2019 DOE Vehicle Technologies Office Annual Merit Review:

Enabling Secure and Resilient XFC: A Software/Hardware-Security Co-Design Approach

Ryan M. Gerdes

Virginia Tech

June 13, 2019

Project ID elt207

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

Overview

Timeline

- 2018-10-01
- 2020-12-31
- Percent Complete: 20%

Barriers

- Compromise is difficult to detect, contain, and mitigate
- Remote remediation of compromise
- Maintaining operational capacity under compromise

Budget

- Total project funding
  - $2,500,000 DOE funding
  - $625,000 cost share

Partners

- Academic: *Virginia Tech*, Georgia Tech, Utah State University
- Industry: ChargePoint Inc., Commonwealth Edison Company, Ford Motor Co., OnBoard Security

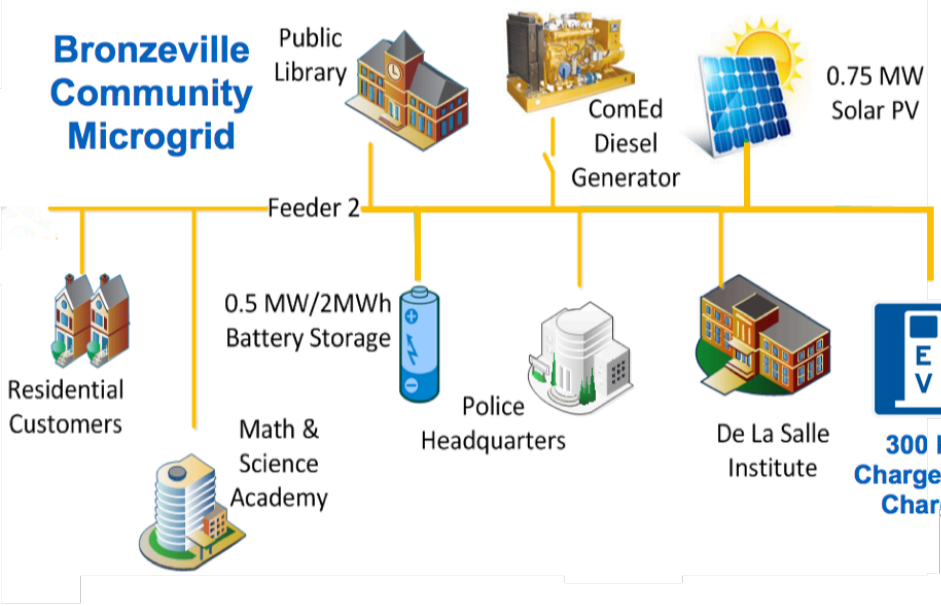
Relevance

- ***Enable the decrease in battery charge time in a secure and efficient manner***
  - coordination and cooperation between the grid, charging stations, and the vehicles
  - electric vehicle service equipment (EVSE) and the BEV themselves are untrustworthy
- **Resilient (and not just secure) system be put in place**
  - compromises of either BEV or EVSE are inevitable
  - maintain some operational capacity while guaranteeing safety
- **Motivating threats:**
  - A network of compromised EVSE could be used to simultaneously discharge the batteries of BEV
  - Compromised BEV, with possible collusion from compromised EVSE, drawing from the grid in a coordinated manner so as to cause instability
  - Malware being spread from a BEV to other BEV through the compromise of single or multiple EVSE

Approach

- **State-of-the-Art**
  - design process used for safety critical systems does not produce inherently more secure systems (e.g., automotive systems)
  - proprietary and/or high-level requirements
  - cyber-centric (best practices)
  - lack cyber-physical systems security perspective
- **Hardware/software-security (HW/SW-Sec) co-design approach**
  - security-hardened controllers, converters, and monitoring systems: secure sensing/actuation techniques, moving-target based detection and mitigation strategies
  - guarantee successful remediation of vulnerabilities in EVSE/BEV through remote updates
  - respecting end-user privacy
  - conductive and inductive charging at power levels of 200 kW to 400

