- Broad industry stakeholder collaboration and broad dissemination of the information intended to create an industry-wide dialog and engender cybersecurity awareness, through publications from this project
- Direct engagement of XFC Vendors has been a challenge – they are not available. We are circumventing this issue by working through ANL and NREL to engage with them (BTC Power and Efacec have ongoing commitments with the labs)
- One of the future goals of the project is to directly engage XFC providers through Secure NIC retrofit