2021 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 24, 2021
Project ID elt207
















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

Overview

Timeline

- 2018-10-01
- 2021-12-31
- Percent Complete: 75% (Q2, 2021)

Budget

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

Barriers

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

Partners

- Academic: *Virginia Tech*, Georgia Tech, Utah State University
- Industry: Commonwealth Edison Company, Ford Motor Co., GE Research, Tritium

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

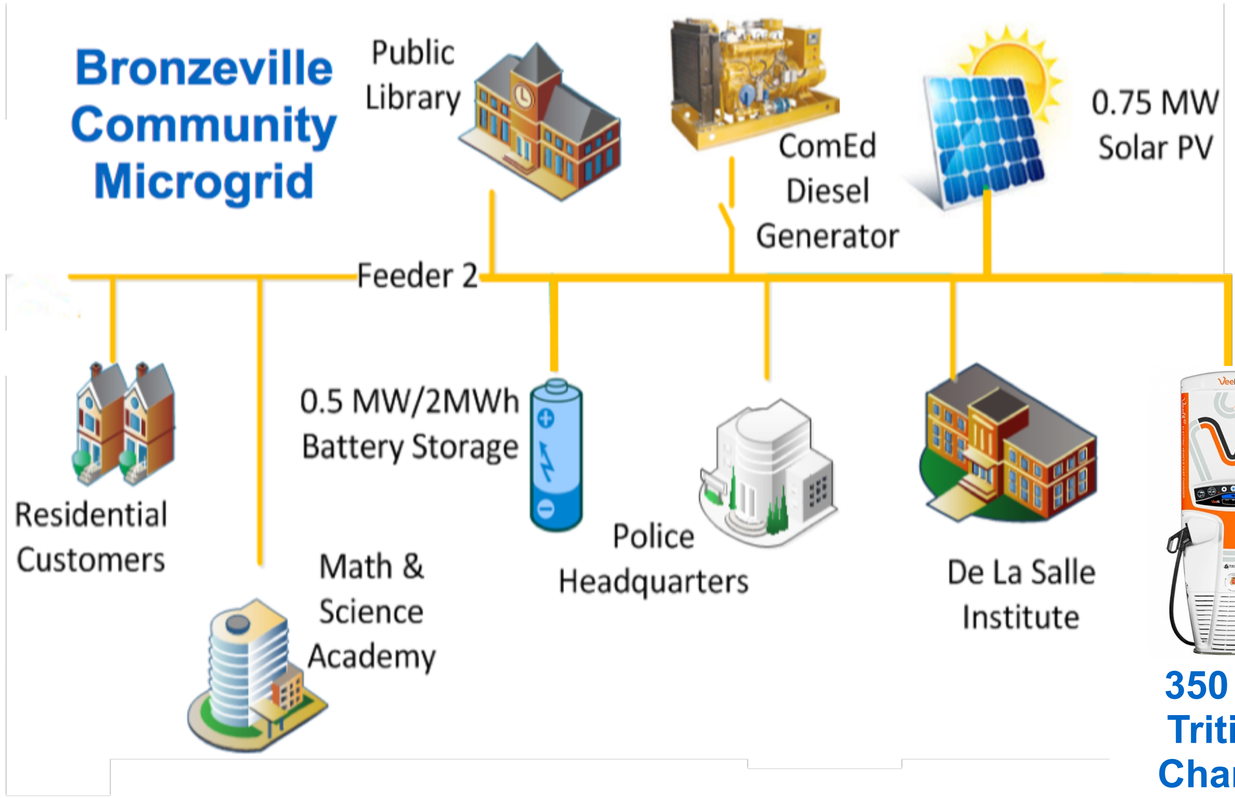
- Motivating threats:
  - A network of compromised EVSE could be used to simultaneously discharge the batteries of BEV
  - Compromised BEV, with possible collusion from compromised EVSE, drawing from the grid in a coordinated manner so as to cause instability
  - Malware being spread from a BEV to other 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 200–400 kW

Approach



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



Ford Focus BEV

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

BP1 Milestones

Milestone #	Task	Milestone	Status
1 (Q3, 2019)	Threat models (OBS lead, VT support)	TARA report that lists the main threats to focus on later in the project	Complete
2 (Q4, 2020)	Vulnerability Assessment of BEV (GER lead, VT and Ford support)	Attack trees and attack graphs that indicate likely compromise points and the attack sequence necessary to achieve attacker goals.	Continuing to BP2
3 (Q4, 2020)	Trust Models (VT lead, GT, GER, Tritium, Ford, ComEd support)	Comprehensive list of attack points and the utility of attacking/defending them.	Complete
4 (Q2, 2021)	Vulnerability Assessment of EVSE (GER lead, VT and Tritium and ComEd support)	Attack trees and attack graphs that indicate likely compromise points and the attack sequence necessary to achieve attacker goals.	Moved to BP2
5 (Q3, 2019)	Gather electrical characteristics of the Bronzeville Community Microgrid (ComEd lead, VT support)	Microgrid data is available for simulation model development	Complete
6 (Q4, 2019)	Develop a simulation circuit of the Bronzeville Community Microgrid (ComEd lead, VT support)	The Single Line Diagram and model of Bronzville microgrid is developed for real-time simulators	Complete
7 (Q1, 2020)	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)	Different BEV charge profiles are created based on real-world data	Continuing to BP2
8 (Q3, 2020)	Combined proactive and reactive defense mechanism (GT lead, VT support)	A proactive and reactive defense framework for the EVSE/BEV/grid controllers.	Complete
9 (Q3, 2020)	Iterative design of 300 kW AC-DC converter and 5 kW integrated active BMS plus DC-DC converter (USU lead, VT, GT, and Tritium support)	Critical design review completed with team and program manager approval of hardened designs.	Complete

BP1 Milestones

Milestone #	Task	Milestone	Status
10 (Q4, 2020)	Hardware construction of BMS with integrated 5 kW DC-DC for vehicle LV loads (USU lead)	Hardware demonstration with functional operation of modified battery pack, BMS, and DC-DC and functional test of hardening features.	Complete
11 (Q4, 2020)	Hardware construction of 60 kW module prototype for AC-DC converter (USU lead)	Hardware demonstration with functional operation of the 60 kW module with verified communications to a central AC/DC controller and verified hardening feature operation.	Complete
12 (Q3, 2020)	Devising device fingerprinting methodologies for conductive and inductive chargers	EVSE capable of securely determining presence and type of vehicle	Comple
13 (Q3, 2020)	Creation of formally verified update procedure (GE/VT Co-lead and Tritium support)	A TCB-based routine capable of initiating remote update procedure, authenticating firmware, and installing it.	Continuing to BP2
14 (Q2, 2021)	Allowing updates to EVSE when primary communication channel is disabled (GE lead, VT and Tritium support)	Proof-of-concept demonstration that update routine can fall-back to secondary communication channel.	Moved to BP2
15 (Q4, 2020)	Privacy of EVSE-BEV, EVSE-Grid communication (GE lead, VT support)	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.	Moved to BP2

