EVs-at-RISC: A Secure and Resilient Interoperable Smart Charge Management Control System Architecture for Electric Vehicles At-Scale

PI: Duncan Woodbury

Dream Team

June 23, 2021

2021 DoE Vehicle Technologies Office Annual Merit Review

Project ID: ELT265



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

Overview

Timeline

- Start date: October 1, 2020
- End date: December 31, 2024
- Percent complete: 15%

Barriers

- Utilities and grid operators lack a standard interface to manage and interact with EV, EVSE, and DER assets at the grid edge
- Non-interoperability (heterogeneity of management interface/protocol) limits Smart Charge Management use cases
- Non-standardization of control/communications interfaces expands attack surface, threatens grid cybersecurity and resilience

Budget

- Total Project Funding: $7.05M
  - DoE share: $4.76M
  - Cost share: $2.28M
- FY21: $1.89M

Partners

- DTE Energy
- Idaho National Laboratory
- RunSafe Security
- American Center for Mobility
- RedStone Tech. Integration
- UM Dearborn
- Utah State University
- Oak Ridge National Lab
- NextEnergy
- WSU (Future partner)

Relevance

Relevance:

- **Heterogeneity between EVSE and EV charging systems limits interoperability, increases grid integration cost, expands attack surface, and prevents coordinated asset optimization for Smart Charge Management (SCM) and DERMS use cases**
- **SCM requires a standard interface to deploy software to interact with and manage EV charging infrastructure**
- **SCADA protocols used in distribution networks lack basic capabilities for encryption, authentication**

➢ Lack of basic cybersecurity measures in distribution networks magnify threats from malicious/compromised EVs and EVSE

Objectives:

- **Research and develop an open-source, open standards-based utility Smart Charge Management system**
- **Research and develop secure interoperability solutions for distribution networks that:**

➢ Provide a standardized, extensible, and scalable interface to interact with distribution assets

➢ Reduce the cost, complexity, and cybersecurity risks of EV, EVSE, and DER grid integration

➢ Enable greater operational flexibility (including isolation) and situational awareness at the grid edge

Milestones

AS OF: May 14, 2021	FY21				FY22				FY23				FY24				FY25
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
SCM requirements specification completed																	
Model development and implementation completed																	
System architecture development completed																	
Data model specification completed																	
Demonstrate OpenFMB implementation completed (GO/NO-GO)																	
Integrate system with laboratory hardware																	
Security microservice applications completed																	
Charge control microservice applications completed																	
Grid service microservice applications completed																	
Laboratory demonstration of project use cases completed (GO/NO-GO)																	
Demonstrate interoperability use case																	
Demonstrate smart charging use case																	
Demonstrate cybersecurity use case																	
Demonstrate grid service capabilities																	
Demonstrate system achievement of project goals (GO/NO-GO)																	
Performance report completed																	
Reference architecture specification completed																	
Best practices report completed																	
Distribution of open-source deliverables completed																	

	Complete
	In progress
	Planned

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

Approach

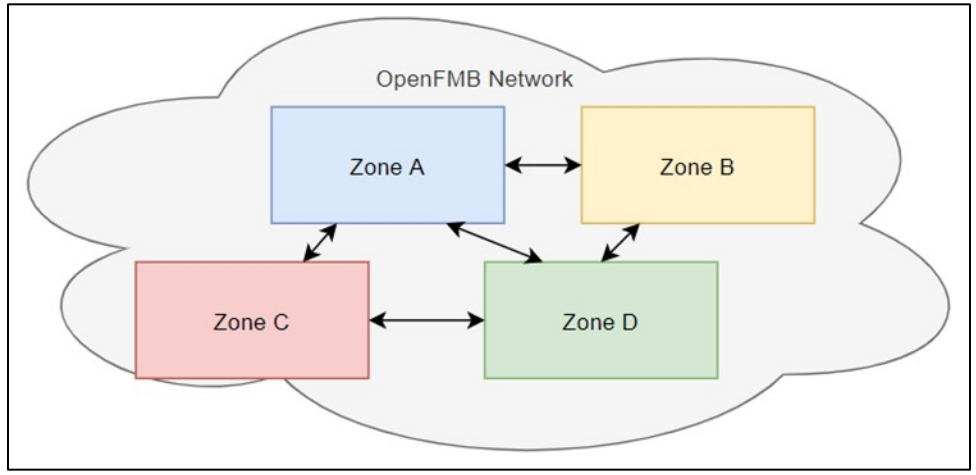
- **Overlay a secure OpenFMB-based middleware framework on existing distribution networks**
  - Standardize a data model for interoperable, protocol-agnostic management and control of cyberphysical assets
  - Extend existing standards (CIM, 61850) to support management and control of EV, EVSE, and DER
  - Standardize interfaces for utility systems, aggregators and service providers, distribution systems, and endpoints (EV, EVSE, and DER)
  - Perform protocol translation at the endpoint/grid edge – scalable and extensible interoperability

