FREEDM CENTER 2019 RESEARCH SYMPOSIUM | RALEIGH | APRIL 10, 2019

Cyber Security for Power Grids

Using Physics to Advance Cyber Security for Energy Delivery Systems

Reynaldo Nuqui, Senior Principal Scientist, US Corporate Research Center

Mission of session

Points of value

1 **Cybersecurity is a real issue and major concern for Energy Delivery Systems on all levels - from transmission to distribution**

2 **OT cybersecurity priorities are not the same as traditional business IT systems**

3 **First-principle based defense methods enhance Energy Delivery Systems cyber-physical security by implementing defense-in-depth protection**

Overview

Subtitle

Trends

- Focus on reliability, availability, power network stability
- Increased pressure from FERC on reliability and cyber security
- Growing interest in the digital substation / Ethernet architectures driven by lower cost, improved performance, reliability and safety
- Security attacks increasing (cyber and physical)

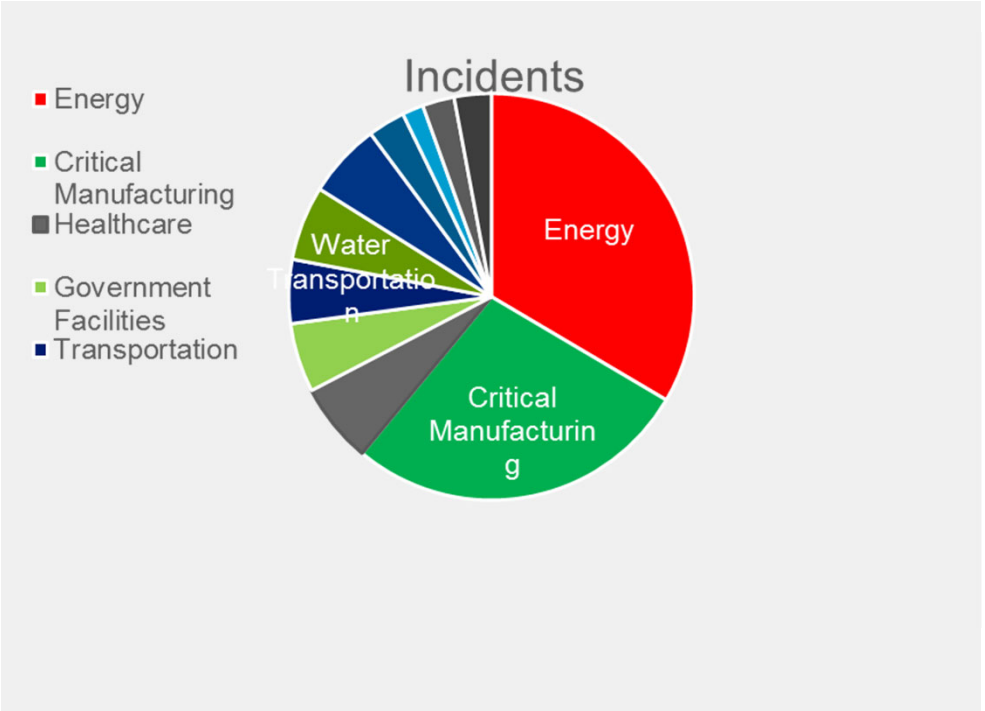
Challenges

- Utility resource constraint leads to inability to evaluate and approve new products
- Protection engineers and IT folks not living in the same world
- Cyber threats are present in both NERC regulated Bulk Energy System substation as well as the distribution voltage levels
- Ukraine incident

Cyber Security

A Major Concern

- The cost of cyber crime for the global economy in 2017 has been estimated at $600 billion annually, up from $445 in 2016
- US industrial control systems attacked 245 times in 12 months in 2015



Energy Sector Cybersecurity 1/

The energy sector has unique cyber security requirements

Energy Delivery Control Systems ≠ Business IT Systems

- Energy delivery control systems (EDS) must be able to survive a cyber incident while sustaining critical functions
- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- The modern grid contains a mixture of legacy and modernized components and controls
- EDS components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment
- EDS components are widely dispersed over wide geographical regions, and located in publicly accessible areas where they are subject to physical tampering
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory

1/ Carol Hawk, Following the Energy Sector Roadmap, presented at the NREL Cybersecurity & Resilience Workshop

