Cybersecurity for Grid Connected eXtreme Fast Charging (XFC) Station (CyberX)

PI: David Coats

ABB Inc.

06/04/2020

ELT205

Overview

Timeline

- Project start date: 01/2019
- Project end date: 12/2020
- Percent complete: 60%

Barriers

- Designing XFC station considering future extensions such as integrated energy storage
- Identify/detect anomalies in the XFC station using adaptive approach
- Integrate prototype result into power HIL testbed for real-world validation (agile management for travel constraints)

Budget

- Total project funding
  - Total: $2.1 M
  - DOE share: $1.68 M
  - Cost share: $0.42 M (20%)

Partners

INL: EV simulator and Power hardware-in-the-loop for demonstration, Don R Scoffield (lead)

APS Global: EV station threat analysis and demonstration, Rick Hansen (lead), Duncan Woodbury

XOS Trucks: Providing demonstration electric vehicle for testing of demonstration, Austin Benzinger (lead)

Relevance

Increasingly connected Electric Vehicle (EV) charging station system solutions provide new threat surfaces:

- EV charging infrastructure and supply equipment (EVSE)
- Electric vehicles and vehicle on-board systems
- Battery energy storage systems (BESS) and distributed energy resources with potential grid and facility integration

The consequence of providing smarter charging management and eXtreme Fast Charging (XFC) management systems is requiring more external connections from the EV station that then need to be secured.

Objectives:

- Determine key attack paths for EVSE and connected systems based on statistical probability, effort level/cost, and impactful events/chains of events, and cyber-physical security approach to detecting anomalies
- Research, develop, and demonstrate a reference XFC (>350kW) station to reduce the risk and impact of cyber intrusions
- Design a resilient XFC station management system to safeguard EVs, EVCI (electric-vehicle charging infrastructure), connected equipment such as Battery Energy Storage Systems (BESS), EV owners, and EV station operators

"Electrify America to add Tesla battery storage to more than 100 new charging stations," https://www.greencarcongress.com/2019/02/20190205-eatesla.html, Feb 2019

Approach

Milestones

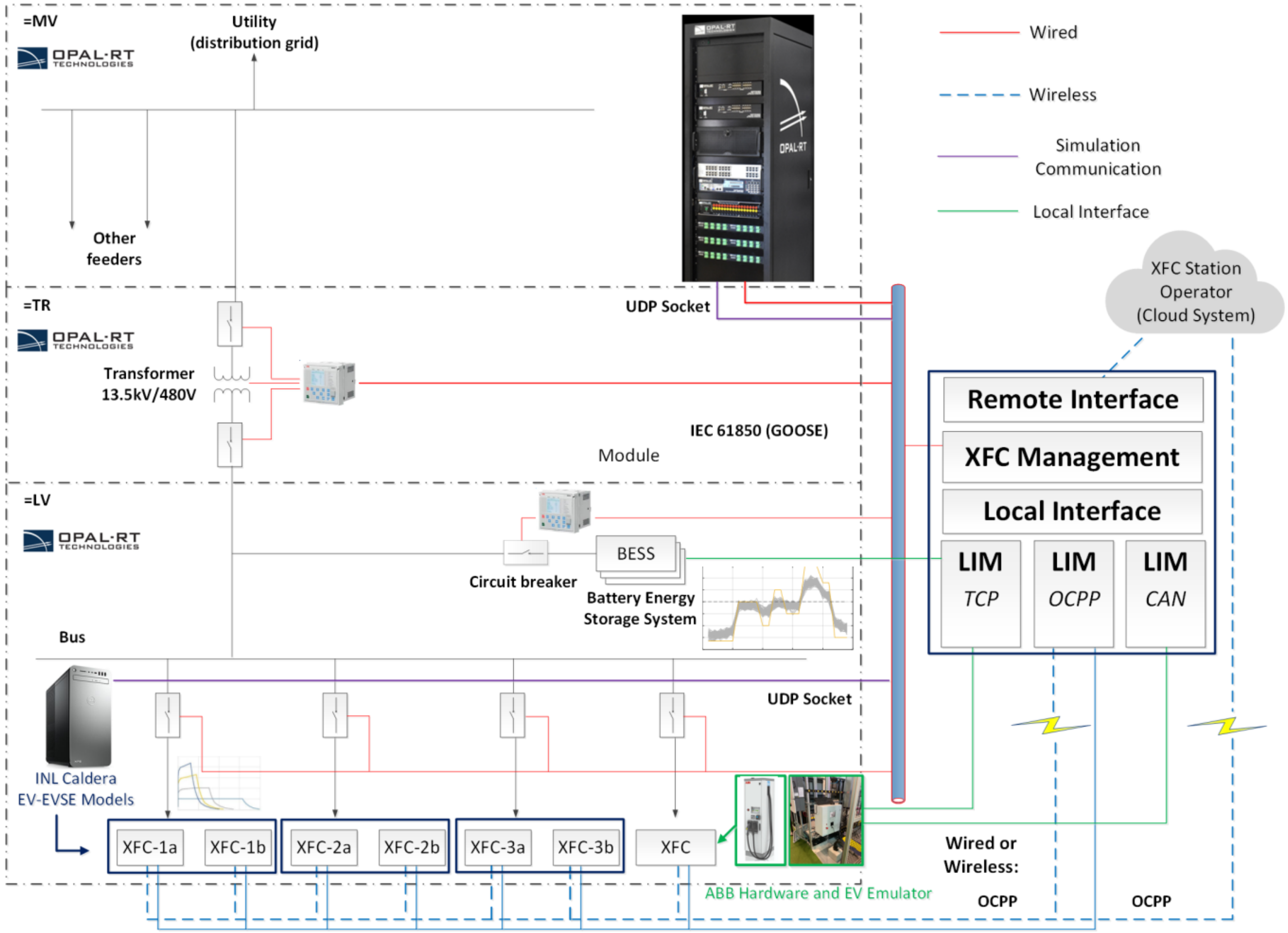
- Planned milestones and go/no-go decisions for FY 2019 and FY 2020