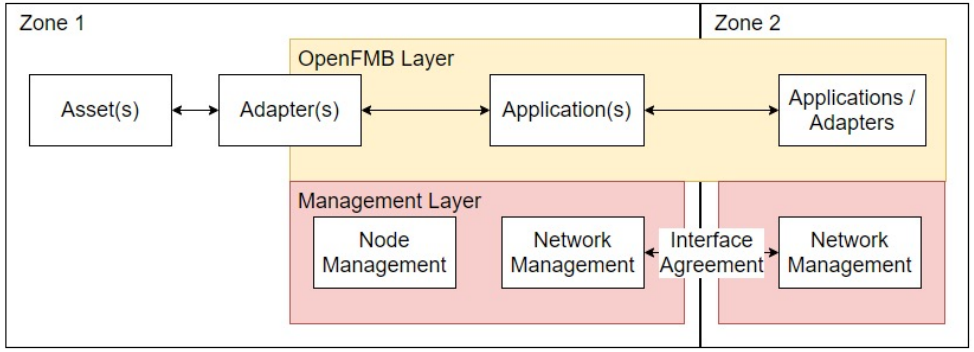
- **Deploy middleware applications to manage and control assets in a standardized way**
  - Realize network-wide capabilities for SCM and cybersecurity use cases

- **Minimize cost – demonstrate secure, scalable, extensible and superior SCM/DERMS capabilities using commodity hardware, free/open-source software, reducing total endpoint cost to < $1,000**

Approach

- Embrace a multi-zonal, multi-party architecture to allow interoperability and arbitrage across utility, RTO/ISO boundaries





- Embrace the open-source model: publish reference architecture, reference implementation, and best practices – equip the industry with open-source capabilities for wide-scale SCM/DERMS

Technical Accomplishments and Progress

- **Milestone 1**: SCM Requirements Specification – complete
- **What it is**: an extensive set of system-level requirements for a utility SCM
- **Why it's important**:

(1) System-level requirements guide design and engineering

(2) These ensure design compatibility with standard regulation and controls (ex. NERC)

- **Next steps**: use these requirements to design and demonstrate feasibility of our system

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

Table of Contents	Total Reqs.	Percent Analyzed	Percent Included
Requirements Volume	Total	% Analyzed	% Included
SEPA DERMS	**716**	**100%**	**73%**
DER-UI	89	100%	65%
DER-REP	22	100%	59%
DER-CFG	57	100%	88%
DER-CON	158	100%	93%
DER-DTC	19	100%	88%
DER-DCM	23	100%	75%
DER-EBR	15	100%	100%
DER-HST	57	100%	54%
DER-CMS	60	100%	81%
DER-FOR	24	100%	0%
SYS-TST	29	100%	68%
SYS-SSI	10	100%	63%
SYS-HRD	20	100%	100%
SYS-SCL	9	100%	100%
SYS-MNT	42	100%	3%
SYS-CIT	82	100%	79%
OpenFMB	**162**	**100%**	**96%**
RMQ26.1	16	100%	100%
RMQ26.2	39	100%	0%
RMQ26.3	38	100%	94%
RMQ26.4	21	100%	100%
RMQ26.5	19	100%	100%
RMQ26.6	29	100%	80%
NERC CIP	**297**	**100%**	**15%**
CIP-003-8	26	100%	0%
CIP-004-6	40	100%	5%
CIP-005-6	14	100%	64%
CIP-006-6	20	100%	5%
CIP-007-6	37	100%	49%
CIP-008-6	31	100%	0%
CIP-009-6	21	100%	19%
CIP-010-3	33	100%	28%
CIP-010-3 Attachment 1	19	100%	0%
CIP-011-2	8	100%	0%
CIP-012-1	5	100%	0%
CIP-013-1	14	100%	7%
CIP-014-2	29	100%	0%
EVR	**148**	**100%**	**99%**
EVR-CYSEC	106	100%	99%
EVR-SOPO	42	100%	100%
	1323	**100%**	**62%**