The Challenge: Enterprise IT vs. Control Systems

A different set of challenges

	Enterprise IT	Control Systems
Primary object under protection	Information	Physical process
Primary risk impact	Information disclosure, financial	Safety, health, environment, financial
Main security objective	Confidentiality	Availability
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 - 3.65 days)	99.9 – 99.999% (accept. downtime/year: 8.76 hrs – **5.25 minutes**)
Problem response	Reboot, patching/upgrade, isolation	Fault tolerance, online repair

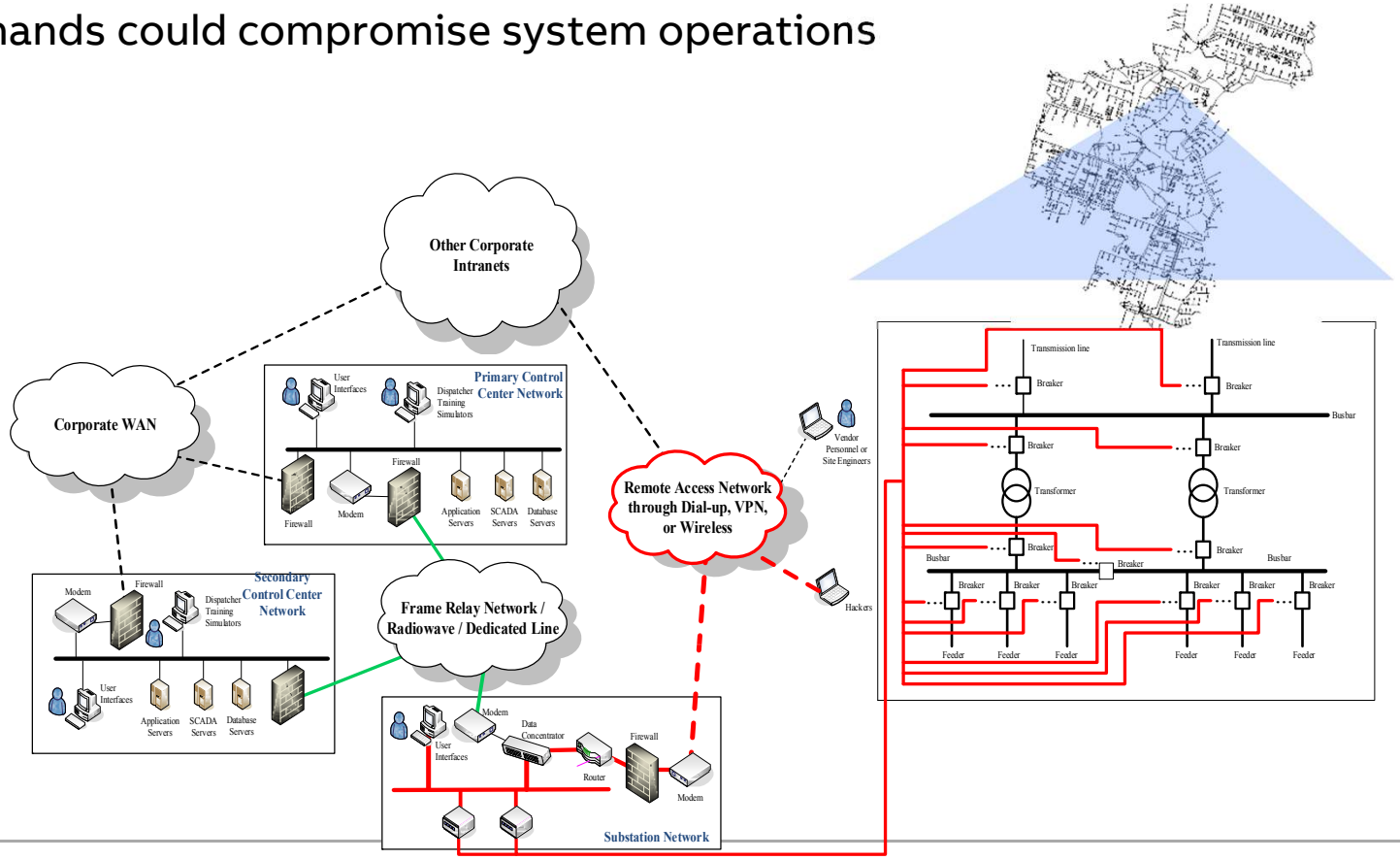
Substations are vulnerable

Loss of a substation could have adverse impact on OT

- Control centers rely on substations and communications to make decisions
- Substations are a critical infrastructure in the power grid (relays, IEDs, PMUs)
- Remote access to substation user interface or IEDs for maintenance purposes
- Unsecured standard protocols (like DNP3.0, 60870-5), remote controllable IED and unauthorized remote access
- Some IED and user-interface have available web servers and it may provide a remote access for configuration and control
- Well coordinated cyber attacks can compromise more than one substation – it may become a multiple, cascaded sequence of events