No.	Milestone	Date	Type
M1	Complete design documentation of XFC station	6/31/2019	Quarterly Progress Measure
M2	Complete threat analysis report	12/31/2019	Annual Milestone
M3	Complete report of resilient control architecture	12/31/2019	Annual Milestone
M4	Grid connected XFC station model, threat analysis, design documentation for XFC station, and developed defense mechanism	12/31/2019	Go/No Go
M5	Prototype implementation of resilient control architecture	6/31/2020	Quarterly Progress Measure
M6	Hardware integrated with HIL co-simulation platform and demonstration	12/31/2020	Quarterly Progress Measure
M7	Complete report of CyberX performance analysis	12/31/2020	Annual Milestone
M8	Knowledge transfer to ABB's EV charger business unit	12/31/2020	Annual Milestone

Approach

Detailed Tasks for CyberX Project Budget Period (Year 1)

- **Task 1.1: XFC station and control system - Completed**
  - Task 1.1.1: System layout and design
  - Task 1.1.2: Building base XFC station model & use cases
  - Task 1.1.3: Steady state use case modeling and analysis
- **Task 1.2: Threat analysis - Completed**
  - Task 1.2.1: EV and EVSE threat analysis
  - Task 1.2.2: XMS and utility control system threat analysis
- **Task 1.3: Secure XFC station control methodology development - Completed**
  - Task 1.3.1: Secure the communication infrastructure
  - Task 1.3.2: Develop CADS for individual XFC station
  - Task 1.3.3: Develop HLSE for XFC station
  - Task 1.3.4: Develop a mitigation mechanism for abnormal operation



Approach

Detailed Tasks for CyberX Project Budget Period (Year 2)

- **Task 2.1: Steady state validation – Low Power Verification**
  - Task 2.1.1: Prototype of algorithms, commercial platform
  - Task 2.1.2: Prototype intrusion scenarios according threat analysis
  - Task 2.1.3: Test the system against intrusion scenarios
- **Task 2.2: Real time validation – Low Power Verification**
  - Task 2.2.1: Integrate implemented CyberX platform with HIL testbed
  - Task 2.2.2: Adapt intrusion scenarios to the HIL environment
  - Task 2.2.3: Test the system against intrusion scenarios
- **Task 2.3: Performance analysis – High Power Verification**
  - Task 2.3.1: Performance measurement matrix
  - Task 2.3.2: Performance analysis reporting
- **Task 3: Knowledge dissemination**

