U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Cyber Attack Resilient HVDC System

ABB Inc.

Reynaldo Nuqui

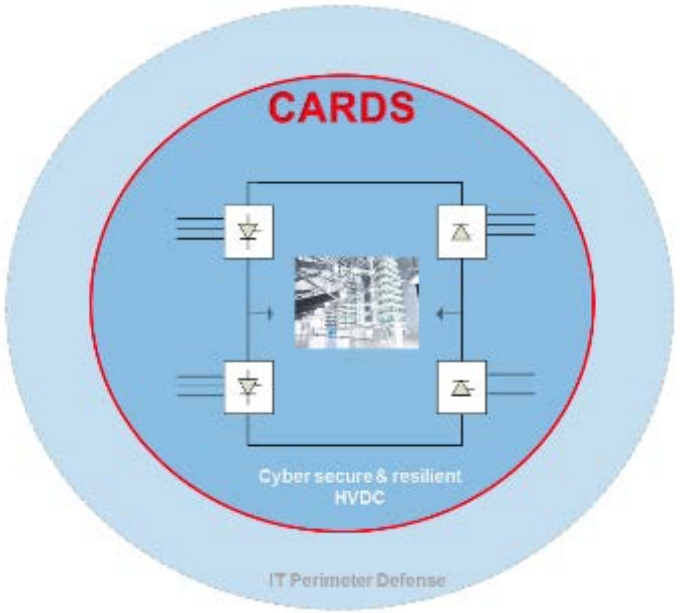
Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Cyber Attack Resilient HVDC System (CARDS)

Objective

- To advance the state of the art in HVDC systems cyber security by developing a security domain layer that enables high voltage direct current (HVDC) systems to defend against cyber-attacks. We will demonstrate our defense system, incorporated into the firmware of enhanced HVDC controller, at the Bonneville Power Administration (BPA) facility.
- Our research will focus on algorithms that defend against insider attacks that aim to disrupt electric power service by spoofing spurious power system control commands, or altering a device configuration, even if commands and data are compliant with respect to syntax, protocol, and targeted device. Detection is based not on conventional cyber network defense, but on the controllers assessing correctness in the context of a physical power system state, with application of physical laws of AC-DC systems and engineering principles.



Schedule

- October 2016 – Sept 2019
  - HVDC System threat models – 7/15/2017
  - Cyber secure HVDC system concepts developed and validated – 2/15/18
  - Power system state aware HVDC cyber security functions tested – 12/31/2018
  - Utility Demonstration – 3/31/19
  - Publications, panel sessions, industry and standard engagement for knowledge dissemination – 9/15/19
- Capability to the energy sector
  - Defense-in-depth cyber security for HVDC systems and associated utility systems using AC-DC systems physics and power system domain knowledge, utilizing DNP3, c37.118 and other industry standards.

Total Value of Award:	**$ 3,018,073**
Funds Expended to Date:	**% 59.8**
Performer:	**ABB Inc.**
Partners:	**Bonneville Power Administration, Argonne National Laboratory, University of Illinois at Urbana Champaign, University of Idaho**

Advancing the State of the Art (SOA)

- **Describe current "state of the art"**
  - Standard IT system security applied to industrial control systems
- **Describe the feasibility of your approach**
  - Our approach involves firmware extensions to HVDC controllers making use of available station measurements
- **Describe why your approach is better than the SOA**
  - Our approach brings cyber security closer to the controllers; the functions utilize the physics of DC-AC systems to mitigate cyber attacks

Advancing the State of the Art (SOA)

- **Describe how the end user of your approach will benefit**
  - The end user will be able to detect, block and/or alarm malicious and/or erroneous commands into the HVDC station resulting in a power grid that is resilient against cyber attacks.

- **Describe how your approach will advance the cybersecurity of energy delivery systems**
  - The approach forms a new defense layer, closer to the HVDC controllers and controlled devices, that is based on the physics of AC-DC systems. The approach is deployed as a user configurable and switchable set of functions extensions to HVDC controllers.
  - Cyber security is further reinforced by associated domain-based defense features in the control center EMS, WAMPAC, and MTDC control platforms.