Approach



Grid side:
- T1) Threat modeling and vulnerability assessment
- T2) Resilient scheduling and load management
- T3) Attack detection and mitigation controller

BEV:
- T1) Threat modeling and vulnerability assessment
- T3) Attack detection and mitigation controller
- T4) Hardened DC-DC Converters and battery management
- T6) Secure updates
- T7) User privacy

EVSE:
- T1) Threat modeling and vulnerability assessment
- T3) Attack detection and mitigation controller
- T4) Hardened AC-DC Converters
- T5) Existence and alignment of BEV
- T6) Secure updates
- T7) User privacy

Approach: Task 1

- **Cyber-physical threat and vulnerability assessment of EVSE/BEV/grid systems using a game-theoretic risk analysis and an automatic attack graph generator**
  - specify attacker characteristics, attack vectors, and assets
    - Traditional: Threat Analysis and Risk Assessment (TARA) for EVSE/BEV/grid
    - New: game theoretic approach (cost-vs-benefit analysis using structural non-equilibrium level-k thinking)
    - New: EVSE/BEV-specific automatic attack assessment tools for common interfaces and systems
  - first step in security co-design process: identify risks, failure states, and fail-safes
- **Novelty: differing rationalities and decision-making mechanisms; automatic generation of attack graphs of non-quasi-static and cyber-physical systems**
- **Need served: no clear threat model or trust model for the EVSE/BEV space; tools for automatic assessment; estimates of costs and capabilities of attackers under various threats**

Approach: Task 2

- **Performing experimentally-validated, grid-side modeling of XFC loading on a microgrid and using a reachability analysis to determine the safety of a given charge request**
  - detect and mitigate attacks under modeling uncertainty: determine if a sequence of charging events would result in grid instability
  - Bronzeville Community Microgrid testbed: empirical models developed in Opal-RT and RTDS and hardware-in-the-loop simulations (islanded and grid-connected)
    - non-attack: BEV charging profiles, baseline load, voltage and frequency profiles of the microgrid under different charging scenarios (non-attack)
    - attack scenarios: reachability analysis to define the unsafe states the system will not be allowed to enter
    - mitigation: moving-target defense for microgrid controller
- **Novelty: reinforcement learning to learn and refine system models so as to be robust against modeling uncertainty under attack**
- **Need served: how XFC chargers can be operated with minimal negative impact on the grid, even under attack**

Approach: Task 3

- **Development of a moving-target defense (MTD) for sensor and actuator attacks against EVSE/BEV/grid controllers**
  - adversarial agents may directly impact either via a corrupting actuator, sensor, or inter-agent (system) communication channels
  - goal: disruption of resources without detection
- **deep Q-learning structures (learn attacker and system over time) for model-free defense**
  - a framework to facilitate deception of potential attackers
  - switching of controllers for optimality and unpredictability
  - guarantee stability of the overall system for switched controllers
  - identify potentially corrupted sets of controllers/sensors/actuators
- **Novelty: model-free secure optimal feedback policies for EVSE/BEV systems**
- **Need served: resilient system (i.e., EVSE, BEV, and grid controllers individually and together) capable of learning and achieving its objective in the presence of adversarial agents**

Approach: Task 4

- **Designing AC-DC (for EVSE) and DC-DC (for BEV) converters and battery management systems (for BEV) capable of resisting false data and false actuation attacks by leveraging redundancy, diversity, and watermarking**
  - attacker: identify the fail-safes in converter and battery management systems (cyber and cyber-physical)
  - iterative design process for BMS and converters: identify fail-safes, attack, and then harden
    - determining which points of the systems are most vulnerable to a particular type of attack and determining whether redundancy can cost-effectively provide increased tolerance to attack (defense one)
    - devising models that relate diverse sensor measurements (defense two)
    - integrated MTD (defense three)
    - creating a two-way watermarking system that would allow a controller to know that an actuation signal was acted upon (detect)
- **Novelty: hardening approaches validated against attacks in a realistic full power system environment**
- **Need served: last line of defense at the vehicle to prevent damage; cyber-physical protection for EVSE/BEV**