Tasks Moved/Continuing to BP2

- Moved
  - T4: Vulnerability Assessment of EVSE (delivery of charger delayed, lab closures)
  - T14: Allowing updates to EVSE when primary communication channel is disabled (replacement of partner)
  - T15: Privacy of EVSE-BEV, EVSE-Grid communication (replacement of partner)
- Continuing
  - T2: Vulnerability Assessment of BEV (contract delayed)
  - T7: Create BEV charging profiles using Monte Carlo simulation and insert BEV charging units with variation of charging profiles into the microgrid (delivery of charger delayed, lab closures)

Go/No-Go: T8 (Complete)

- MTD techniques with theoretical stability, optimality, and robustness guarantees
  - A proactive and reactive defense framework for the EVSE/BEV/grid controllers
  - Proof of optimality of approach (sensor and actuator attacks)
  - Proof-of-concept via simulation of moving-target defense
  - Integration into prototype hardware in BP2
  - Provides defenses for hardened AC/DC and BMS
    - Software (compromise of controller): multiple, isolated PID controllers randomly selected
    - Hardware (compromise of sensor): multiple sensors used to measure same state, randomly selected
    - Hardware (compromise of actuator): multiple actuation signal paths, randomly selected

Technical Accomplishments and Progress: T2

- Vulnerability assessment of a Ford BEV
  - 18 attack vectors identified: Permanent disabling/degradation of vehicle and harm to occupants/ persons nearby
  - Validation of two high-impact vectors
  - Diagnostics specification
    - Battery Power Sensor Module (BPSM) can be compromised
    - BPSM provides BECM with critical sensor data
    - Develop injector to control traffic to/from BPSM (emulate compromise)
  - Team of undergraduate researchers: Assume attacker foothold in vehicle
    - Sniffing HS-CAN bus(es)
    - Injecting, modifying, and blocking CAN traffic (hardware and software)
    - Emergency shutdowns (safety-conscious experiments)
  - Formal assessment undertaken by GER (Q3, 2021): ISO 15118 (Ford Mustang Mach-E)
  - Deliverable: Publication TBD
  - Insight: Authenticated sensor data (battery temperature and voltage) allows for (possible) overheating of battery leading to thermal runaway

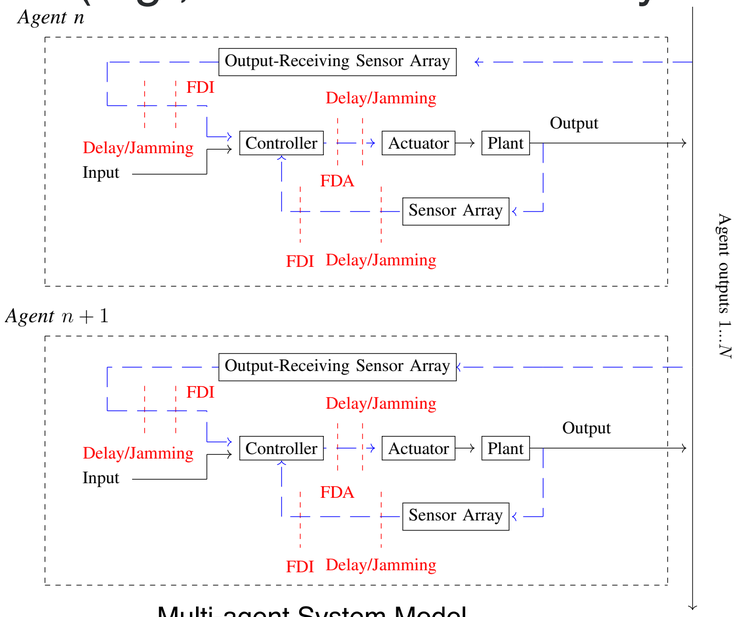
GOAL: (G0) Cause the battery to exceed the electric motor circuit temperature limit (80 C)

AND G1. Transmit CAN messages with spurious coolant temperature to prevent increase in coolant flow (@ 35 C) or initiate shutdown procedure (@ 80 C) from ECU1

OR 1. Alter MESSAGE1 from ECU2 to ECU1 that conveys coolant temp information such that the readings are below 80 C and within expected typical ranges.

Technical Accomplishments and Progress: T3

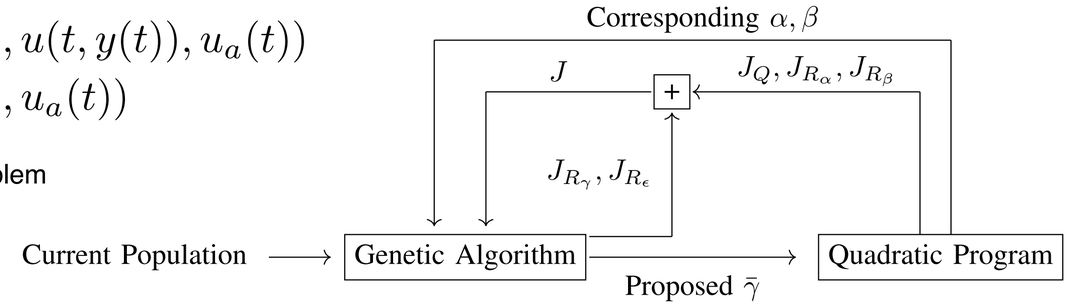
- Trust Models of EVSE/BEV
  - Attack vectors: delay, jamming, replay, false-data injection, false-actuation injection
  - Optimization problem: all attacks represented as input to system
    - Incorporate: nominal control, attack states of interest
    - Manual specification of attacker objective(s)
    - Multi-agent formulation: same state can be observed differently by individual agents
    - Hybrid optimization approach: separates convex (FDI/FDA) from non-convex (jamming, delay, replay)
  - Deliverable: Towards Systematic Defense Testing with Optimal Attack Generation in Cyber-Physical Systems
  - Insights: Identify cost-effective defense points and systematic evaluation of CPS defense mechanisms (e.g., demonstrated ability to evade Kalman filter based detectors)