Unique aspects - *(1) XFC station management system (XMS) with cybersecurity features (2) Prototype implementation using HIL testbed*

Low Power Verification @ ABB in Raleigh

High Power Verification @ INL in Idaho

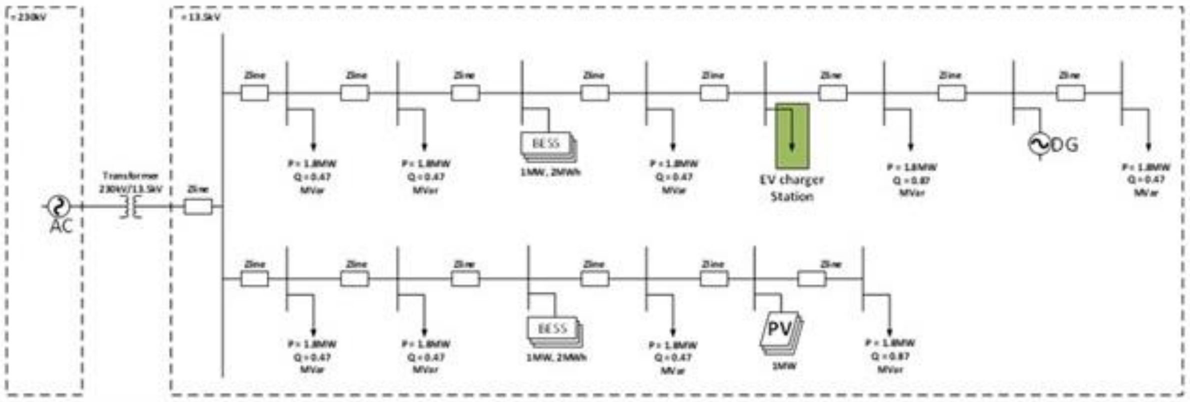
Technical Accomplishments to Date

Task Info	Tracking Metric	Goal for Period	Accomplishments	Completion	
				Expected	Actual
1.1 XFC Design Tasks (M1)	Design and simulate grid connected XFC station model	Successful simulation and testing of normal operation of XFC station	(1) Model based on 13.5kV to 480V distribution system (2) EV charging and battery integration use cases shown (3) Tested design with 3 abnormal conditions (4) Incorporated INL caldera data and converted model to real-time	Milestone 1 6/30/2019	Milestone 1 6/30/2019
1.2 Threat Analysis Tasks (M2)	Number of threat models developed and defined	Develop at least 8 threat models; demonstrate 1 model	(1) Developed system threat models to measure risks and impacts (2) Developed 7 main branching threat models (3) Demonstrated three 3 threat models, identifying critical events (4) Demonstrated XFC meter measurement spoofing attack concept	Milestone 2 12/31/2019	Milestone 2 12/31/2019
1.3 Resilient Control Architecture Tasks (M3,M4)	Number of cyber secure concepts developed for XFC station operation	Develop at least 2 cyber secure concepts for XFC station	(1) Developed communication monitoring and analysis for key protocols (2) Demonstrated monitoring, analysis, and machine learning for mitigation approach (3) Demonstrated capability to detect false data likelihood in state estimation method (4) Demonstrated abnormal EV state of charge mitigations based on Anomaly detection	Milestone 3 12/31/2019 Go/No-Go 1/31/2020	Milestone 3 12/31/2019 Go/No-Go 1/31/2020