Approach: Task 5

- **Using device fingerprinting to determine whether an actual EV is connected to the EVSE; building a secure ranging system with spoofing detection to ensure that a vehicle is properly and safely aligned with the charging pad**
  - attacker: compromised EVSE could coordinate charging into phantom vehicles to cause under-voltage on the grid; if a BEV is not properly aligned compromised could cause damage
  - EVSE can know vehicle is present:
    - charging characteristics can be used to classify BEV: robust to battery state of charge and ambient temperature
    - inductively charged BEV detected through changes of inductance of the charging pad
  - EVSE can know vehicle is aligned: secure ranging based on redundant semi-securing ranging systems (IR-UWB) and attack detectors
- **Novelty: secure ranging systems are rare and require specialized hardware; incorporate COTS components and still yield a high degree of security**
- **Need served: verify that an actual vehicle is being charged and vehicle is properly aligned (to reduce occurrence of A1,2)**

Approach: Task 6

- **Leveraging a trusted-computing base to guarantee that a formally verified, remote firmware update procedure takes place, even in the case of unreliable primary communications**
  - inevitable that vulnerabilities in EVSE will be discovered and exploited
  - light-weight crypto and a trusted computing base (TCB) for the embedded system running the EVSE firmware
  - update procedure will exist entirely in the TCB and be formally verified to ensure that it is free of vulnerabilities
  - secondary communication channels will be investigated to guard against denial of service
  - side-channel resistance: fuzzy extractor for key generation based on grid signals
- **Novelty: guarantee that firmware will be patched even when an adversary is allowed physical access to the system**
- **Need served: a resilient secure update procedure for EVSE/BEV integrated into existing frameworks (UPTANE)**

Approach: Task 7

- **Extending the ISO/IEC 15118 protocol to ensure user privacy even in the case of untrustworthy agents or when communication has been impaired**
  - charging infrastructure require protocols and standards that control authentication, authorization, and billing of BEV charging
  - Privacy Impact Assessment (PIA)
  - extended ISO/IEC 15118 protocol for privacy preservation:
    - untrustworthy agents at each of the transaction and
    - providing privacy guarantees even when connectivity between the charger and billing service is unavailable
- **Novelty: no significant mechanisms for privacy protection in place in existing protocols**
- **Need served: first open-source end-to-end solution for managing user credentials and data between differing network operators**

Approach: Milestones (FY2019-20)

Milestone	Type/Status	Description
Threat models (06/2019)	Technical (Complete)	TARA report that lists the main threats to focus on later in the project
Microgrid model (09/2019)	Technical (Ongoing)	The model of Bronzville microgrid is developed in real-time simulators
New designs for converter and BMS hardware (12/2019)	Technical (Ongoing)	Critical design review completed with team and program manager approval of hardened designs
MTD techniques with theoretical stability, optimality, and robustness guarantees (03/2020)	Go/No-Go (Ongoing)	A proactive and reactive defense framework for the EVSE/BEV/grid controllers

- **Hardware to be deployed:**
  - ChargePoint XFC charger (October 2019, Chicago, IL)
  - Ford Focus BEV (Blacksburg, VA & Boston, MA)

Approach: Milestones (FY2020)

Milestone	Type	Description
Privacy Impact Assessment of EVSE/BEV communication (06/2020)	Technical	Analyze data flows to identify personally identifiable information and ensure appropriate privacy controls
Vulnerability assessment of EVSE/BEV-grid interactions (09/2020)	Technical	Attack trees and attack graphs.
Trade-offs of grid-side resiliency approaches (12/2020)	Technical	Trade-offs for BEV-induced attacks are quantified
Install and demonstrate the technology within the Bronzeville Community Microgrid (03/2021)	Go/No-Go	Successful field demonstration given the minimum negative impact during the planning study