Technical Accomplishments and Progress

- High-level design of SCM network, communications, and management architecture – in progress
  - Discovery and categorization of real-world deployment environments and systems
  - Initial software and hardware specifications drafted; prototype implementation in progress
  - Mature (TRL-5) implementation requires integration in cyberphysical environment (est. 07/21)

- Proof-of-concept demonstration of metering and telemetry SCM use cases – in progress
  - Prototype interfaces and metering/telemetry applications developed for Modbus, OCPP, OSCP
  - Corresponds to BP1 GO/NO-GO

- Intended deployment to cyberphysical environment with multiple EVSE in June-July 2021

- Note: Reference architecture and implementation intended to be made open-source in 2023-2024. At this point, we are not ready to publicly release detailed technical specifications.

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

Response to Previous Year Reviewer's Comments

N/A – this is the first time this project has been briefed at AMR.

Collaborations

TEAM DTLLC – a diverse mix of stakeholders necessary to design and develop a system aligned with real-world customer requirements and deployment scenarios

Subrecipients:

- **Utility partner**: DTE Energy (architecture design, grid integration, SCM R&D)
- **National Lab partners**: INL (security research, SCM algorithm design), ORNL (WPT integration)
- **Industry partners**: RunSafe Security (security tool vendor), RedStone Tech. Integration (systems integration)
- **University partners**: Utah State University (modeling and simulation, SCM algorithm design), UM-Dearborn (security research - prevention), WSU (future, security research - detection)
- **Test sites**: American Center for Mobility, NextEnergy

Remaining Challenges and Barriers

- Developing accurate models and SCM control strategies to account for future levels of EV, EVSE grid penetration
- Resolving inconsistencies in mappings between heterogeneous standard and proprietary management protocols (61850, CIM, OCPP, OPC-UA, etc.)
- Achieving software-based interoperability in real-world distribution environments

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

Proposed Future Research

FY21 activities

- Model and simulate high-impact charging events in existing distribution network models to identify additional system requirements
- Develop software interfaces (protocol adapters) for distribution protocols (Modbus, DNP3, etc.)
- Design software interfaces for EV and EVSE management protocols (OCPP, OPC-UA, etc.)
- Using OpenFMB, implement proof-of-concept capabilities for metering, telemetry, and command-and-control use cases, and demonstrate in laboratory setting

FY22 activities

- Complete development of software interfaces for distribution systems, EVs, EVSE, and DER
- Develop middleware applications for SCM and grid services. Design charge control strategies.
- Demonstrate mature implementations of SCM capabilities in laboratory and fielded R&D environments.

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

Summary

- **EVs-at-RISC will produce an open-source, open standards-based SCM system for distribution networks with support for interoperable, secure management and grid integration of EVs, EVSE, and DER**

➢ Develop an extensible architecture for secure, interoperable control of heterogeneous distribution assets

➢ Standardize a software deployment architecture for distribution networks – develop and deploy protocol-agnostic software applications that can interact with any distribution asset

➢ Realize wide-scale capabilities to use EV, EVSE, DER for SCM and grid support services

➢ Mitigate cybersecurity risks from legacy systems, SCADA protocols, and compromised EV, EVSE, and DER

- **Current state: early-stage development of SCM metering, telemetry, and command-and-control capabilities**

➢ Conceptual system and high-level secure architecture design – complete

➢ Implementation in modeling and simulation environments – in progress

➢ Deployment to cyberphysical test environments – scheduled for 07/21

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