Challenges to Success

Unavailability of representative RTDS power system model

- Extend and configure a generic RTDS model using PSCAD and PSLF models from our utility partner

Limitations in the number of control and IO (input-output) hardware in the HVDC test bed

- Adapt technologies from prior CEDS project to communicate other HVDC station measurements
- Set up hybrid configurations of HVDC IO and virtual IO components

Operating time of cyber security features delay existing control

- Focus on slower acting control applications
- Design and build more simplified code and algorithms

Progress to Date

Major Accomplishments

- Threat model document produced following the NESCOR format – Milestone #1
- Concepts developed for security against malicious DC power order commands from the SCADA system – Milestone #2
- Concepts for security against malicious emergency power order commands from special protection systems – Milestone #2
- Concepts for a station level AC-DC streaming state estimation to secure HVDC communication system – Milestone #2
- Concepts for a SCADA/EMS security feature against malicious power order commands injection into the SCADA network – Milestone #3
- Concepts for multi-terminal HVDC network security against malicious control commands and measurements – Milestone #3
- Concepts for a WAMPAC platform-staged security feature against malicious phasor measurements in a wide area controlled HVDC – Milestone #3
- GO decision achieved – Milestone #4

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

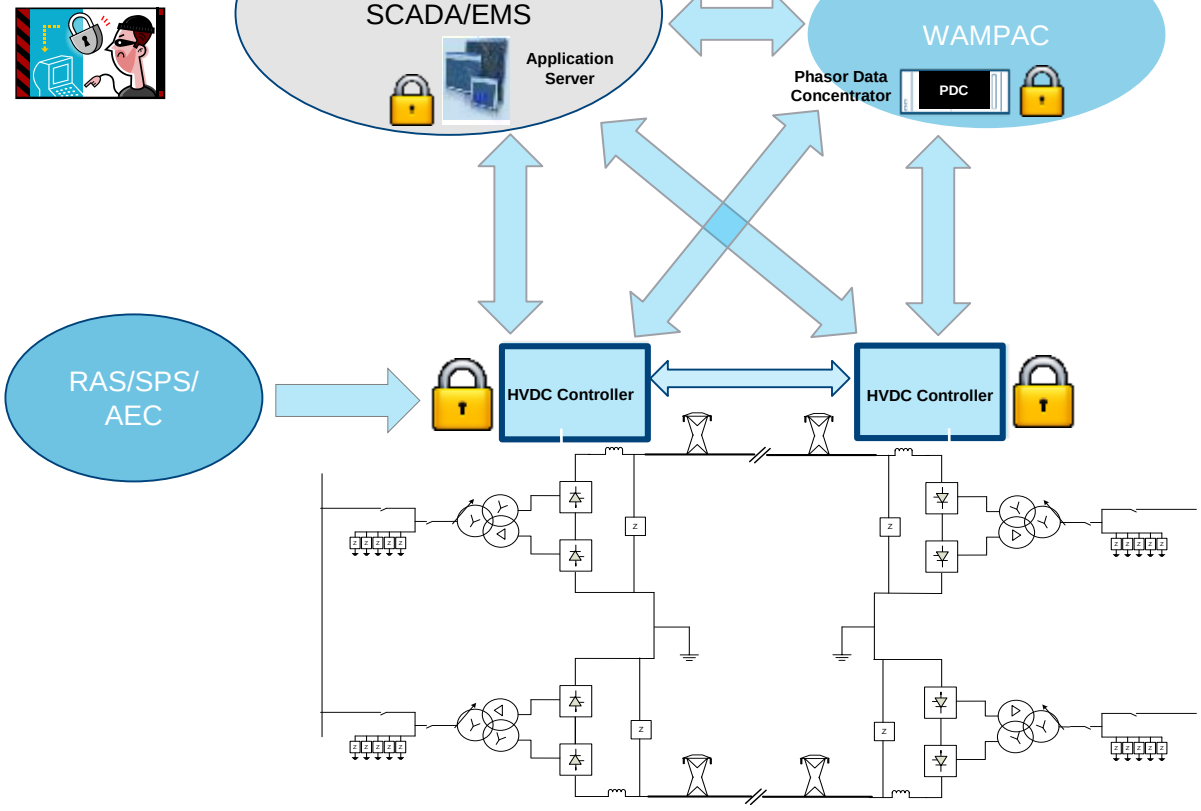
- What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)
  - ➢ The targeted end user for the Cyber Attack Resilient HVDC technology or knowledge will be the asset owner, specifically electric utilities
- What are your plans to gain industry acceptance?
  - o Describe testing and demonstrations planned
    - ➢ Testing shall be done in a laboratory environment consisting of commercial grade HVDC controllers and sensors.
    - ➢ Demonstration and further testing is planned to be held at BPA using commercial grade HVDC controllers, sensors, and representative communication.