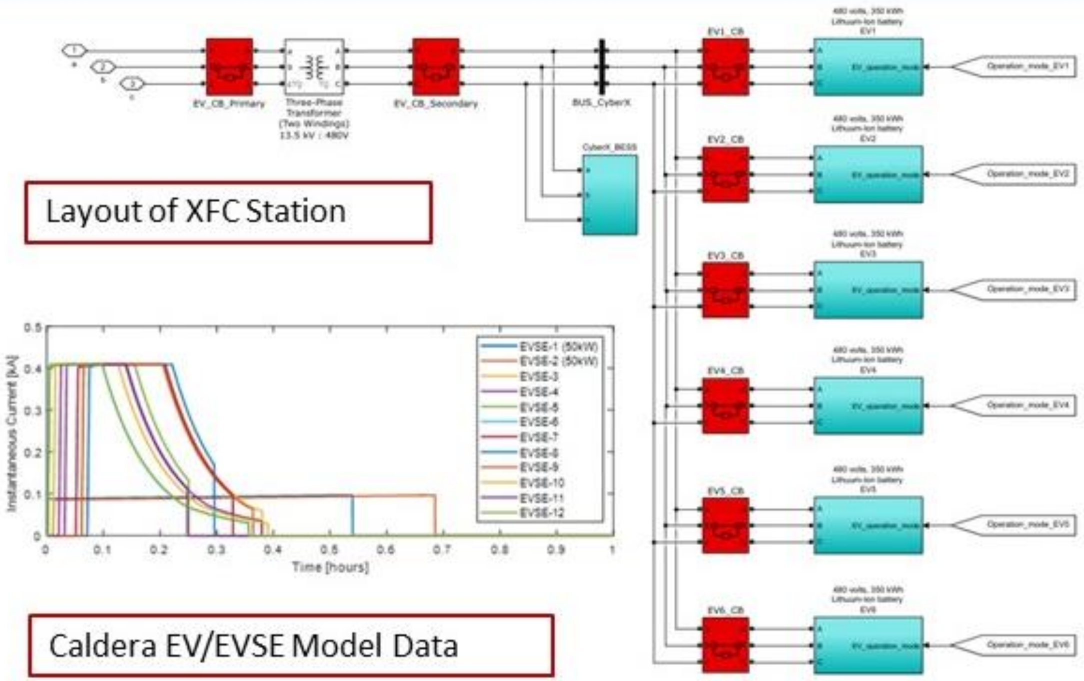
Technical Accomplishments to Date

Milestone 1: XFC Design Results

- Representative extreme fast charging (XFC) station and feeder system modeled within Simulink and then Opal-RT
- Based on the American Center for Mobility (ACM)’s planned circuit topology:
  - Distribution system elements at 13.5kV
  - Charging network and BESS elements at 480V
  - DERs such as Diesel Generators and Solar PV modules
  - Protection and control systems
- EV chargers simulated by INL Caldera model
- Connect to real-time model through Opal-RT dynamic load
- Communications systems prototyped
- Forms the basis of the future HIL tests at INL facilities



Single Line Diagram of XFC Station and Distribution System



Layout of XFC Station
Caldera EV/EVSE Model Data

Technical Accomplishments to Date

Milestone 2: Threat Analysis Generalized Results

- Representative model of 7 charging site components: XFC, BESS, XMS, Transformer, Rectifier, SCADA & Remote Management Systems
- Based on architecture specifications and practical analysis by APS Global and INL, 3,982 attack paths modeled
- Mapped attack paths to statistical probabilities to identify most impactful chains and individual events
- Initial conclusions general to all XFC EVSE
  - Front panel cellular modem – most likely attack surface to be targeted
  - Rapidly start/stop charging to affect charging cable – most likely cyber physical target

1	**Target Protocol Downgrade Attack (Cellular) (XFC) (Remote)**	Threat chain to end consequence →	**Rapidly Start and Stop Charging Session to Affect Cable (CP) (XFC)**
2	Target Cellular Base Station (Cellular) (XFC) (Remote)	Threat chain to end consequence →	Rapidly Start and Stop Charging Session to Affect Cable (CP) (XFC)
3	**Target Baseband Firmware Stack (Cellular) (XFC) (Remote)**	Threat chain to end consequence →	**Rapidly Start and Stop Charging Session to Affect Cable (CP) (XFC)**
4	Target Network Service Ports (OS) (XFC) (Remote)	Threat chain to end consequence →	Rapidly Start and Stop Charging Session to Affect Cable (CP) (XFC)
5	**Target System Component in Supply Chain (SWD) (XFC) (Local)**	Threat chain to end consequence →	**Rapidly Start and Stop Charging Session to Affect Cable (CP) (XFC)**