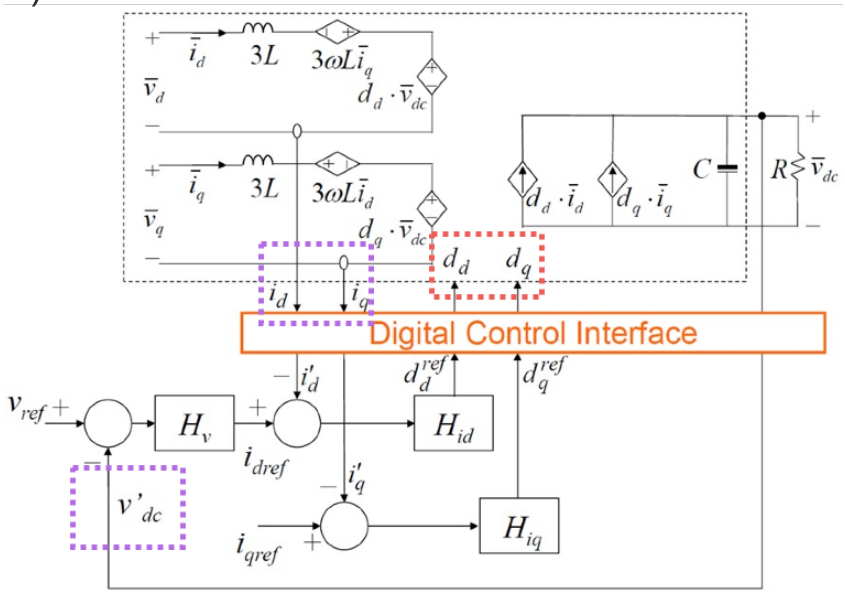
- **Hardware to be deployed:**
  - USU XFC (conductive & inductive) bus (Logan, UT)

Technical Accomplishments and Progress

- **Threat assessment of EVSE/BEV/grid using TARA methodology (T1, M1)**
  - BEV assessment complete
  - EVSE/grid assessment to be completed upon integration of EVSE into research lab (Q3, 2019)
  - Participation in NMFTA XFC Cybersecurity Working Sub-Group A
- **Vulnerability assessment of a Ford BEV (T1, M2)**
  - Identify safety-critical faults, methods to detect, and fail-safes: induce, mask, and subvert
  - 18 attack vectors identified: Permanent disabling/degradation of vehicle and harm to occupants/persons nearby
  - Validation of two high-impact vectors
  - Ten undergraduate researchers
- **Gather electrical characteristics of the Bronzeville Community Microgrid (T2, M5)**
  - Anonymized data collected for construction of OPAL-RT and RTDS models

Technical Accomplishments and Progress

- **Trust Models of EVSE/BEV/grid (T1, M3)**
  - Attack vectors: delay, jamming, false-data injection, false-actuation injection
  - Initial system: AC/DC Converter (linearized)
  - Game theoretic formulation that allows for
    - Level-k hierarchy (differing rationalities and capabilities)
    - Goal: make system unstable, uncontrollable, or unobservable (eventually arbitrary unsafe states)
    - Expenditure of resources
      - Incorporation of costs
      - Attack points and number
      - Defensive strategies
        - » Redundancy
        - » Diversity
        - » Encryption



Technical Accomplishments and Progress

- **Trust Models of EVSE/BEV/grid (T1, M3)**
  - Attack vectors: delay, jamming, false-data injection, false-actuation injection
  - Initial system: AC/DC Converter (linearized)
  - Hybrid systems formulation that incorporates
    - Sensing, actuation, legitimate control, and communication
    - Manual specification of attacker objective(s)
    - Tractability: NP hard
      - Branch-and-bound
      - SAT solver to prune state space
    - Novel attack sequences discoverable