Next Steps for this Project

Approach for the next year or to the end of project

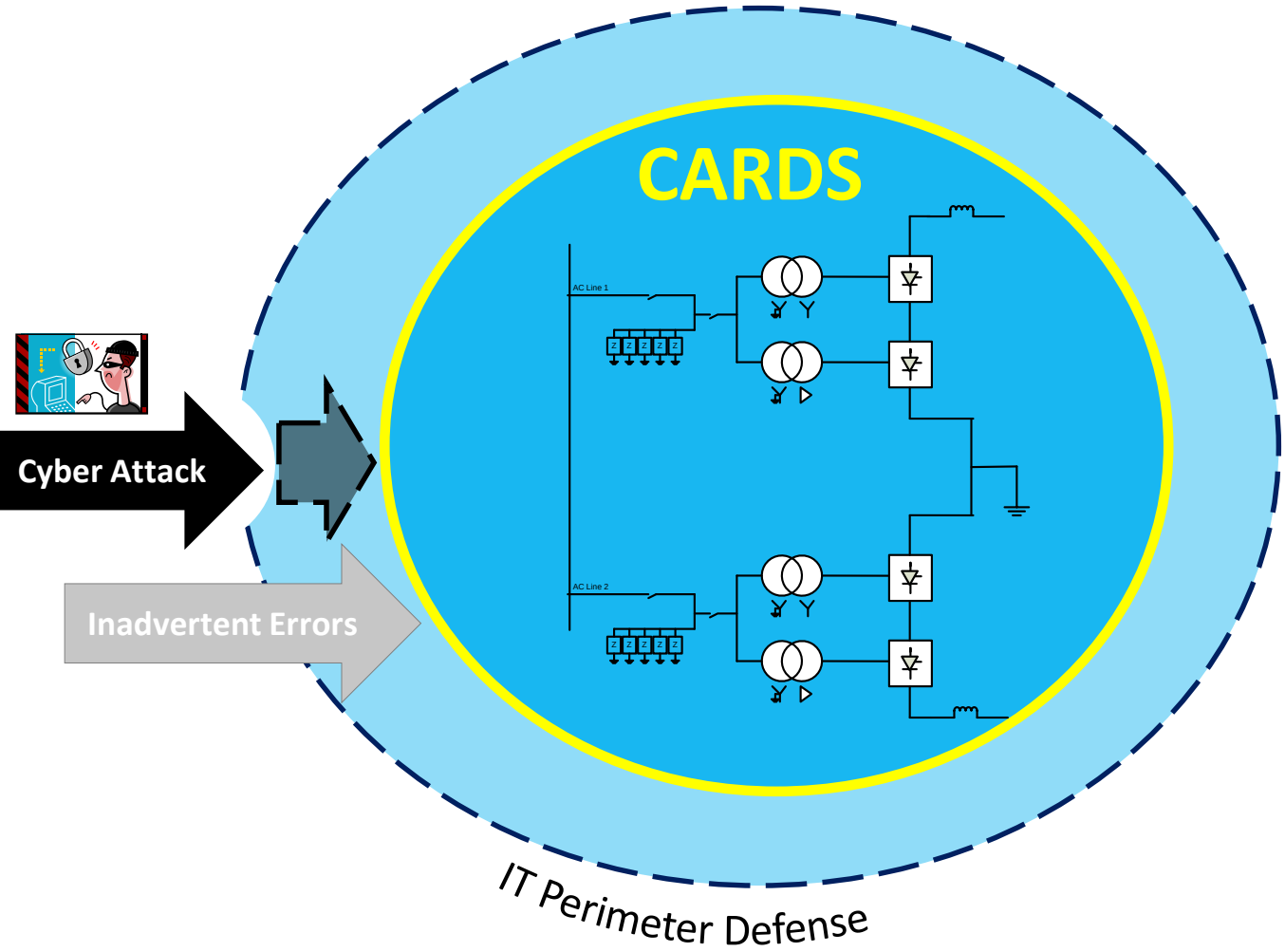
- Key Milestones: Milestone #5 until Milestone #9 to complete
- Deploy, test and verify the performance of developed functions in a hardware in the loop simulation composed of HVDC control hardware and IO devices
- Demonstrate research-grade prototypes at a BPA facility using commercial HVDC control and protection hardware
- Organize panel sessions, author publications, and engage industry standards to disseminate knowledge gained from the research project