Multi-agent System Model

$$\begin{aligned} \underset{u_a(t)}{\text{minimize}} \quad & J(x^*(t), u_a(t), x(t), T_f, t_0) \\ \text{subject to} \quad & \dot{x}(t) = F(t, x(t), u(t, y(t)), u_a(t)) \\ & y(t) = G(t, x(t), u_a(t)) \end{aligned}$$

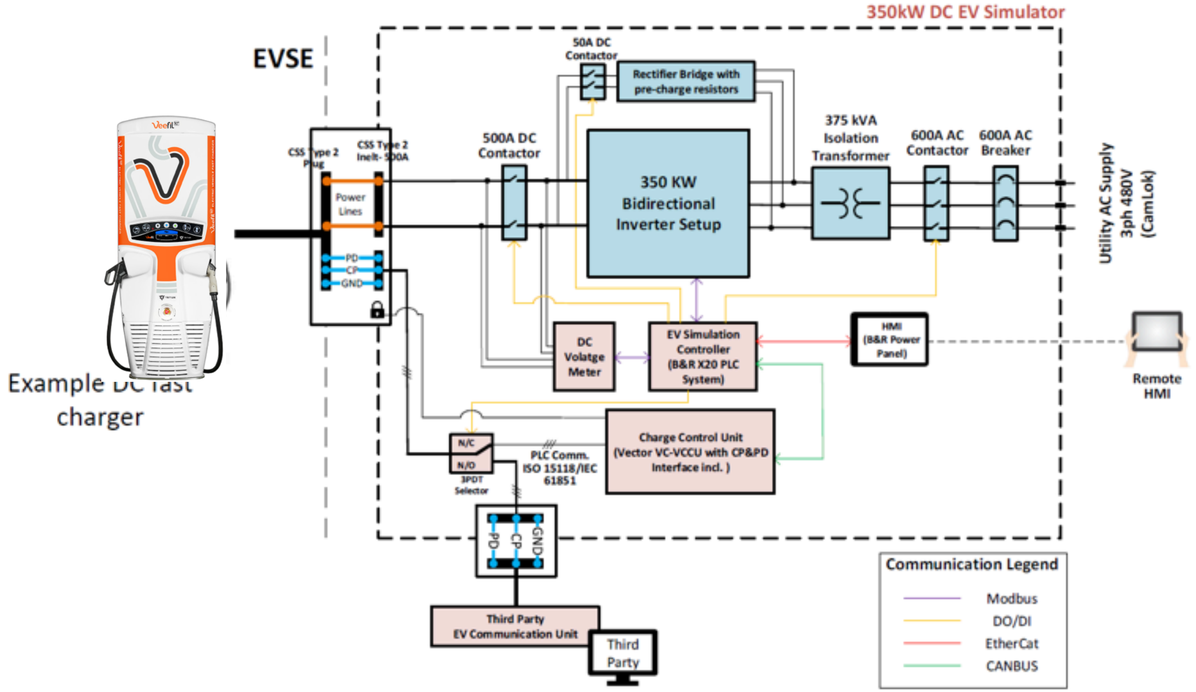
Attack-based Optimization Problem



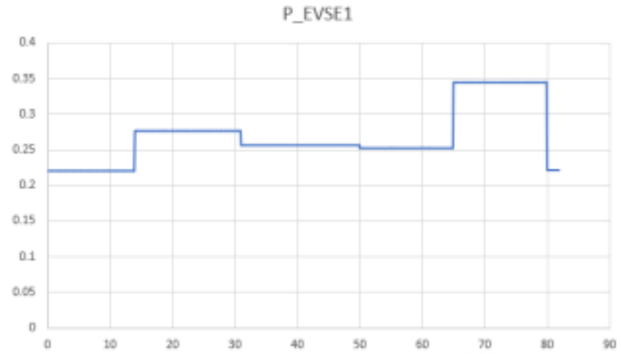
Hybrid Solution Framework for Optimization Problem

Technical Accomplishments and Progress: T4,7

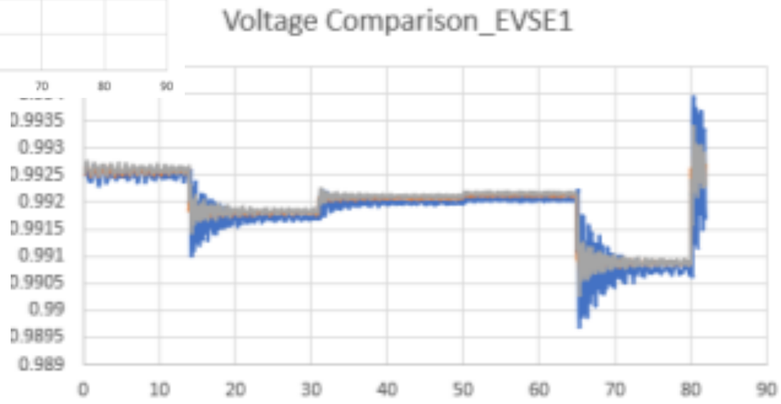
- 50kW DC Fast Charger and a 350kW XFC Obtained from Tritium
  - 50 kW received in December 2019
  - 350 kW XFC received July 2020
  - As XFC-capable vehicle unavailable, custom ‘EV Simulator’ designed and built
    - 350 kW capable, ISO 15118 compliant, arbitrary charging patterns
    - EVSE vulnerability assessment (T4, Q4, 2021)
    - Installation of the chargers and their integration within the HIL test environment (T7)



