U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Security Enhancements for DERs in Standardized IEEE 1547 Environments

ABB Inc.

Dmitry Ishchenko

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- The project addresses the gap in the IEEE 1547-2018 requirements on secure integration of DER, particularly DER systems consisting of multiple DER units.

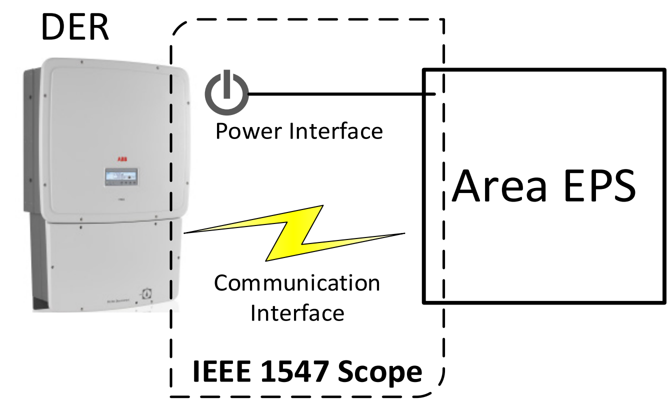
- **Schedule**

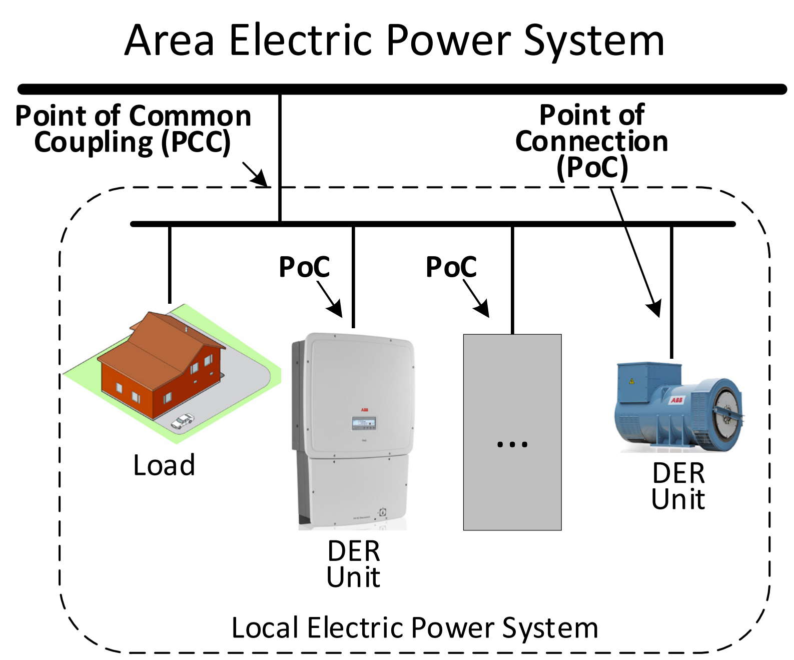
- 10/1/18 – 9/30/21 (delayed start 01/19)
- Threat modeling (Q1 2020)
- Resilient DER system architecture (Q2 2020)
- IEEE 1547 security extensions (Q3 2020)
- Lab-scale implementation (planned, Q1 21)
- Red team testing (planned, Q2 2021)
- Field demonstration (planned, Q3 2021)

Total Value of Award:	**$ 3,358,734**
Funds Expended to Date:	**30.4% as of 8/31/20 (Not all funds have been invoiced to DOE yet.)**
Performer:	**ABB Inc.**
Partners:	**University of Illinois at Urbana-Champaign; Duke Energy; Oak Ridge National Laboratory**

Advancing the State of the Art (SOA)

- IEEE 1547-2018 revision introduced new requirements for DER performance and interoperability:
  - Points of applicability may be defined at Point of Connection or Point of Common Coupling.
  - No guidance on implementing interoperability and response for microgrids with multiple DER units.
  - Cybersecurity requirements are not addressed.
- Our approach extends the SOA by implementing cyber-physical secure resilient IEEE 1547 use cases for DER systems:
  - Aggregated regulation, ride-through and system-level anti-islanding considering the potential impact of the mode/setpoint change on the overall system performance.
  - DER circuit communication architecture and security enhancements for IEEE 1547 protocols.