HVDC and its interaction with utility systems



- HVDC Interacts with several utility systems
- Operational reliability and operational security requirements drive these interactions
- Vulnerabilities exist between these utility systems
- Vulnerabilities could be exploited by malicious actor to inject commands and measurements

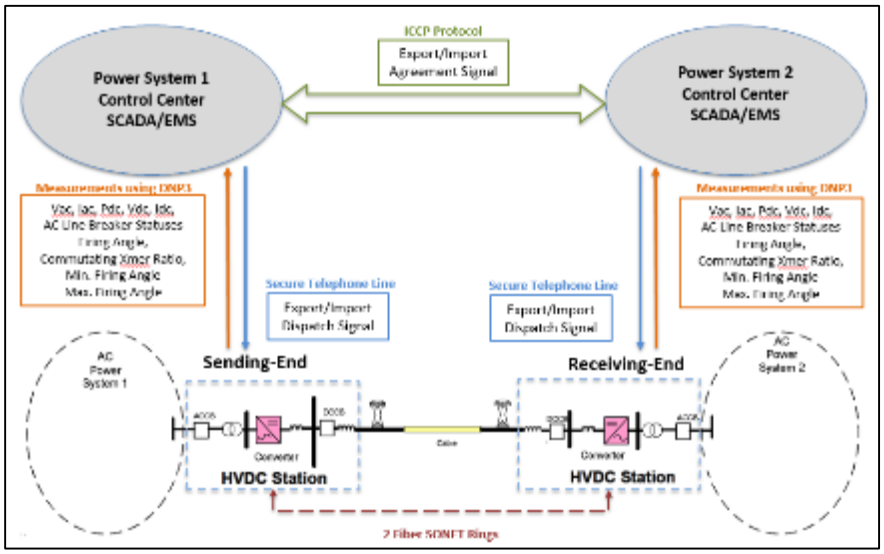
Defense-in-depth using AC-DC physics and power system domain knowledge



- HVDC control function extensions for cyber security
- Works with existing HVDC station measurement system
- Switchable and configurable functions