Technical Accomplishments to Date

Milestone 3: Resilient Control Architecture Results

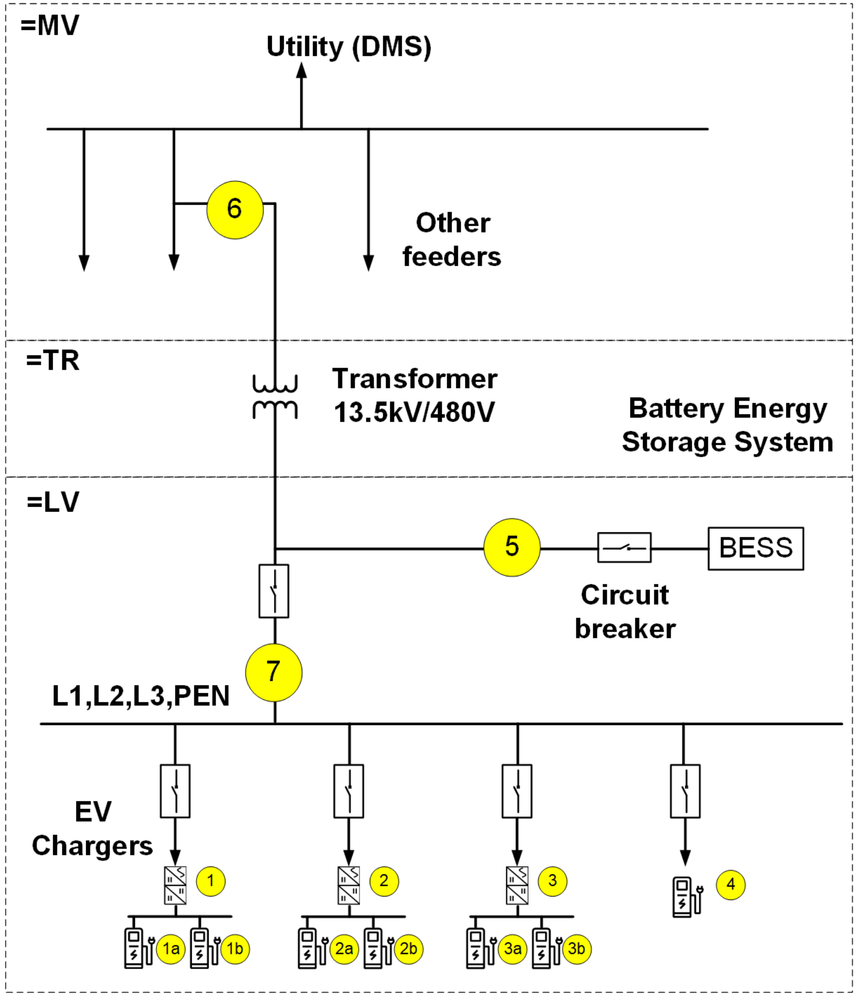
EV Station Control Model including BESS integration (Charge and discharge optimization)

Station Level Weighted State Estimation

- Total of 13 points (7 measurement and 6 sub-measurements) for state estimation provided to the XMS Gateway form a State Estimation Matrix
- Measurements are then weighted based on confidence
- Detection method implemented for falsified EV State of Charge (SoC) and current data based around Kirchoff Current Law (KCL) conditions represented in State Estimation Matrix
- Provides measurement error estimates and false data likelihood

Coordinated Anomaly Detection System

- Using classification and regression tree (CART) machine learning algorithm to determine expected charging time/measurements of vehicle
- Inputs are charging power, battery type, EV make/model, battery SoC at arrival, type of EV, and charging time
- Example threats based on manipulated SoC and current measurement at the EV supply equipment level



Responses to Previous Year Reviewers' Comments

- *Reviewer comment:* The reviewer wished the team had shown more specific information on station system layout and on use cases.
  - *Response*: Effort was made to show results for Milestones 1-3 to show the system layout (model and communications) and use cases (threat models considered)

- *Reviewer comment:* The reviewer suggested a vulnerability analysis should be done at the same time as the threat analysis. Most important is that the analysis of anomalies, their probabilities and their consequences should have been done at the same time (concurrent with the threat analysis)
  - *Response*: Part of what complicates the parallel threat analysis and vulnerability analysis approach suggested is that the team saw value in implementing some of the XFC Management system in model and doing the threat /vulnerability assessment including BESS, SCADA, etc. Working at DOE cyber-security coordination meetings and additional meetings with INL, we tried to reduce overlap of vulnerability analysis tasks relative to their Lab project. Part of the approach to anomaly detection is training machine learning models to cover emergent anomalies in operating conditions.