U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Advancing the State of the Art (SOA)

- Resilient IEEE 1547 DER system architecture and the use cases developed on top of open standards (IEC 61850-7-420) will enable interoperability.

- Similarly, proposed security extensions for IEEE 1547 protocols follow IEC 62351 practices.

- Use cases and semantic information models developed in the project contributed to UCA/OpenFMB Working Group to ensure industry acceptance.

- Field demonstration at Duke Energy to confirm the feasibility of the proposed approach.

Progress to Date

Major Accomplishments

- Defined threat models for major IEEE 1547 use case categories.
- Derived communication architecture and information models for hierarchical DER system based on open standards.
- Prototype implementation of IEEE 1547-constrained energy managements and resilient dynamic voltage support during ride-through with enhanced security mechanisms for Layer 2 and Layer 3 publisher-subscriber communications.
- Patent Application "Distribution Power System Fault Control Apparatus and Method" submitted.

Challenges to Success

Implementation delayed due to restricted physical access to laboratory facilities.

- Enhancing remote access capabilities to all hardware and software components that are needed for creating controller-hardware-in-the-loop setup.

Plans for field demonstration and red team testing affected by limited access to facilities.

- Work with the partners on arranging remote access to the facilities; consider HIL-only demonstration as a back up.

Limited technology transfer and outreach possibilities.

- Consider virtual event participation, possibly with pre-recorded video demonstrations.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- What category is the targeted end user for the technology or knowledge?
  - Asset owners (Utilities) and Vendors
- What are your plans to gain industry acceptance?
  - Controller and Power Hardware-in-the-loop testing, demonstrations at conferences/events in 2021
  - Field demonstration at Duke Energy facility in NC
  - Providing inputs to UCA OpenFMB/IEEE/ IEC working groups
- What is the timeline for demonstration and sector adoption?
  - Field demonstration and technology transfer with additional demos and working group presentations planned for 2021

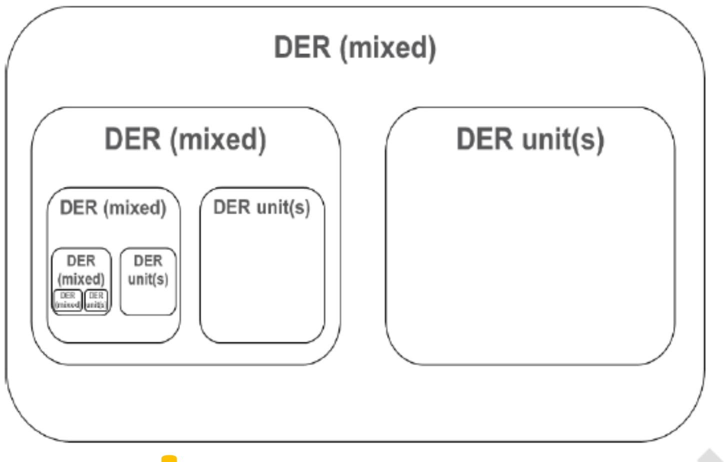
Next Steps for this Project

Approach for the next year or to the end of project:

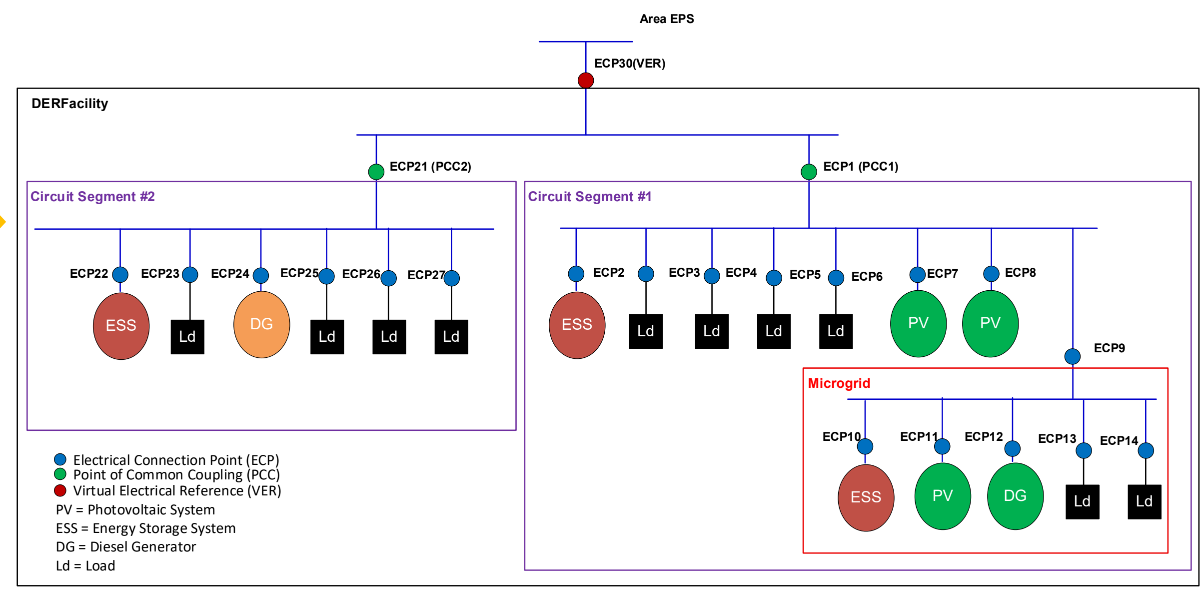
- Implementation and testing of the major use cases in CHIL and PHIL laboratory environment
- Red Team testing at ORNL
- Transition to field demonstration with algorithm tuning as needed
- Technology transfer – use cases and semantic models contributed to the community

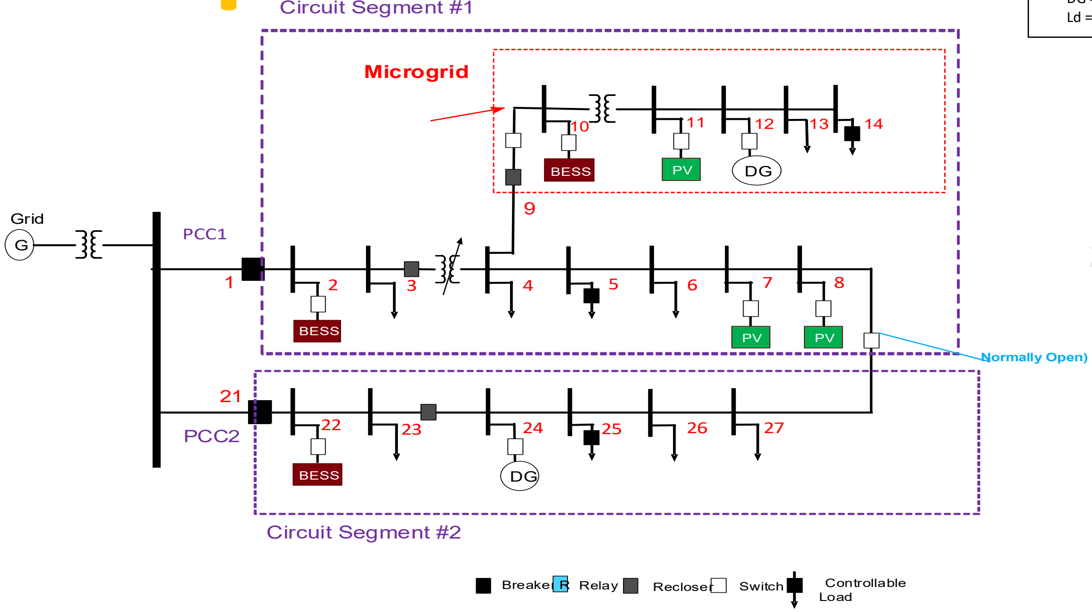
DER System Hierarchical Architecture

Concept of a recursive model for DER
IEC 61850-7-420 Ed. 2



Conceptual hierarchical Information model for IEEE 1547 operational and power management functions