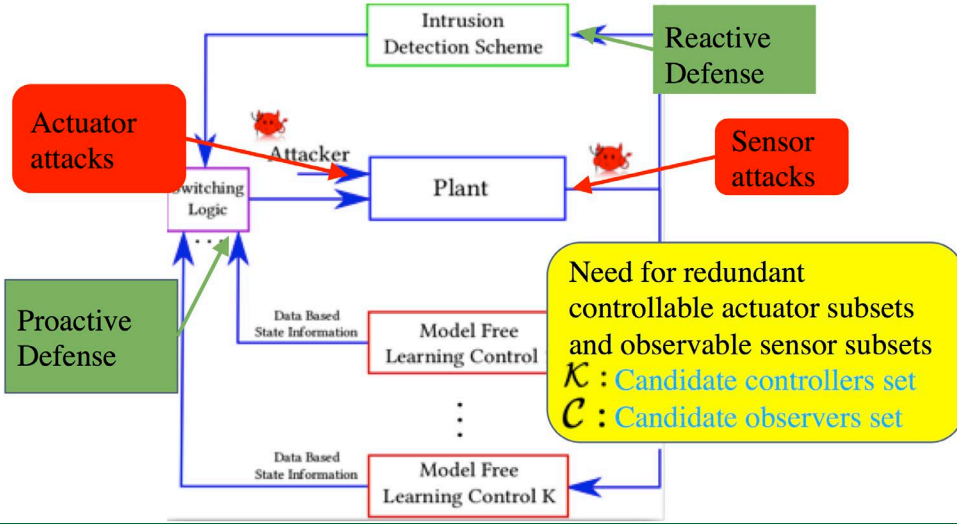
$$\min_{\mathbf{u}_a(t)} \quad ||\mathbf{x}(t) - \mathbf{x}_a(t)||_p$$

$$\text{s.t.} \quad \dot{\mathbf{x}}(t) = f\left(\mathbf{x}(t), \mathbf{u}(t), \mathbf{u}_a(t)\right)$$