- *Reviewer comment:* The reviewer said there should have been more collaboration with the end-users (i.e. Vehicle OEM).
  - *Response*: The project team is working more closely with XOS trucks this year assess additional communication-based threats

Collaboration and Coordination

- **Project collaborators**
  - ABB (prime), industry
  - INL (sub), national lab
  - APS Global (sub), industry
  - XOS Trucks (sub): industry

- **Communications**
  - Weekly meeting, ABB internal
  - Monthly meeting, Project partners
  - As needed meeting with DOE and partners

- **ABB: Cyber event detection and mitigation architecture and practices, algorithm development and validation with HIL testbed**
  - Anomaly detection, machine learning, communications, and system modeling
- **INL: EV modeling, EV Cybersecurity, and Power hardware-in-the-loop simulator for demonstration**
  - EV/EVSE modeling, HIL testbed and power systems
- **APS Global: Electric distribution system model and threat analysis**
  - EV/EVSE cybersecurity and threat analysis
- **XOS Trucks: Electric vehicle for testing of demonstration**
  - EV engineering and demonstration platform

Remaining Challenges and Barriers

- Simulating anomalous conditions and identify/detect anomalies in the XFC station
- Providing a forecasting model based on INL's Caldera tools to facilitate with resilient control of the XMS and contribute to machine learning models for anomaly detection
- Validating feasibility of developed algorithms for detecting key threat models and integrate the prototype result into power HIL testbed
- Providing agile response to supply chain changes (scheduling and availability) based around response to present world/economic conditions

Proposed Future Works

- **Ongoing FY-20**
  - Currently working on testing and validation of prototype XMS and CADS algorithms on a commercial platform (hardware and software) to be utilized within the HIL EV station
  - Low Power HIL testing to be completed using EV emulator at ABB Laboratory
  - Test the system against intrusion scenarios, working to provide partners time on target for proof-of-concept demonstrations

- **FY-21**
  - High Power HIL testing to be completed using EV demonstrator platform at INL EVI Laboratory
  - Performance analysis and final demonstration at INL EVI Laboratory
  - Knowledge Dissemination

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

Summary

- Secure architecture grid connected XFC (>350kW) station modeled and in intermediate state for Hardware in the Loop demonstration
- Four completed milestones
  - Completed design documentation of XFC station and modeling
  - Completed threat analysis report
  - Completed report of resilient control architecture
  - Pass Go/No-Go Decision Point
- Validating CyberX layer for “CADS” cyber attack detection and mitigation
- Power HIL testbed and demonstration preparations and agile management to face travel and other restrictions