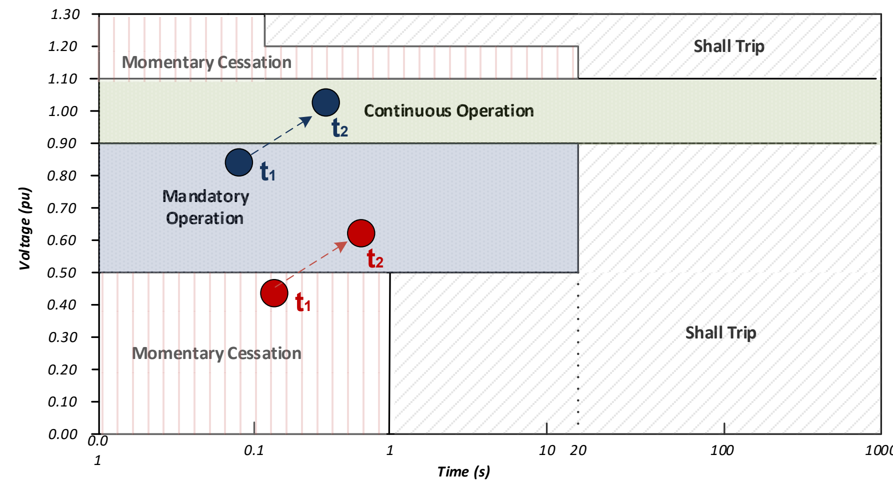


DER Two Circuit Segment
Feeder Model

Result: UML Model with derived semantic information models, actors, interactions, sequence diagrams and message profiles

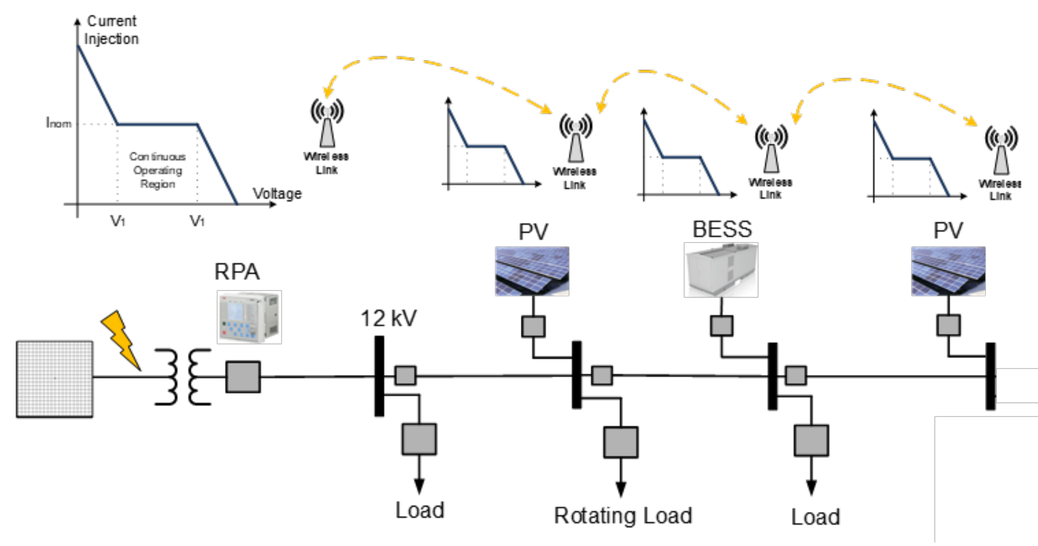
Use Case: Resilient Distributed Dynamic Voltage Support During Fault Ride-Through

- Grid faults -> Sensitive DER tripping
  - Fault ride-though and dynamic voltage support to keep DERs remain online and faster voltage recovery
- Uncontrolled local voltage support may become risky
- Aggregated cooperative response can shift ride-though operating point to safer region
  - Communication based methods require defining the appropriate message profiles and need enhanced security



<u>Solution Method:</u>

- Distributed cooperative dynamic voltage support (DCDVS) resilient to single point of failure
- Implements a multiagent based leader target tracking algorithm
- Avoids uncoordinated current injections via cooperative behavior
- Secure publisher-subscriber mechanisms according to IEC 61850-90-5, 62351-6, and IEC 62351-9 principles for wired or wireless communications