Intrusion into a Substation Network

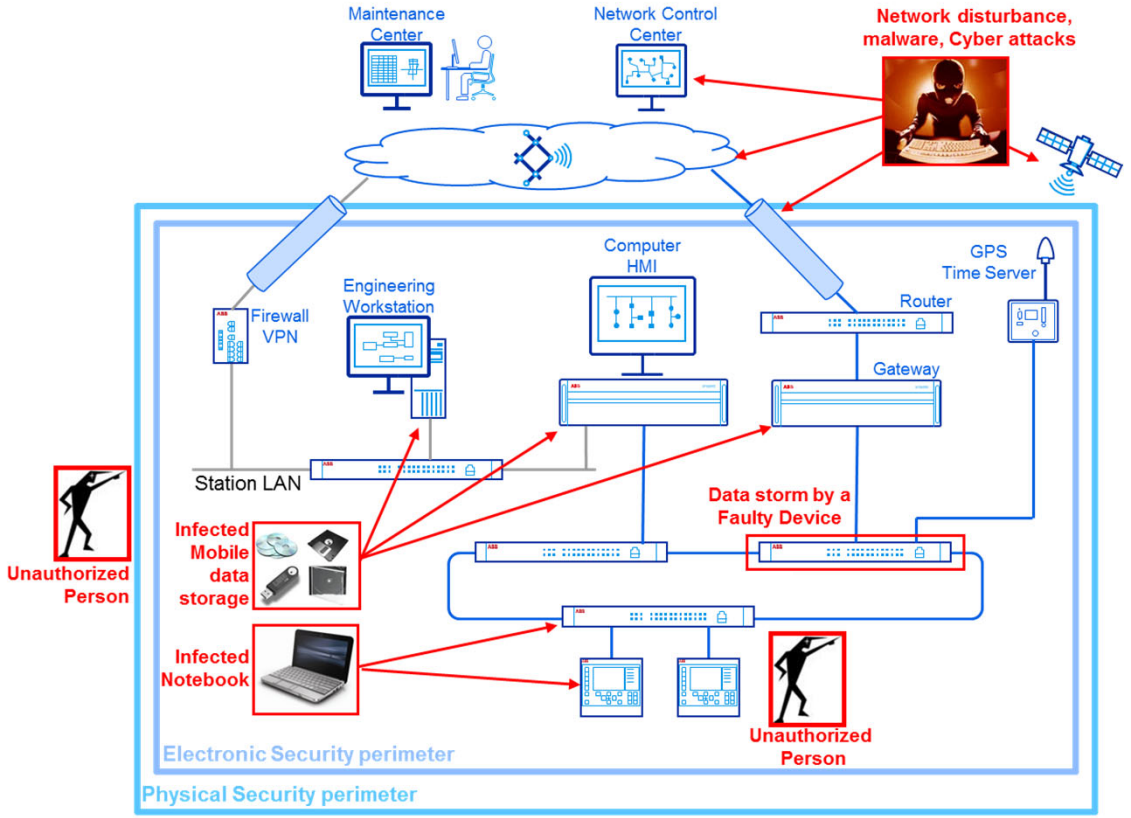
Malicious commands could compromise system operations



Protect – Defense in Depth

Unauthorized access or attack

The research projects presented here deliver defense-in-depth technology



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

Objectives

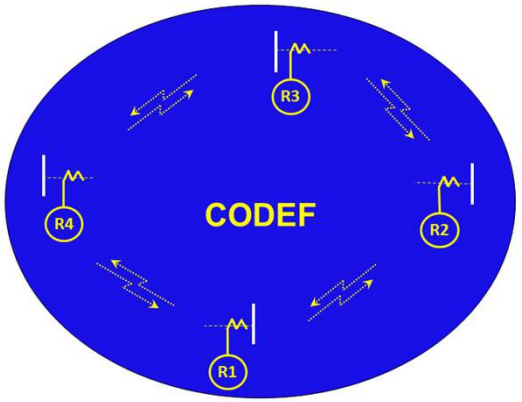
- To advance the state of the art for cyber defense methods for transmission and distribution grid protection and control devices by developing and demonstrating a distributed security domain layer that enables transmission and distribution protection devices to collaboratively defend against cyber attacks.