Conceptual configuration diagram for the 350kW EVSE and EV simulator



Desired Charging Profile

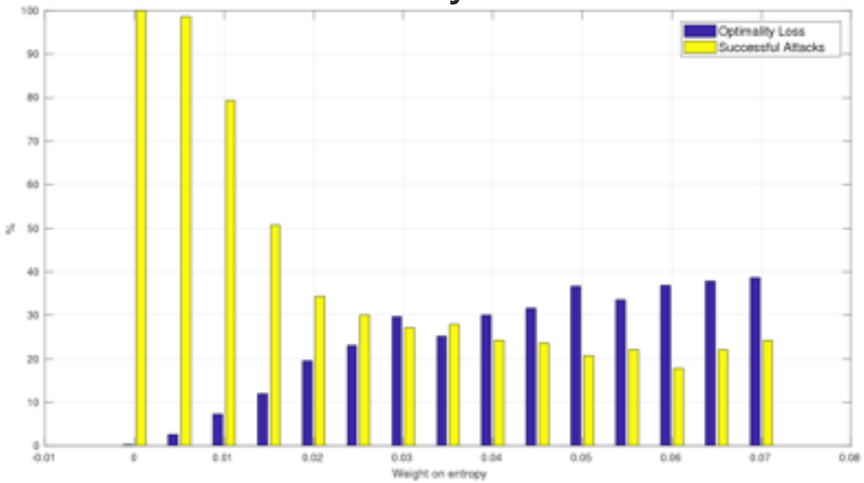


Voltage Across Sense Resistor

Technical Accomplishments and Progress: T8

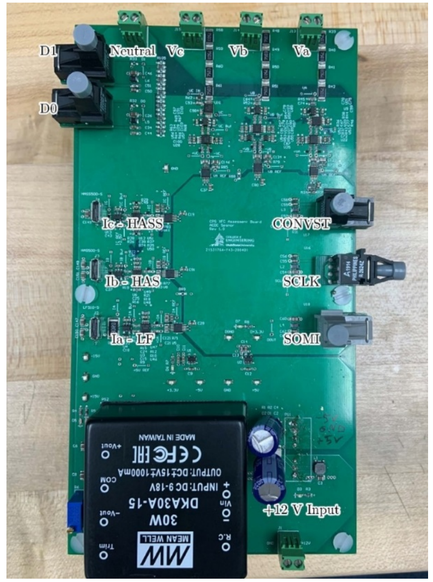
- Proactive and Reactive Defense Mechanism (MTD)
  - Use of redundant sensor and actuators
    - Developed a general framework to facilitate deception of potential sensor attacks (attacker does not know which sensor is used for control)
      - Defined an unpredictability metric to optimize, i.e., considered the entropy induced by switching between sensors
      - Quantified the optimality loss (control performance) that occurs when more weight is given to unpredictability
  - Combined Approximate Dynamic Programming (ADP) with MTD
    - Developed an on-line and completely data-based data-driven technique that controls an uncertain system in the presence of worst case disturbances, stochastic noises, and replay attacks
    - Developed a learning-based intrusion detection mechanism based on a Bellman error to mitigate attacks
    - Proposed switching rules which enforce proactive and reactive defense mechanisms against actuator and sensor attacks as well as guarantee the stability of the equilibrium point
  - Cost-benefit analysis: Examine the minimum number of sensors and actuators to cost-effectively secure hardware

attacker influence diminished more than control performance decreases:

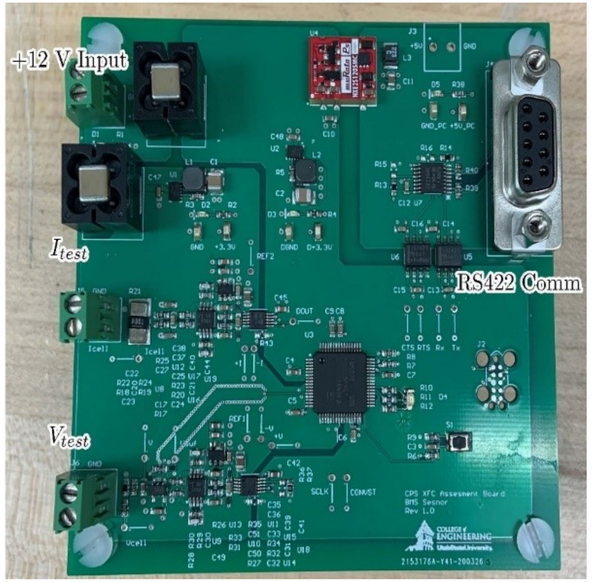


Technical Accomplishments and Progress: T9

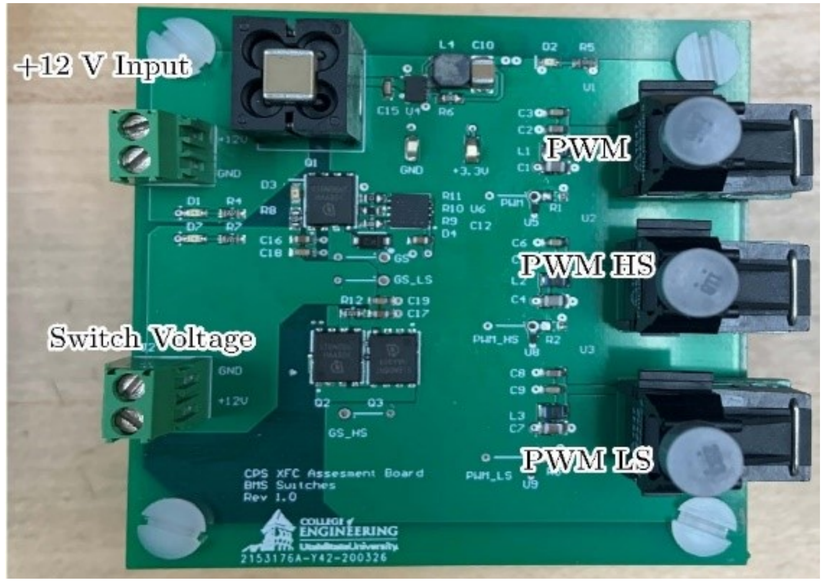
- Developed cyber-physical security evaluation boards: AC/DC (sense), BMS (sense + switch)
  - Countermeasures include sensor diversity, via fencing, differential signals, fiber optics, and multiplexers for sensing and gate drive signals
  - Evaluate the effectiveness of different countermeasures against IEMI attacks
  - Insight: differential signaling most effective *but* difficult in practice and vulnerable to single transmitter due to phase between traces/measurement