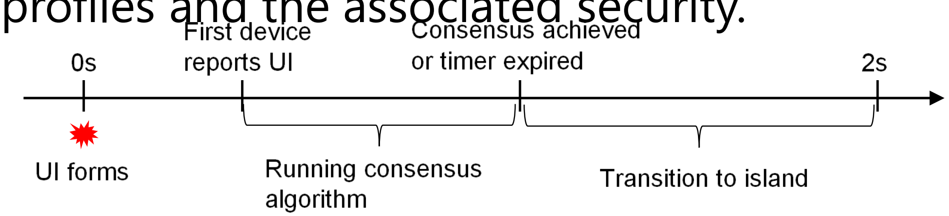
Use Case: Resilient Coordinated Anti-Islanding

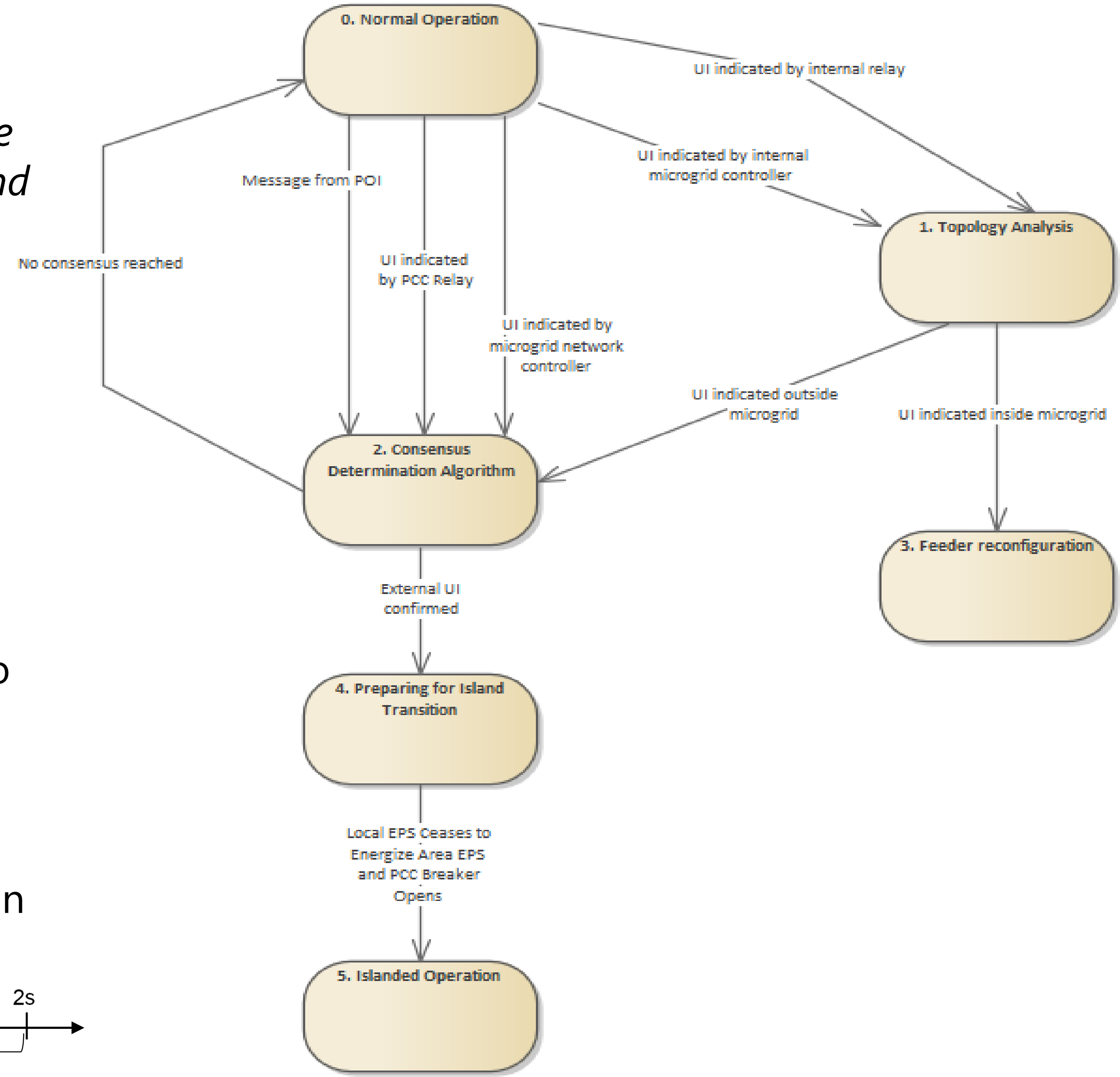
- *For an unintentional island in which the DER energizes a portion of the Area EPS through the PCC, the DER shall detect the island, cease to energize the Area EPS, and trip within 2 s of the formation of an island.*