Schedule

- 10/2013 – 09/2016
- Distributed Security Enhancement Layer Design – July 14, 2014
- Distributed Security Enhancement Layer Implementation – April 11, 2015
- Utility 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



Funding: DOE Cyber Security for Energy Delivery Systems Program (CEDS)

Performer: ABB

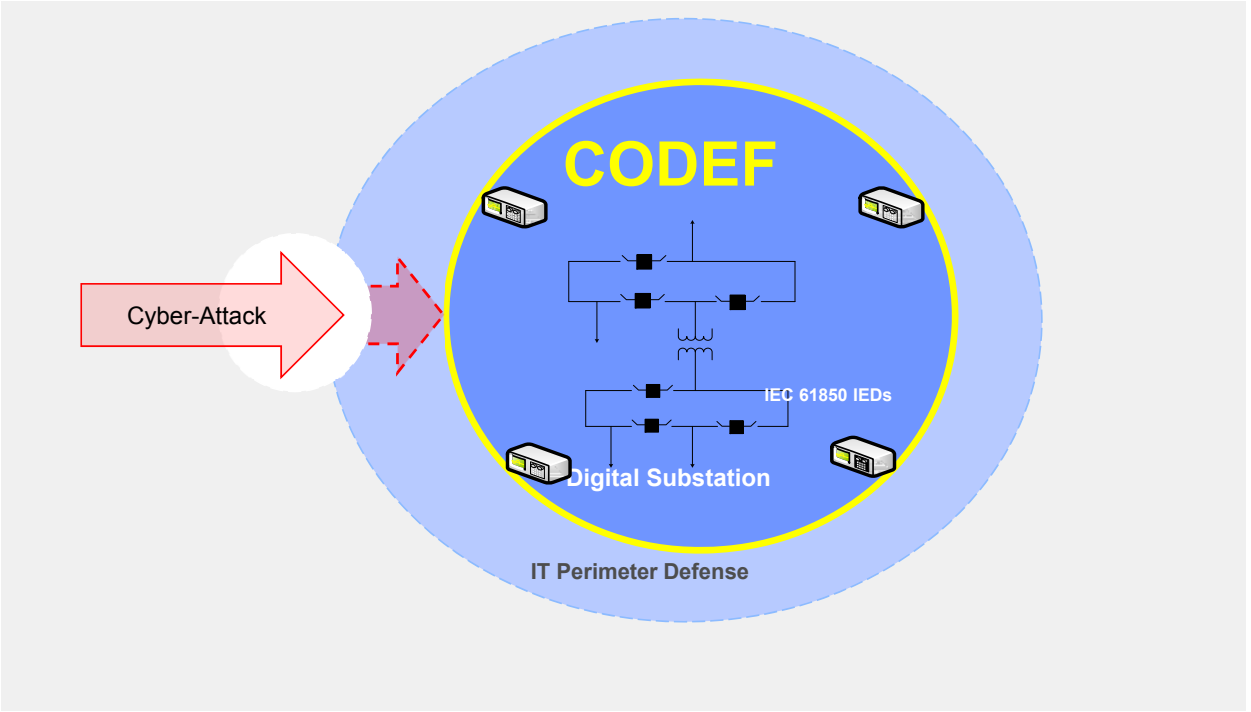
Partners: BPA, Ameren-Illinois, University of Illinois at Urbana-Champaign

CODEF Technical Approach

We use power system measurements to detect and block cyber attacks

Security Features

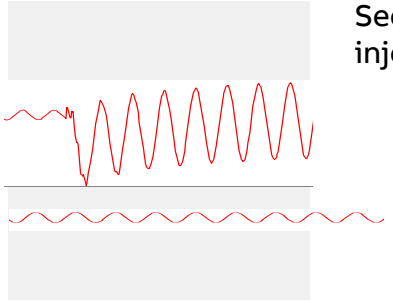
- Distributed intelligence between substation intelligent electronic devices (IEDs)
- Collaborative mechanism for detecting cyber attacks
- Domain based cyber security layer for electrical substations and intelligent electronic devices (IEDs)
- Additional cyber-layer for added security