$$\mathbf{u}_a(t) \in \{\text{delay, jamming, fdi, fda}\}$$

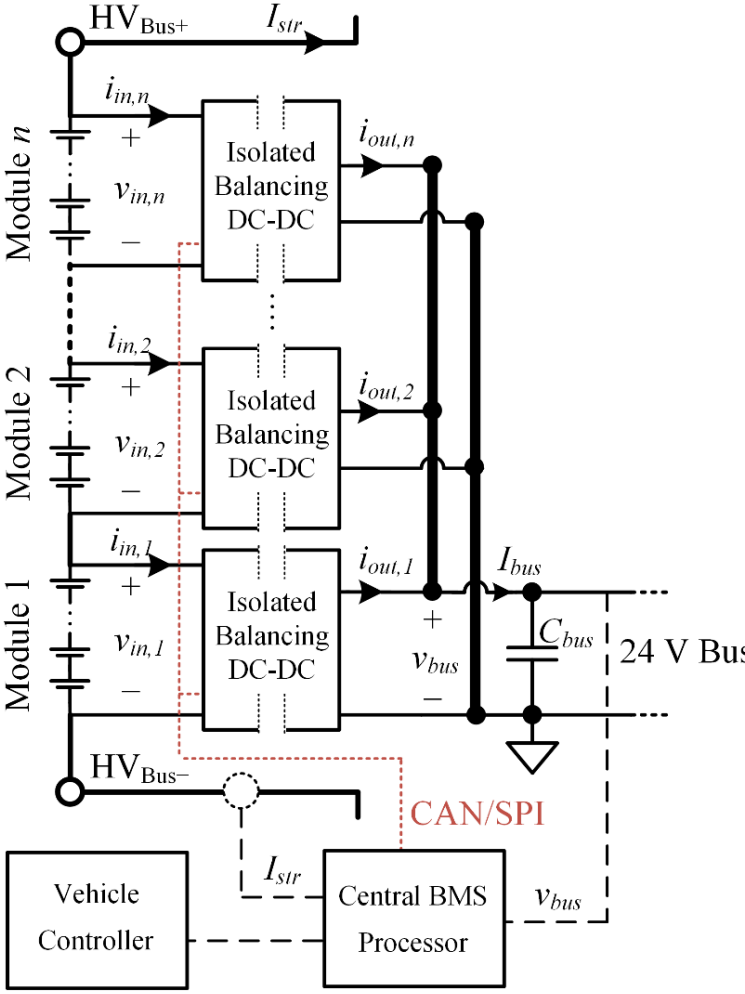
Technical Accomplishments and Progress

- **Proactive and reactive defense mechanism (T3, M8)**
  - Use of redundant sensor and actuators (generic CPS)
    - Switch active unit(s) in unpredictable and stochastic fashion
    - Increases cost to attacker with minimal cost to defender
  - System/environmental uncertainty: optimality achieved using non-equilibrium intermittent learning
  - Reactive defense necessary
    - Attacker goals realized under traditional MTD
    - Isolate the suspicious units
    - Continued safe operation



Technical Accomplishments and Progress

- **Iterative design of AC-DC converter and active BMS plus DC-DC converter (T4, M9)**
  - 480 V 3-phase ac input, 350 kW rated power XFC using 5 modules with 70 kW rated power each
  - Major power components for the AC/DC converter have been selected
  - Models for battery state-of-charge/health
  - Initial topology and control design of the BMS module (DC-DC converter and battery monitoring) with the consideration of cyber-physical security hardening
    - Analyzing the potential attack points of the system
    - Investigating the possible attack types for the potential attack points in the system
    - Determining which points of the systems are most vulnerable to a particular type of attack



Responses to Previous Year Reviewers' Comments

- Project not reviewed last year

Collaboration and Coordination

- **Academic Partners:**
  - Virginia Tech (Prime): cyber-physical systems security; micro and smart grid; sensor integration; intelligent transportation systems
  - Georgia Tech (Sub): optimal, adaptive control; game theory; reinforcement learning
  - Utah State University (Sub): Development and commercialization of electric vehicle fast charging equipment (inductive and conductive) and custom active battery management systems
- **Industry Partners:**
  - ChargePoint Inc. (Sub): operates the largest EV charging network in North America; works closely with electric vehicle manufacturers and utilities to implement EV charging and energy management programs
  - Commonwealth Edison Company (Sub): one of the nation's largest electric utilities; evaluation and development of emerging grid technologies, including but not limited to energy storage and microgrid systems.
  - Ford Motor Company (Sub): expect to have 24 hybrid and 16 fully electric vehicles in their model lineup and $11 billion invested in BEV
  - OnBoard Security (Sub): cyber-physical systems security, CIA analysis, vulnerability assessment and design of embedded and intelligent transportation systems

Collaboration and Coordination

- **Interactions**
  - Prime call w/DOE PM: monthly (phone)
  - Prime call w/all partners: monthly (videoconference)
  - Prime call w/individual partners: monthly (videoconference)

	T1.1	T1.2	T1.3	T1.4	T2.1	T2.2	T2.3	T3.1	T4.1	T4.2	T4.3	T5.1	T6.1	T6.2	T7.1
VT	S	S	L	S	S	S	L	S	S			L	L	S	S
GT			S					L	S						
USU									L	L	L	S			
CPI			S	S					S				S	S	
CEC			S		L	L	S								
FMC		S	S												
OBS	L	L	S	L					S			S	S	L	L