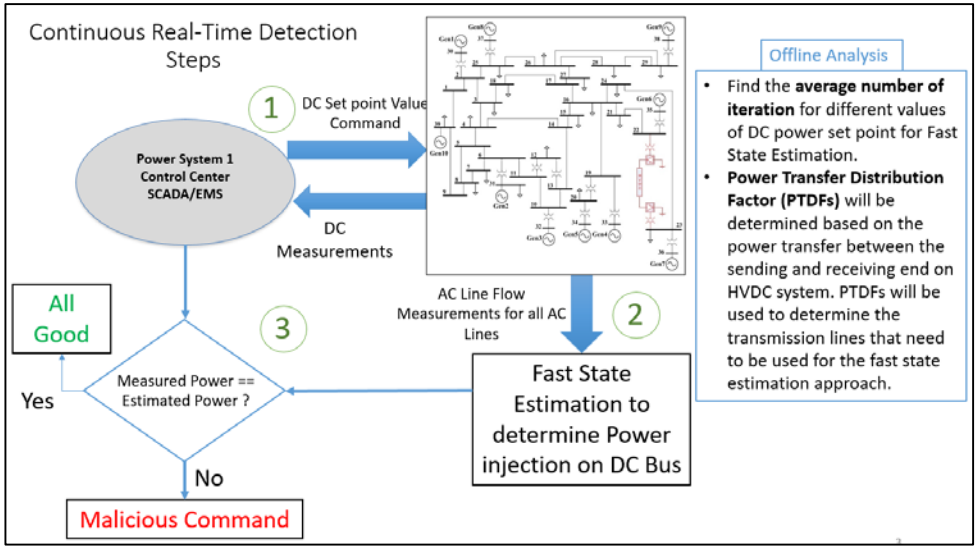
Control Center to HVDC Cyber Security

University of Illinois Urbana Champaign



- Using the fast state estimation (FSE) approach we determine the actual power flow on the HVDC system using only the measurements from the rest of the AC transmission lines
- If the estimated power is different from the measured power on the HVDC system, we regard the HVDC system to be in malicious state
- An offline analysis for the given system topology is performed to determine the number of iterations for FSE, and PTDFs for determining the number and location of transmission lines for measurements to used in FSE

- University of Illinois' role in the project is focused on examining issues of interoperability and vulnerabilities in control center to HVDC station data communication
- Figure on the left shows the basic system operation and data communication between HVDC station and the Control Center
- At present we are considering the threat scenario of simultaneous attack on the power order command from the control center and the HVDC measurement going to the control center
- Figure below illustrates off-line analysis and on-line detection steps



Cyber secure wide area controlled HVDC

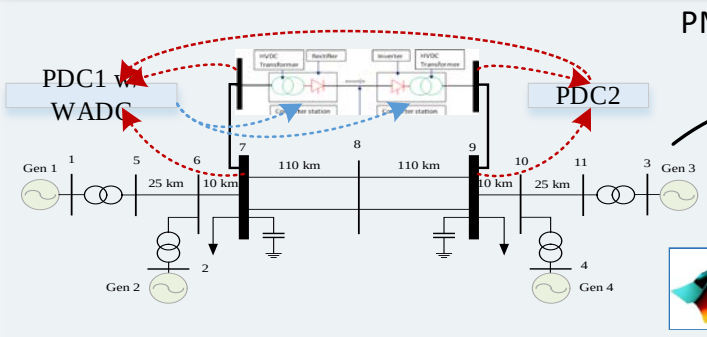
Argonne National Laboratory

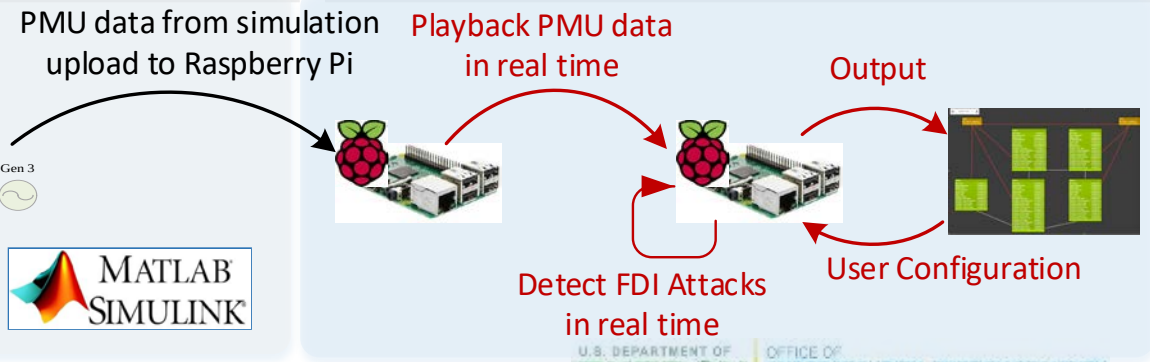
Task 1: Research and develop solutions to detect and prevent False Data Injection (FDI) attacks