AC/DC Sensing Board



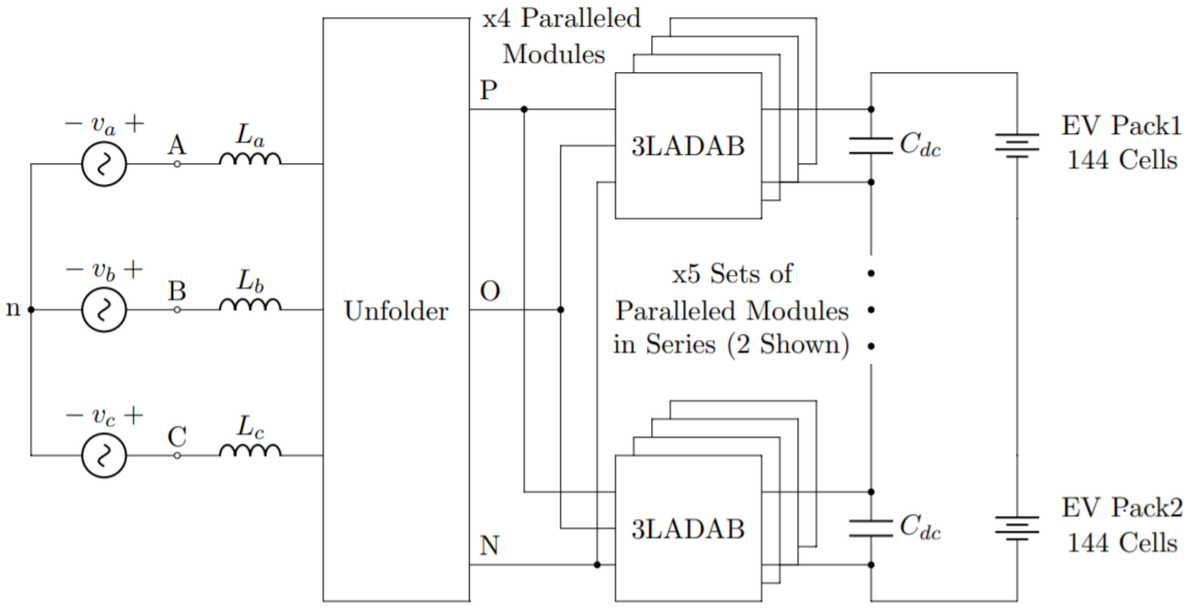
BMS Sensing Board



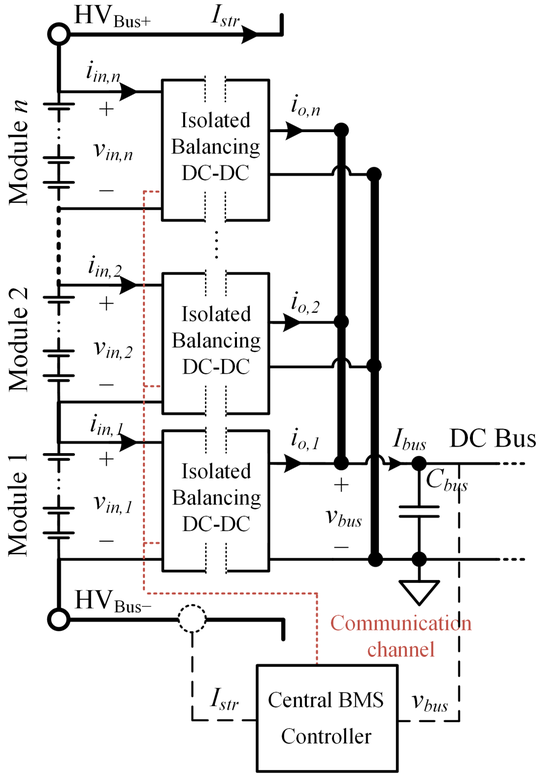
BMS Switching Board

Technical Accomplishments and Progress: T9

- Iterative design of 300 kW AC-DC converter and 5 kW integrated active BMS plus DC-DC converter
  - Unfolder + 3-Level Asymmetrical Dual Active Bridge
    - 350 kW output power with 450 A output current and 400V to 800 V output voltage
    - Modular design with 20 18 kW 3LADAB modules
    - 5 series connected sets of 4 parallel modules
  - Dual Active Bridge
    - Modular design with 18 ± 300 W Dual Active Bridges
    - 8 cells per DAB module



350 kW AC/DC System Architecture

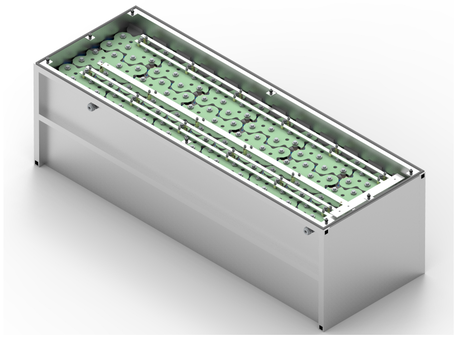


5 kW BMS System Architecture

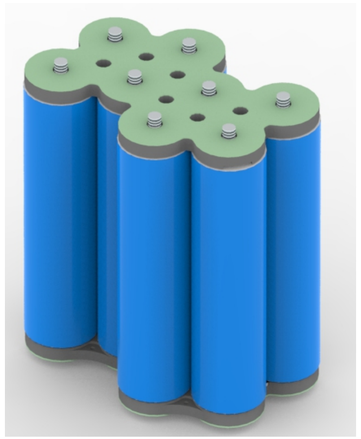
Technical Accomplishments and Progress: T10

- Hardware construction of BMS with integrated 5 kW DC-DC for vehicle low voltage loads
  - Battery Pack Development
    - 55 Ah LTO cells for high-C rate charging
    - 2 packs with 144 cells each
    - 2 packs can be either series or parallel
    - ~9C charge rate at 350 kW
    - Cells procured

LTO Battery Pack Specifications	
Capacity	18.2 kWh
Voltage (0-100% SOC)	230-396 V
Voltage (10-90% SOC)	305-354 V
Number of Cells	144
Number of Converters	18