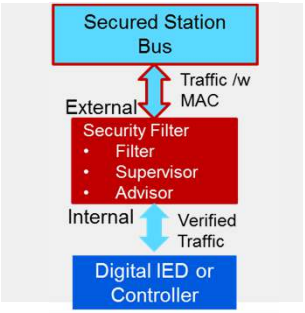
CODEF Cyber Security Solutions

Directed against attacks with greater impacts to substation and power systems

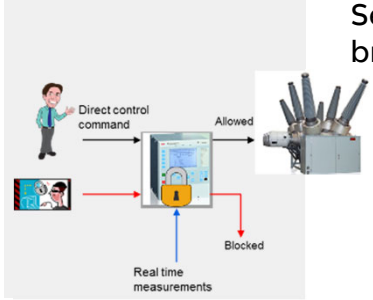
Security Solutions



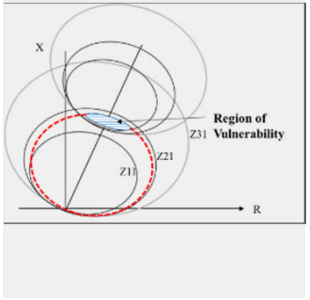
Security against malicious measurement injection



Security against attack on binary signals



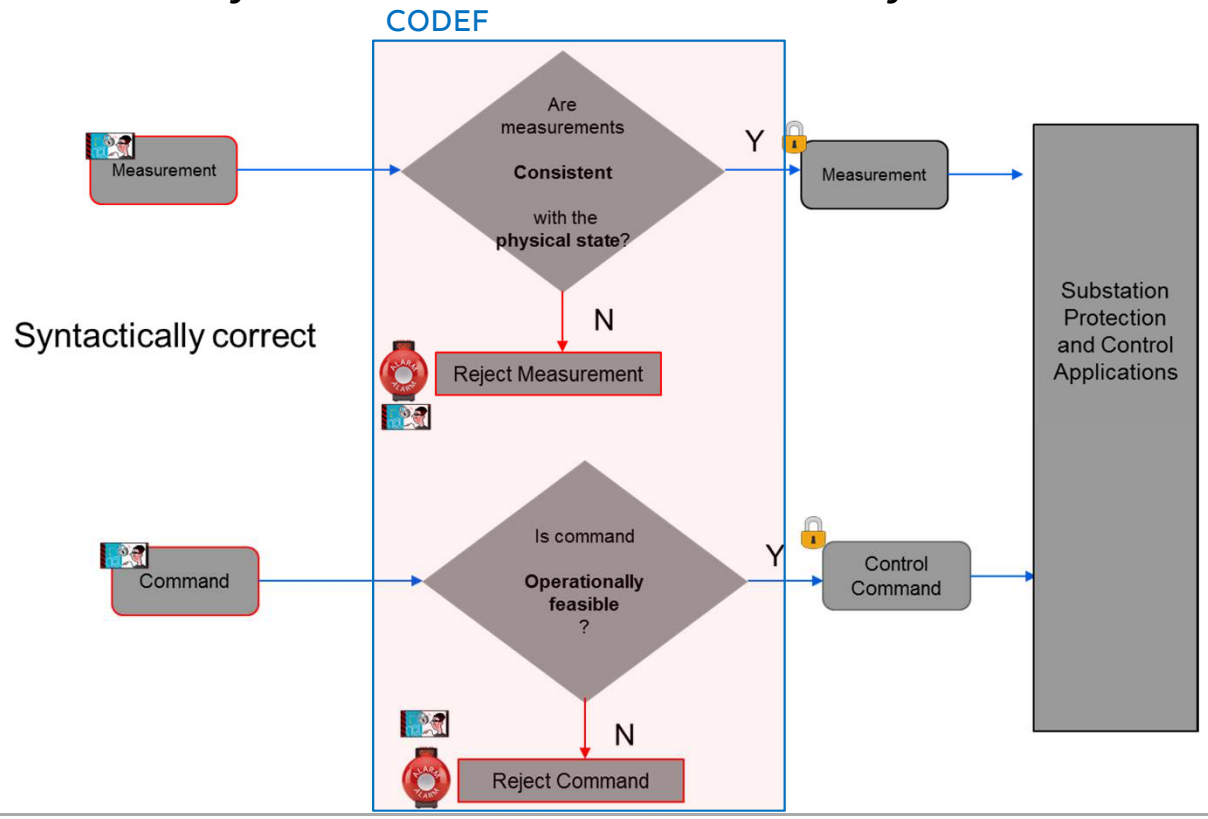
Security against direct control of circuit breakers



Security against attacks on device configurations

Technical Approach in more detail

Checking consistency between commands and the system state



CODEF Project Key Result

Demonstrable functions implemented in IEC61850 digital substation simulator with ABB hardware and software

