Reynaldo Nuqui
ABB

Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks (CODEF)

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Power and productivity
for a better world™ ABB

BONNEVILLE
POWER ADMINISTRATION

Ameren
ILLINOIS

I L L I N O I S
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

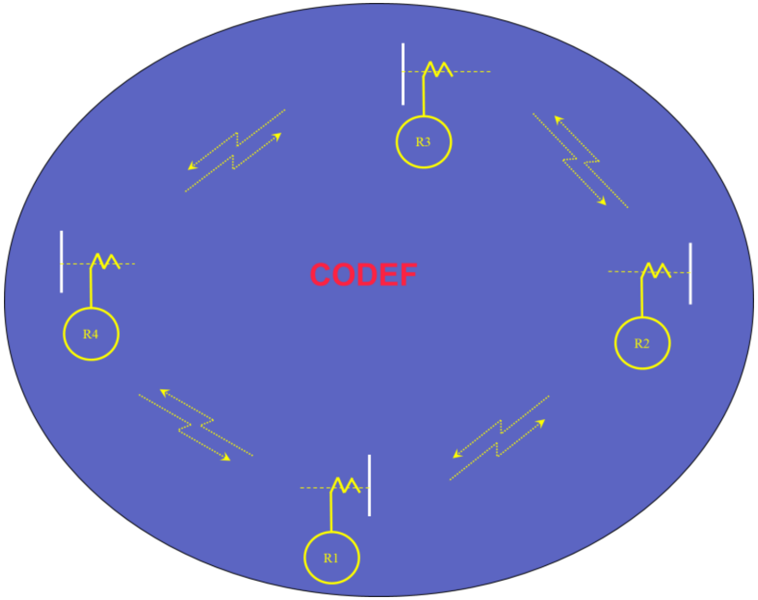
CODEF

Objective

- TO advance the state of the art for cyber defense methods for transmission and distribution grid protection and control devices by developing and demonstrating a distributed security domain layer that enables transmission and protection devices to collaboratively defend against cyber attacks in an IEC 61850 environment.

Schedule

- 10/2013 – 12/2016
  - Distributed Security Enhancement Layer Design – July 14, 2014
  - Distributed Security Enhancement Layer Implementation – March 13, 2015
  - Security Demonstrator – May 12, 2016
- Capability to the energy sector:
  - Inter-device level solution for smart detection of cyber attacks using power system domain knowledge, IEC 61850 and other standard security extensions

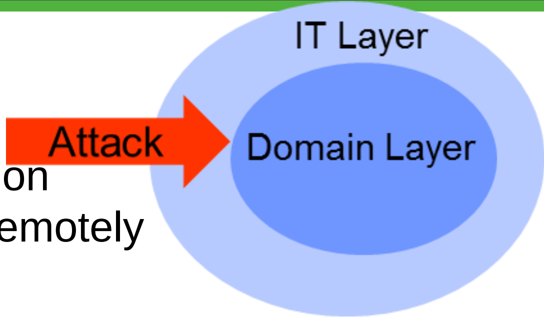


Performer:	ABB
Partners:	University of Illinois at Urbana-Campaign, Bonneville Power Administration, Ameren-Illinois
Federal Cost:	2,765,755
Cost Share:	936,729
Total Value of Award:	$ 3,702,484
Funds Expended to Date:	% 90

Advancing the State of the Art (SOA)

- Current “state of the art”
  - “Security by obscurity”
  - Unsecured or slightly secured data communication protocols
    - An attacker could inject false command and measurements and if they are syntactically correct will allow control of substation equipment.
- Why this approach is better than the SOA
  - Real time cyber security that is aware of power system operations
  - The physical state of the protected system is used to validate commands and measurements from the cyber layer.
  - Intelligence is distributed, collaborative and co-located or located close to the protected devices
- Feasibility of the approach
  - IEC 61850 substation automation protocol’s GOOSE and sampled value messages were used to realize collaboration among devices
  - Cyber secure mechanisms prototypes were embedded in each device’s firmware or in separate hardware.

Advancing the State of the Art (SOA)



- How the end user of your approach will benefit
  - Utilities benefit from increased cyber security of their substation automation devices and equipment from attacks conducted remotely or from insider threats in electrical substations.
- How the approach respects the operational requirements of energy delivery systems
  - CODEF works with existing substation automation protocols and devices with no need for additional instrumentation in electrical substations.
  - CODEF intelligence could be deployed as part of normal firmware updates and engineered using existing tools and software.
- Describe how your approach will advance the cybersecurity of energy delivery systems
  - The approach advances the cyber security of energy delivery systems by reinforcing existing IT security layers and adding an extra inner domain-based defense layer

Progress to Date

Major Accomplishments

- Transmission level cyber security functions demonstrated at Bonneville Power Administration in May 2016

- Distribution level cyber security functions demonstrated at Ameren-Illinois TAC substation in March 2016

- CODEF roadshow cyber security demonstrator featured at the PAC-World Americas Conference and Western Protective Relay Conference

Challenges to Success

Challenge 1: Speed of cyber security functions

- Sub cycle fault detection algorithm, GMAC authentication of GOOSE and sampled value streams

Challenge 2: Embedding the prototype solutions in commercial relay platform

- Utilized dedicated commodity hardware that are connected in hardware in a loop with the IEC 61850 enabled relays.

Challenge 3: Engineering the utility demonstrations

- Very close collaboration and teamwork with UIUC, BPA and Ameren-Illinois.
- Using a multitude of space heaters to mimic a real fault in a live test circuit

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Category of targeted end user for the technology or knowledge
  - The targeted end users are asset owners, specifically, electric utilities in both transmission and distribution business
- Plans to gain industry acceptance
  - Utility demonstrations with participants from both OT and IT groups present – 2 utilities
  - Roadshows in focused conferences using a self contained CODEF rack for on-demand demonstrations
  - Dedicated demonstrations within electric utilities
  - Publications, presentations and panel sessions in conferences
    - BPA and Ameren presented their utility demonstration experiences
  - Engaging standard making bodies to influence the adoption of the project's standard security extensions

CODEF Roadshow and Utility Demonstrations

U.S. DEPARTMENT OF
ENERGY
Cybersecurity for Energy Delivery Systems (C
Collaborative Defense of Transmission and Distribution Protection and Control D
Against Cyber Attacks (CO
Cybersecurity for Energy Delivery Systems R&D
Collaborative Defense of Transmission & Distribution Protection & Control Devices Against Cyber Attacks
ABB