One pack with 144 cells



8 cell module

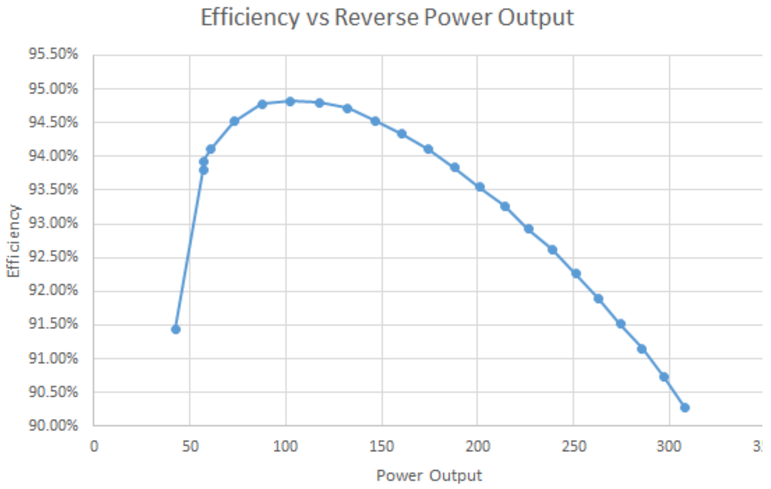


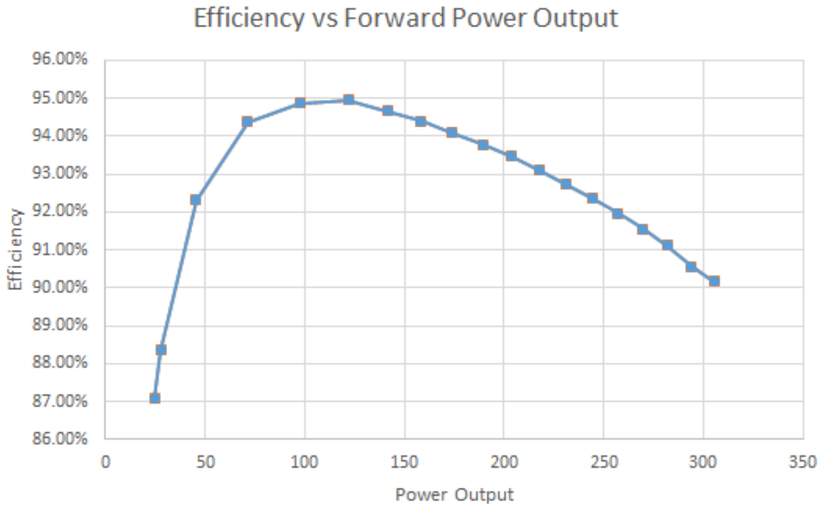
Technical Accomplishments and Progress: T10

- Hardware construction of BMS with integrated 5 kW DC-DC for vehicle low voltage loads
  - 5 kW BMS Development
    - ±300 W DC-DC module fully tested
    - Input voltage: 17 V – 20 V
    - Output voltage: 10.8 V – 13.2 V
    - CAN communication tested
    - Manufacturing of 18 modules for the 5 kW BMS in progress



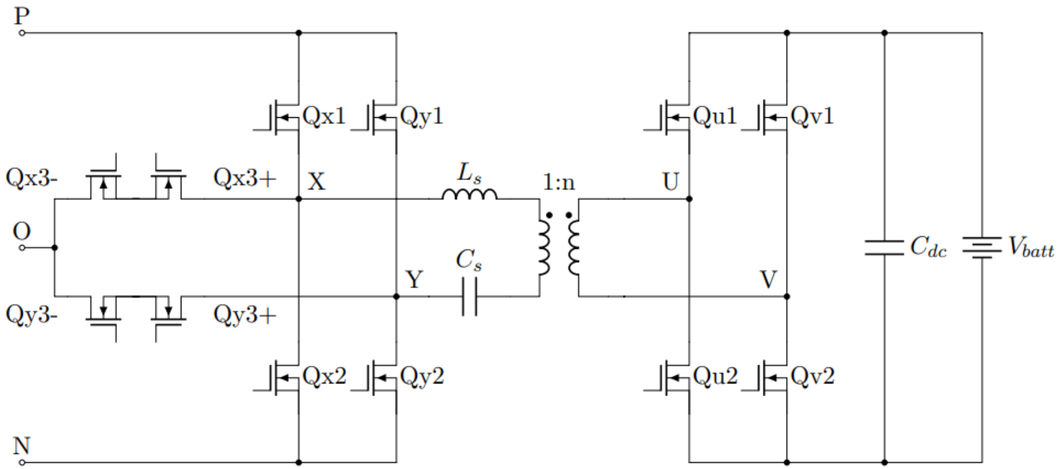
Converter connect to modules



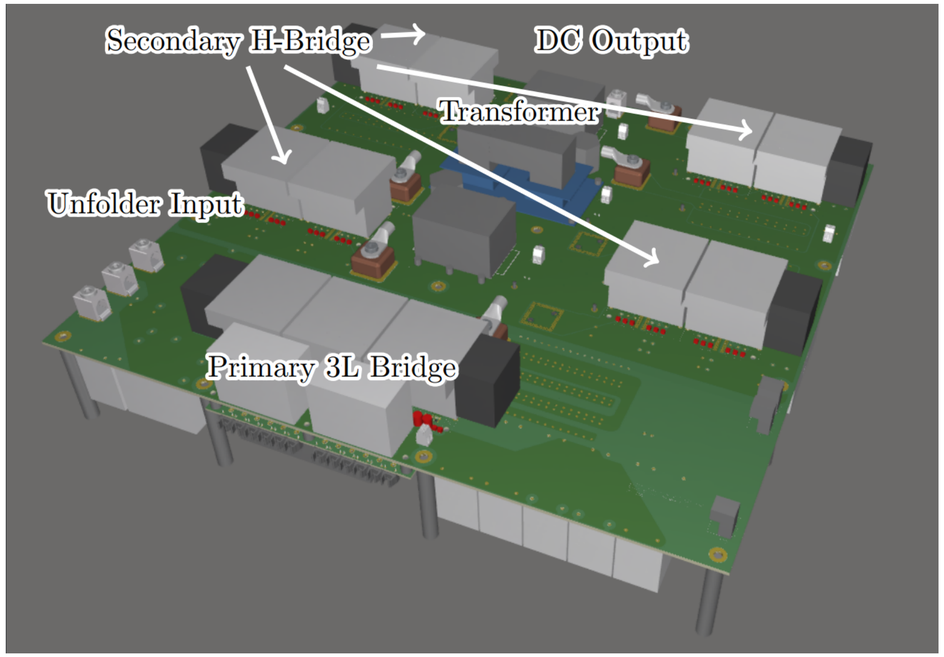


Technical Accomplishments and Progress: T11

- Hardware construction of approximately 60 kW module prototype for AC-DC converter
  - Iterating on the 2 kW AC-DC resulted in the 3LADAB module design
  - Modular design allows for the isolated outputs to connected in series/parallel as needed
  - Completed hardware design of high-power (18 kW) AC-DC module
  - PCBs sent out for manufacturing in early September
  - Waiting for the PCBs to begin tests