Technical Back-Up Slides

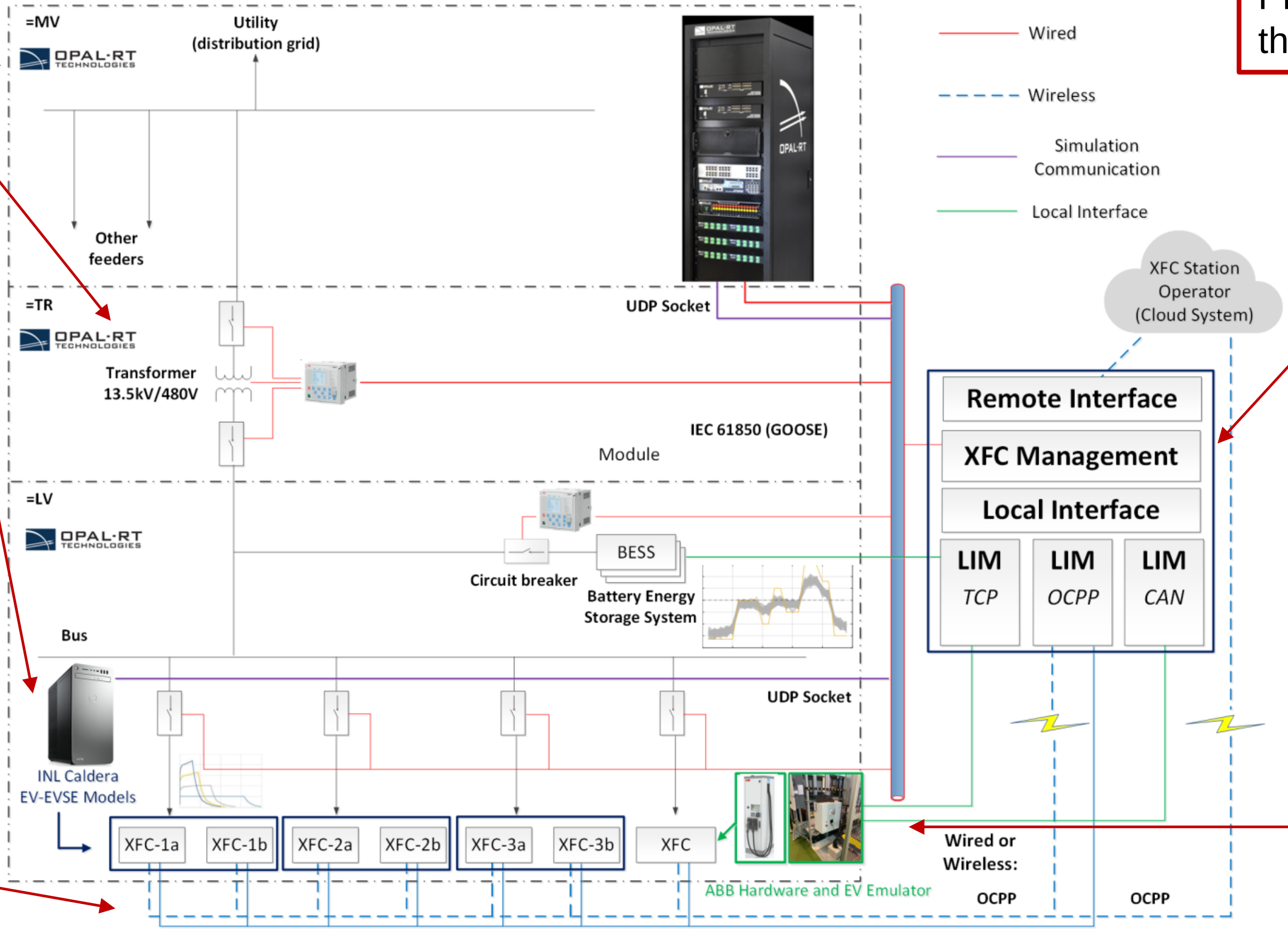
XMS Communication and HIL Testbed

Simulate distribution grid and XFC station BESS, protection

Emulate additional EVSEs on Linux device(s) using INL models

-Run Caldera on workstation/ gateway w/in VM or Container
-Socket communication of P and Q to Opal-RT from Caldera
-Socket from Opal-RT to receive Vpu
-OCPP streaming of metering info

Emulate EVSEs external communication interface to connect XMS



Provide local gateway for EVSEs that can interface w/ grid

Provide OCPP central server core functions

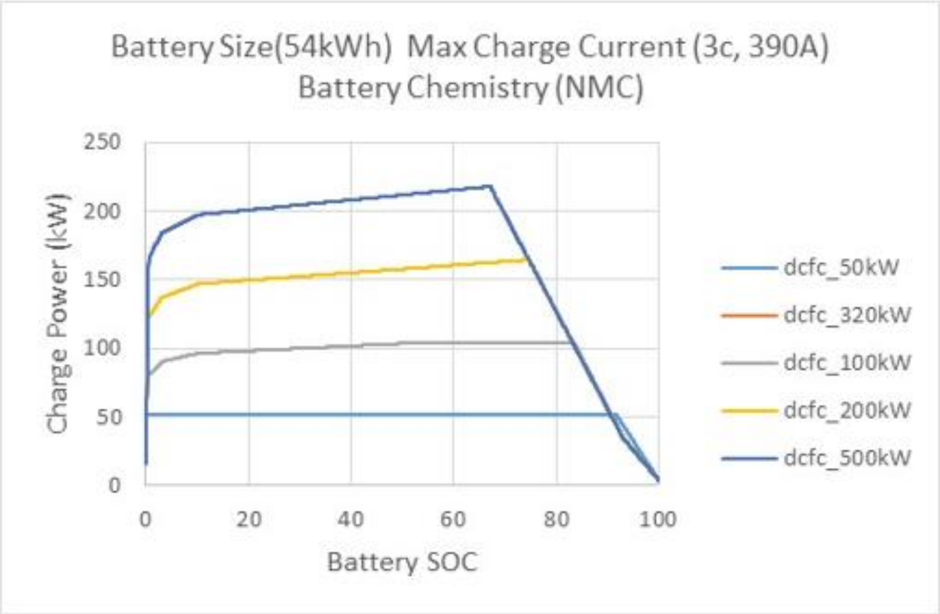
Connect ABB hardware and EV emulator (local) or EV demo platform (INL)