- Leveraging measurements and local islanding detection methods at multiple locations to confirm an unintentional island condition has occurred.

- Consensus-based resilient mechanism to reduce non-detection zone and reduce attack surface.

- New information models, communication profiles and the associated security.





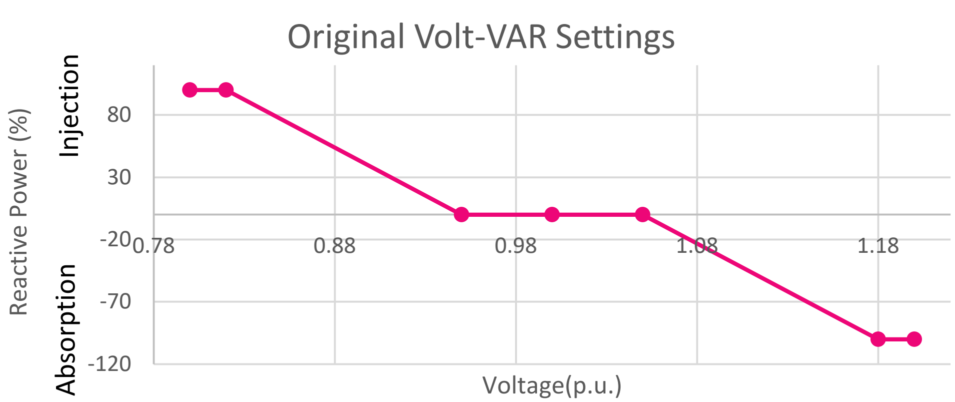
UIUC: Use Cases, Attacks, and Mitigation

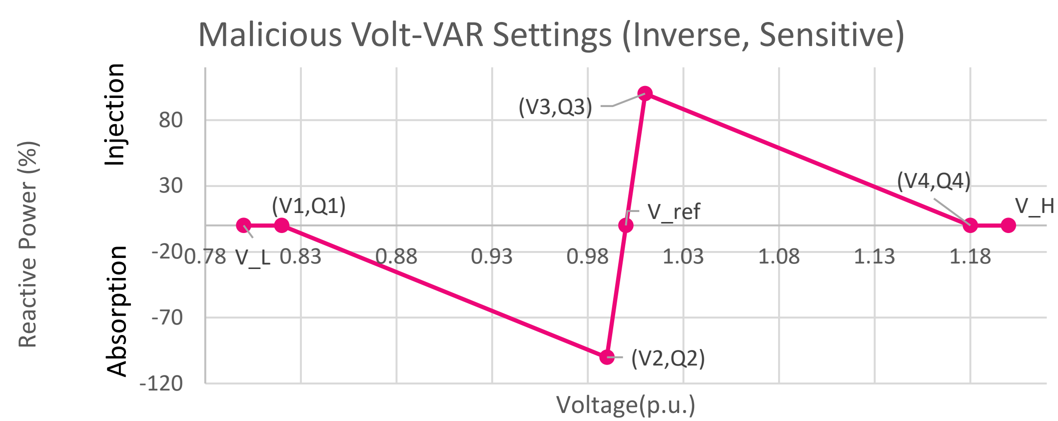
Use Cases demonstrating how misuse of IEEE 1547-2018 standard could result in grid instability.

- Malicious change of reactive power modes.
- Malicious change of state-of-charge information.
- Misuse of Volt-Var setpoints and conservative trip settings (See figures below).