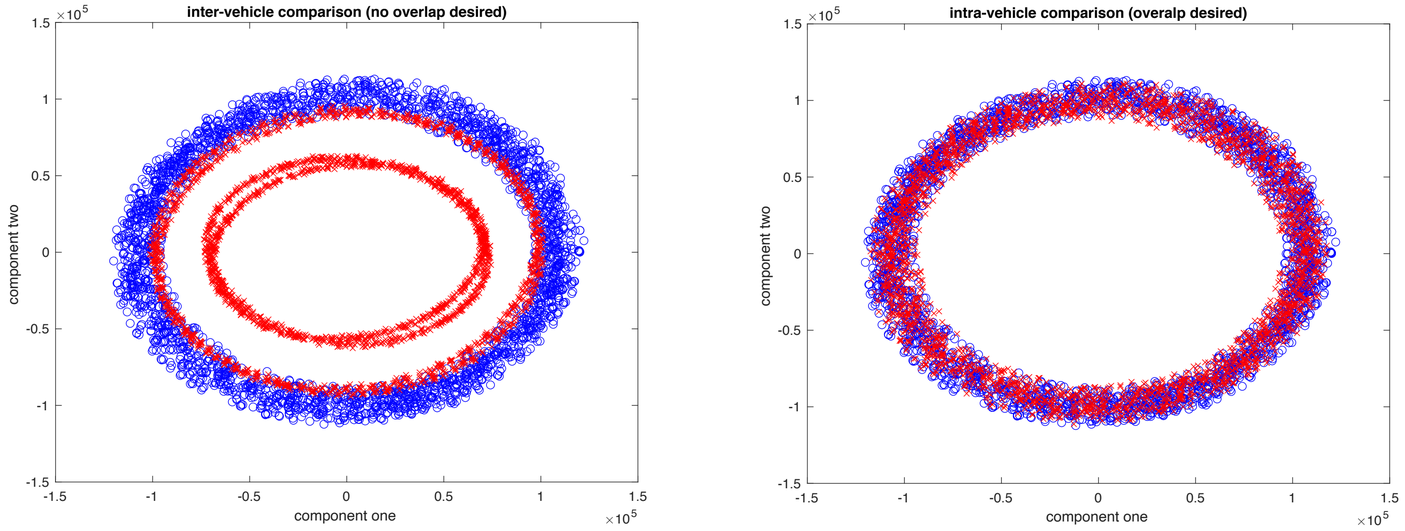
3-Level Asymmetrical Dual Active Bridge (3LADAB)



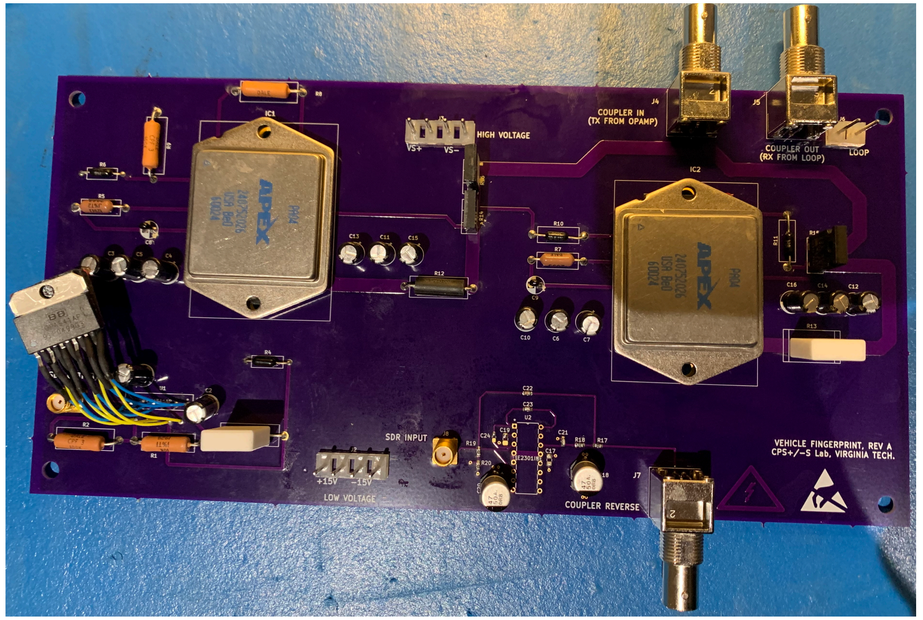
18 kW AC-DC XFC (Topside)

Technical Accomplishments and Progress: T12

- Inductive Fingerprinting of Vehicles
  - Prototype board:
    - uniform current (1 A), over 16 octaves, across highly reactive load
    - proof-of-concept: able to differentiate between two vehicles, reliably
      - Each vehicle has unique fingerprint
      - Fingerprint unaffected by position of loop
  - Final board:
    - 6 A (25—100 kHz)
    - Data collection ongoing: effects of temperature, orientation, more diversity in vehicles
  - Deliverables: Publication TBD



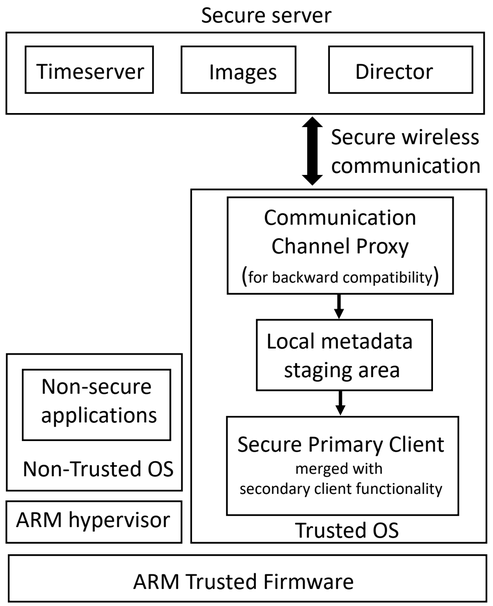
First two principal components (left) between two vehicles: no overlap indicates they can be differentiated and (right) for the same vehicle over two runs: since they overlap the fingerprint is stable