Application Domain

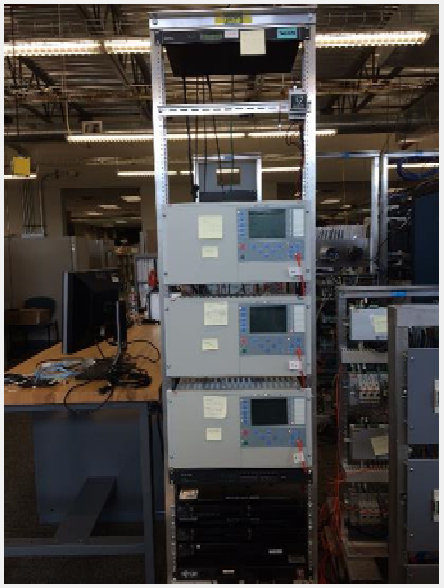
- Applications focused on cyber security of electrical substations
- Transmission and Distribution substations

Utility Demonstration Platforms

Functions were tested in near field and field conditions

Demonstration Platforms

- BPA
  - Transmission level cyber security
- Ameren-Illinois
  - Distribution level cyber security
- Test results suggest the feasibility of and readiness of CODEF functions to perform in field environment



BPA CODEF DEMONSTRATION MAY 12, 2016

AMEREN CODEF DEMONSTRATION held on MARCH 30, 2016

Cyber Attack Resilient HVDC System

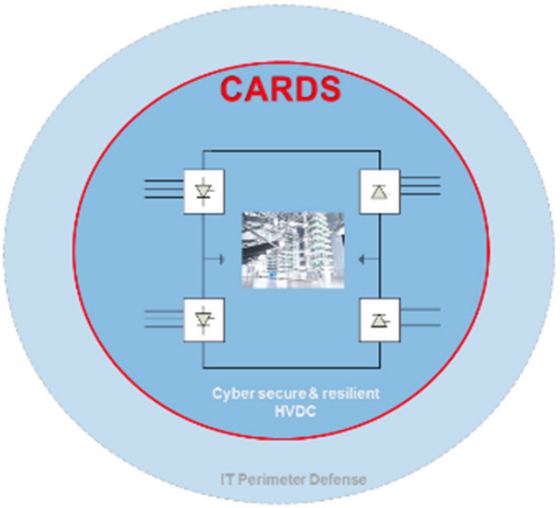
Defense-in-depth for High Voltage Direct Current Systems

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– 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.



Performer:	**ABB Inc.**
Partners:	**Bonneville Power Administration, Argonne National Laboratory, University of Illinois at Urbana Champaign, University of Idaho**

References

For further reading

1. US Department of Energy, Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF), available at https://www.energy.gov/sites/prod/files/2015/12/f27/CODEF%20fact%20sheet%20June%202015.pdf
2. US Department of Energy, Cyber Attack Resilient High Voltage Direct Current (HVDC) System, available at https://www.energy.gov/sites/prod/files/2017/06/f34/ABB_HVDC_FactSheet.pdf
3. Aaron K. Martin, Reynaldo Nuqui, Junho Hong, Anil Kondabathini, Warren Reese, Dmitry Ishchenko, A Collaborative Defense System of Protection Devices Against Cyber Attacks, Western Protective Relay Conference, Spokane, WA, October 18-20, 2016
4. Reynaldo Nuqui ; Junho Hong ; Anil Kondabathini ; Dmitry Ishchenko ; David Coats, A Collaborative Defense for Securing Protective Relay Settings in Electrical Cyber Physical Systems, 2018 Resilience Week (RWS), 2018, pages: 49 – 54
5. Dmitry Ishchenko ; Reynaldo Nuqui, Secure Communication of Intelligent Electronic Devices in Digital Substations, 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Year: 2018
6. R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, and D. Ishchenko Collaborative Defense Against Data Injection Attack in IEC61850 Based Smart Substations, IEEE PES General Meeting, 2016
7. T. Rousan, R. Hilburn, D. Borries, M. Backes, C. Drew, R. Macwan, P. Panumpabi, A. Valdes, Collaborative Defense in IEC 61850 Substation Environments (CODEF): From Research Lab to Utility Field Demonstration Experience, PACWorld Americas Conference, 2016

Q&A and contact information

If you have questions, please contact me further

Speakers

Reynaldo Nuqui

- ABB US Corporate Research Center
- +1-919-807-5039
- reynaldo.nuqui@us.abb.com