- **Goal**: Detect and prevent FDI attacks using PMU data considering measurement noises and various operation conditions
- **Technical Challenge and Solution Approach**: Develop a detection method to meet the requirement for accuracy and execution time; Evaluate the method under various noise and operation conditions
- **Status**:
  - ✓ Developed a rule-based detection method based on physical laws and interdependency between physical quantities
  - ✓ Developed PMU data sets considering measurement noises and various operation conditions
  - ✓ Optimize the detection code to reduce execution time
  - ❑ Develop parameter tuning methods to improve accuracy

Task 2: Implementation and Demonstration

- **Goal**: Demonstrate the detection technology in a real-time demonstration environment
- **Technical Challenge and Solution Approach**: Develop the demonstration environment on Raspberry Pi in terms of simulation file playback, data communication, graphical user interface (GUI), use case development and validation
- **Status**:
  - ✓ Implemented the algorithm code in Python
  - ✓ Tested the Python code on Raspberry Pi
  - ✓ Developed a GUI
  - ❑ Implement the demonstration environment and data communication on Raspberry Pi
  - ❑ Develop use cases and validate the demonstration system



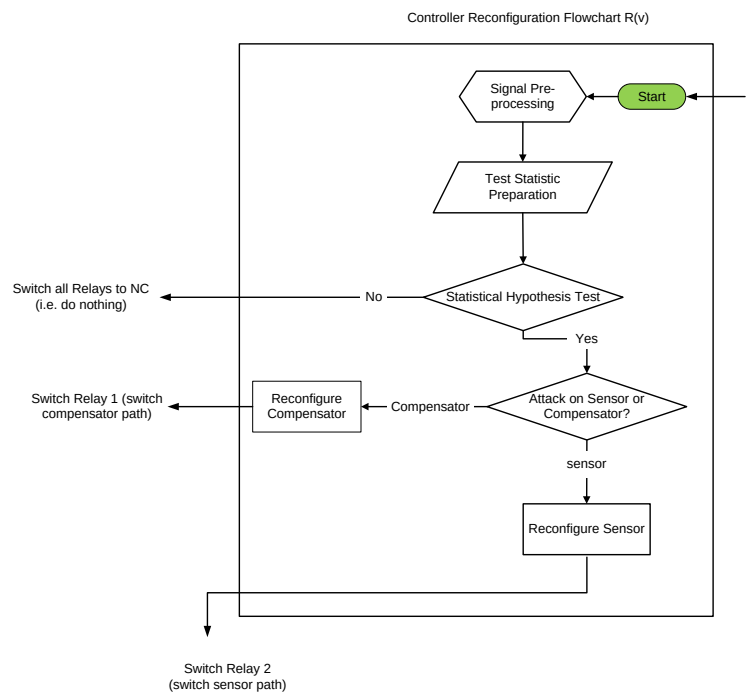


U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Cyber security of multi-terminal HVDC

University of Idaho

- Develop security solutions against cyber attacks on multi-terminal HVDC (MTDC) systems
- Identify potential threats
- Modeling and control design support to the project team



Technical tasks

1. Threat assessment document
   - Completed
2. Detection of attacks on voltage source converter based MTDC test system model
   - Differentiate between attacks and disturbances
   - Develop schemes to detect attacks on measurement and commands based estimates from larger measurement set
   - Substitution for corrupted measurements
   - In progress
3. Evaluate response of control loops to detect incorrect measurements or set points
   - Threshold for operator action to assess conditions
   - Controller actions with less aggressive performance expectations
   - Differentiate measurement noise
   - Develop theoretical basis for thresholds to differentiate attacks from disturbances
     - In progress
4. Development of series MTDC model to apply detection and mitigation methods
   - Model still in development