Mitigations: Network detection methods being explored:

- Firewalls with intelligent packet inspection rules.
- Simulations to decide if a new command will make the system unstable.
- Machine learning approach to decide if new settings pose a threat to stability.

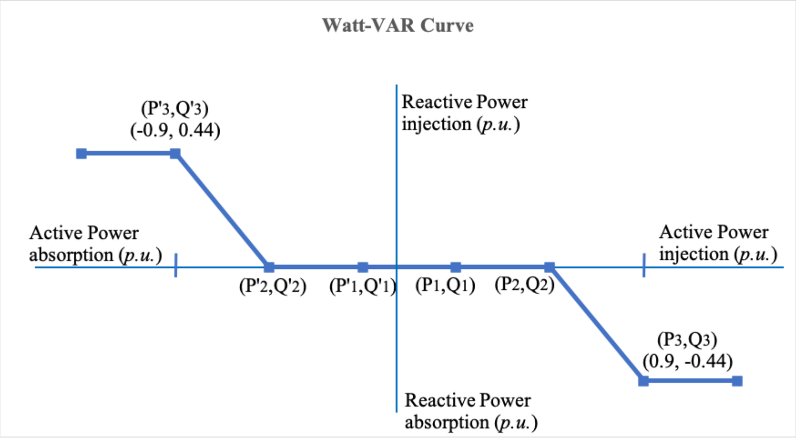




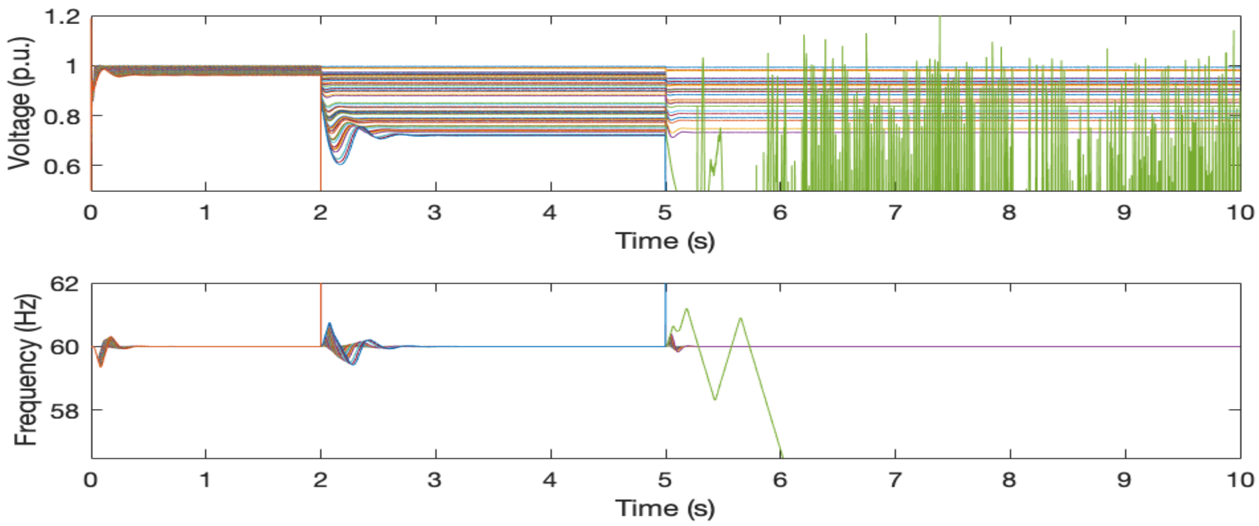
Example: Impacts of Malicious Mode Changes

Demo – Malicious change of reactive power modes

- Assume the system is operating in constant power factor mode, active and reactive power are injected.
- Voltage-active power mode is on (or turned on by attacker), causing maximum active power injection.
- Attacker sends a command to change to Watt-VAR mode, causing maximum reactive power absorption.



- Sudden change from Q injection to Q absorption causes voltage depression.
- Monte Carlo simulations show that with DER penetration as low as 14% of AEPS capacity, voltage and frequency collapse occurs.



U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Thank you!

Questions?