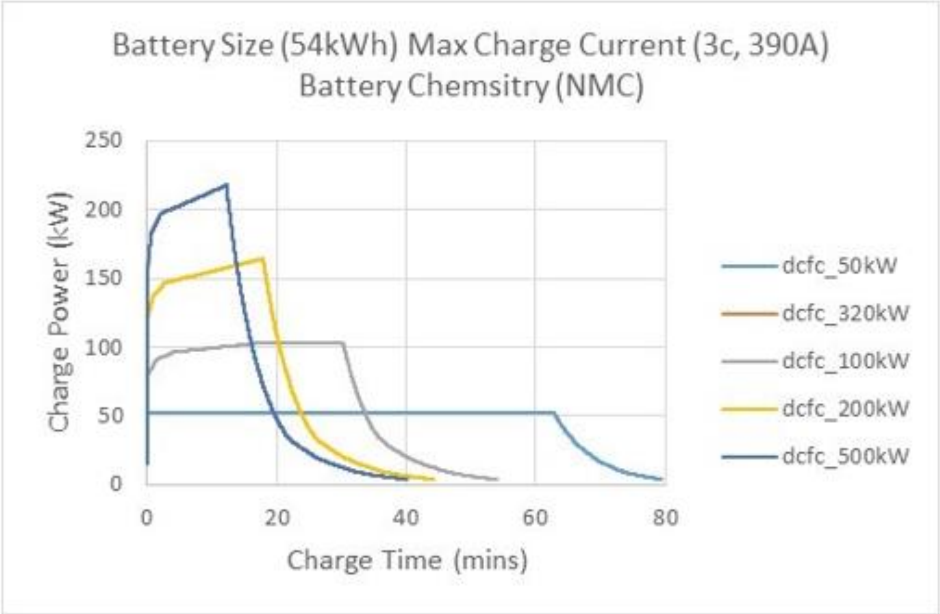
ABB

Resources and Capabilities (cont.)

High fidelity XFC charging models (INL)

- INL has done extensive battery testing for various battery chemistries
- Using test data able to generate high-fidelity charge profiles for PEVs that are not commercially available

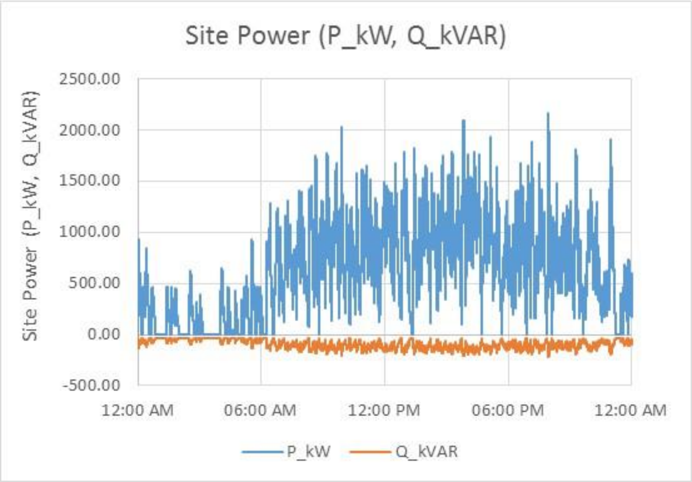




Resources and Capabilities (cont.)

High fidelity XFC charging models (INL)

- XFC site load profiles can be very volatile
- Volatile behavior may cause False Positives in anomaly detection systems
- Accurate charging models needed when designing system to avoid False Positives



- XFC site charge profile generated from charging models
- XFC site with 3 chargers and 6 total charge points
- All PEVs charged at site able to charge at 150 to 350 kW maximum dependent on existing connections at time of charge

ABB