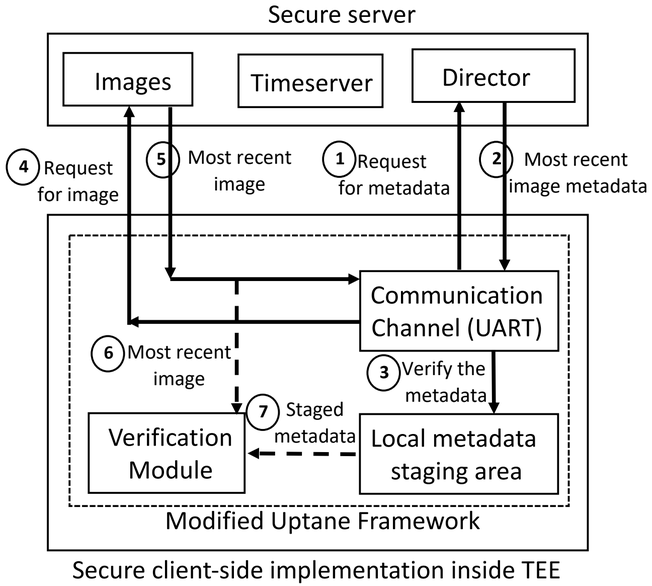
Inductive Fingerprinting Board, version two

Technical Accomplishments and Progress: T13

- Formally-Verified Firmware Update Procedure
  - Runs in Trusted Execution Environment
    - Guaranteed to execute (periodic interrupt non-maskable, highest priority)
    - Cannot be modified (resides in inaccessible memory)
  - UPTANE-compatible, open source
  - Implementation complete: SAW-verified data parsing (guarantee incoming data adheres to specification)
  - Deliverables: Trusted Verification of Over-the-Air (OTA) Secure Software Updates on COTS Embedded Systems, AutoSec 2021



Update architecture



Update procedure: formally verified input data correctness/parsing

```
Update cycle started.....
Submitting a request for a signed time to the Timeserver.
validated timeserver signature
Time attestation validated. New time registered.
Now updating top-level metadata from the Director and Image Reposi
 (timestamp, snapshot, root, targets)
YEAR MONTH DAY 2020 11 12
HR MIN SEC 20 50 45
Curr YEAR MONTH DAY 2020 10 13
Curr HR MIN SEC 3 23 12
Saved metadata is valid
The remote filename is root1.json
Retrieving validated image file metadata from Image and Director R
created vehicle manifest
created signable vehicle manifest
The signature has been generated
The signature method is: ed25519
The signature keyID is : none
Sending a request to server to submit vehicle manifest
Writing to Serial Port........
{
 "signatures": [
  {
   "keyid": "9a406d99e362e7c93e7acfe1e4d6585221315be817f350c026bbe
```

Responses to Previous Year Reviewers'

- *Perhaps a remapping of goals would be appropriate, given COVID-19 impacts on the project.* (and others)
  - Additional NCE requested (December, 2021); negotiated with DOE on scope
- *Some hardening approaches should be evaluated by third parties on a separate system to see if approaches have merit.*
  - We designed a test board to evaluate approaches and will submit results for peer review
- *The progress is stated as 55% which is well behind schedule.*
  - Some tasks had to be moved to BP2. NCE requested for BP2 and on track for project completion at end of year
- *there are still barriers with cross team knowledge of various domains*
  - Expanded number of meetings, participants, and collaboration activities

Responses to Previous Year Reviewers' Comments

- The tasks, workload, level of involvements, and accomplishments of each collaborator need to be clearly and accurately mentioned
  - See collaboration table; leads have > 51% responsibility for each task (often > 90%)
- *(a vehicle which is incapable of XFC charge rates) will reduce effectiveness of testing and the results will be biased*
  - EV simulator is able to emulate vehicle with XFC charge rages; Ford Mustang Mach-E uses XFC-capable protocol (ISO 15118)
- *Expansion to other suppliers and charge point operators along with additional utilities is a key to maximizing input for a robust solution and needs to expand to include more of these variations*
  - We welcome input and have spoken/will speak at industry/academia events

Collaboration and Coordination

- Interactions
  - Prime provides quarterly reports to DOE PM
  - Prime call w/all partners: monthly (videoconference)
  - Prime call w/individual partners: monthly (videoconference)

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15
VT	S	S	L	S	S	S	L	S	S			L	L	S	S
GT			S					L	S						
USU									L	L	L	S			
TRI			S	S					S				S	S	
CEC			S		L	L	S								
FMC		S	S												
GER	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

- Barriers and Roadblocks
  - Delays due to XFC EVSE availability and NCE execution (Oct, 2021)
  - COVID-19 resulted in lab shutdowns for VT, USU, and ComEd and travel bans for VT and GER
  - Anticipate NCE for Dec, 2021
- 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 (and Ongoing) Research

- Task 2.1 – Perform a cyber-physical threat and vulnerability assessment of grid
  - Outcome: Attack trees and attack graphs for grid based on output from automated tools
  - Progress: simulation models complete, allowing for validation of attacks
- Task 2.2 – Perform 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
  - Outcome: Models of XFC loading behavior on microgrid based on simulated and real-world data
  - Progress: Straight-forward reachability intractable; approximation (clustering) will be used
- Task 2.3 – Development of a moving-target defense for sensor and actuator attacks against EVSE/BEV controllers
  - Outcome: HW integrated model-based framework that allows for detecting sensor and actuator attacks and switching to mitigating controller
  - Progress: completed model of AC/DC converter in Matlab (first ODE-based model of power converter) to use with learning-based (data drive) controller; weekly meetings between USU, GT, VT
- Task 2.4 – Design 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
  - Outcome: Cyber-physical security-hardened 60 kW AC-DC converter and 5 kW DC-DC converter

Proposed Future (and Ongoing) Research

- Task 2.5 – Use device fingerprinting to determine whether an actual EV is connected to the EVSE and, for the case of inductive charging, building a secure ranging system with spoofing detection to ensure that a vehicle is properly and safely aligned with the charging pad
  - Outcome: EVSE would be able to localize a target BEV
- Task 2.6 – Leverage a trusted-computing base to guarantee that a formally verified, remote firmware update procedure takes place, even in the case of unreliable primary communications
  - Outcome: Formally verified firmware update routine running in a TCB with capabilities to use primary and secondary communication channels.
  - Progress: Using Frama-C have discovered vulnerability in C version of UPTANE client/ discrepancy between reference implementation (python) and specification
- Task 2.7 – Extend the ISO/IEC 15118 protocol to ensure user privacy even in the case of untrustworthy agents or when communication has been impaired
  - Outcome: Implementation of privacy-enhanced ISO/IEC 15118 protocol