(L)ead, (S)upport

Each sub-task averages 2.67 partners in participation

Remaining Challenges and Barriers

- **Assessment and countermeasures**
  - Guarantees for linear time-invariant systems, only
  - Unsafe states for non-linear systems must be specified
  - Incorporation of cyber attacks into cyber-physical frameworks
- **Disparate knowledge/simulation domains across teams**
- **Physical realization of countermeasures**
  - Generic cyber-physical systems provably secure (against known attacks)
  - Implementations are flawed
    - Design of redundant /diverse sensing regimes not vulnerable to common (same) attacks
    - Cost-effective and resilient parallel actuation strategies
    - Redundancy/diversity leading to exponential gains in security (commonly only linear)

Proposed Future Research

Milestone #	Task	Milestone
3	Trust Models (VT lead, GT, OBS, ChargePoint, Ford, ComEd support) (M1-12)	Comprehensive list of attack points and the utility of attacking/defending them.
4	Vulnerability Assessment of EVSE (OBS lead, VT and ChargePoint support) (M7-12)	Attack trees and attack graphs that indicate likely compromise points and the attack sequence necessary to achieve attacker goals.
6	Develop a simulation circuit of the Bronzeville Community Microgrid (ComEd lead, VT support) (M7-9)	The model of Bronzville microgrid is developed in real-time simulators
7	Create BEV charging profiles using Monte Carlo simulation and insert BEV charging units with variation of charging profiles into the microgrid (VT lead, ComEd support) (M10-12)	Different BEV charge profiles are created based on real-world data
8	Combined proactive and reactive defense mechanism (GT lead, VT support) (M1-12)	A proactive and reactive defense framework for the EVSE/BEV/grid controllers.
9	Iterative design of 300 kW AC-DC converter and 5 kW integrated active BMS plus DC-DC converter (USU lead, VT, GT, OBS, and ChargePoint support) (M1-6)	Critical design review completed with team and program manager approval of hardened designs.
10	Hardware construction of BMS with integrated 5 kW DC-DC for vehicle LV loads (USU lead) (M7-12)	Hardware demonstration with functional operation of modified battery pack, BMS, and DC-DC and functional test of hardening features.
11	Hardware construction of 60 kW module prototype for AC-DC converter (USU lead) (M7-12)	Hardware demonstration with functional operation of the 60 kW module with verified communications to a central AC/DC controller and verified hardening feature operation.

Proposed Future Research

Milestone #	Task	Milestone
12	Devising device fingerprinting methodologies for conductive and inductive chargers (M7-12)	
13	Creation of formally verified update procedure (OBS lead, VT and ChargePoint support) (M1-12)	A TCB-based routine capable of initiating remote update procedure, authenticating firmware, and installing it.
14	Allowing updates to EVSE when primary communication channel is disabled (OBS lead, VT and ChargePoint support) (M6-12)	Proof-of-concept demonstration that update routine can fall-back to secondary communication channel.
15	Privacy of EVSE-BEV, EVSE-Grid communication (OBS lead, VT support) (M7-12)	Privacy Impact Assessment of EVSE/BEV communication: The PIA analyzes the data flows to identify personally identifiable information. Data collection, retention, use, disclosure are then analyzed to ensure appropriate privacy controls.

Summary

- **Goal: secure and efficient charging**
- **Approach: hardware/software-security (HW/SW-Sec) co-design**
  - Develop security-hardened controllers, converters, and monitoring systems for XFC
    - maintain user privacy
    - secure sensing and actuation techniques
    - learning-enabled moving-target defense
    - remediation of vulnerabilities through remote updates
  - Benefits
    - Minimizing (secure) design time of future systems
    - Address findings of vulnerability assessments
    - Critical infrastructure that can resist (as a function of cost), and be resilient to, attack
  - The feasibility demonstrated on a real-world testbed that includes an XFC unit and BEV situated in a microgrid
  - Multi-disciplinary team and industry-academic partnership
    - Unique perspectives and expertise to examine threats and solutions