Enrico Ragaini - selected material from: Dmitry Ishchenko/Reynaldo Nuqui/Steve Kunsman

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

Cyber Security of the Grid

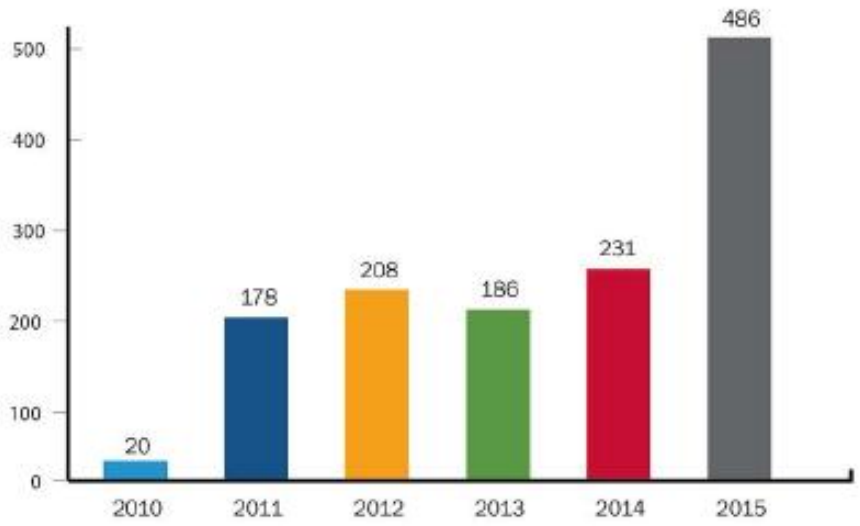
Cyber Security
A major concern

- The cost of cyber crime for the global economy has been estimated at **$445 billion** annually
- “Unknown actors successfully compromised the product supply chains of at ***least three [industrial control system] vendors*** so that customers downloaded malicious software designed to facilitate exploitation directly from the vendors’ websites along with legitimate software updates.”
  - Simplicity, WinCC, and WebAccess.
- US industrial control systems attacked 295 times in 12 months

ICS- CERT 2015 Report

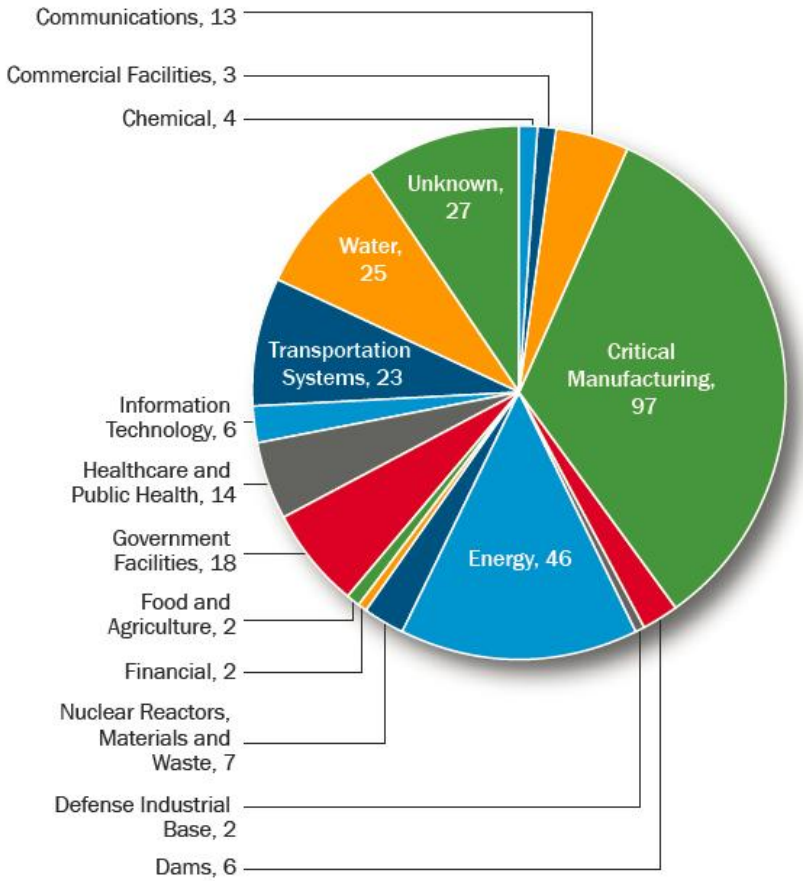
295 cyber attacks on ICS reported by asset owners and industry

Reported Vulnerabilities



Source: National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team Year in Review, 2015

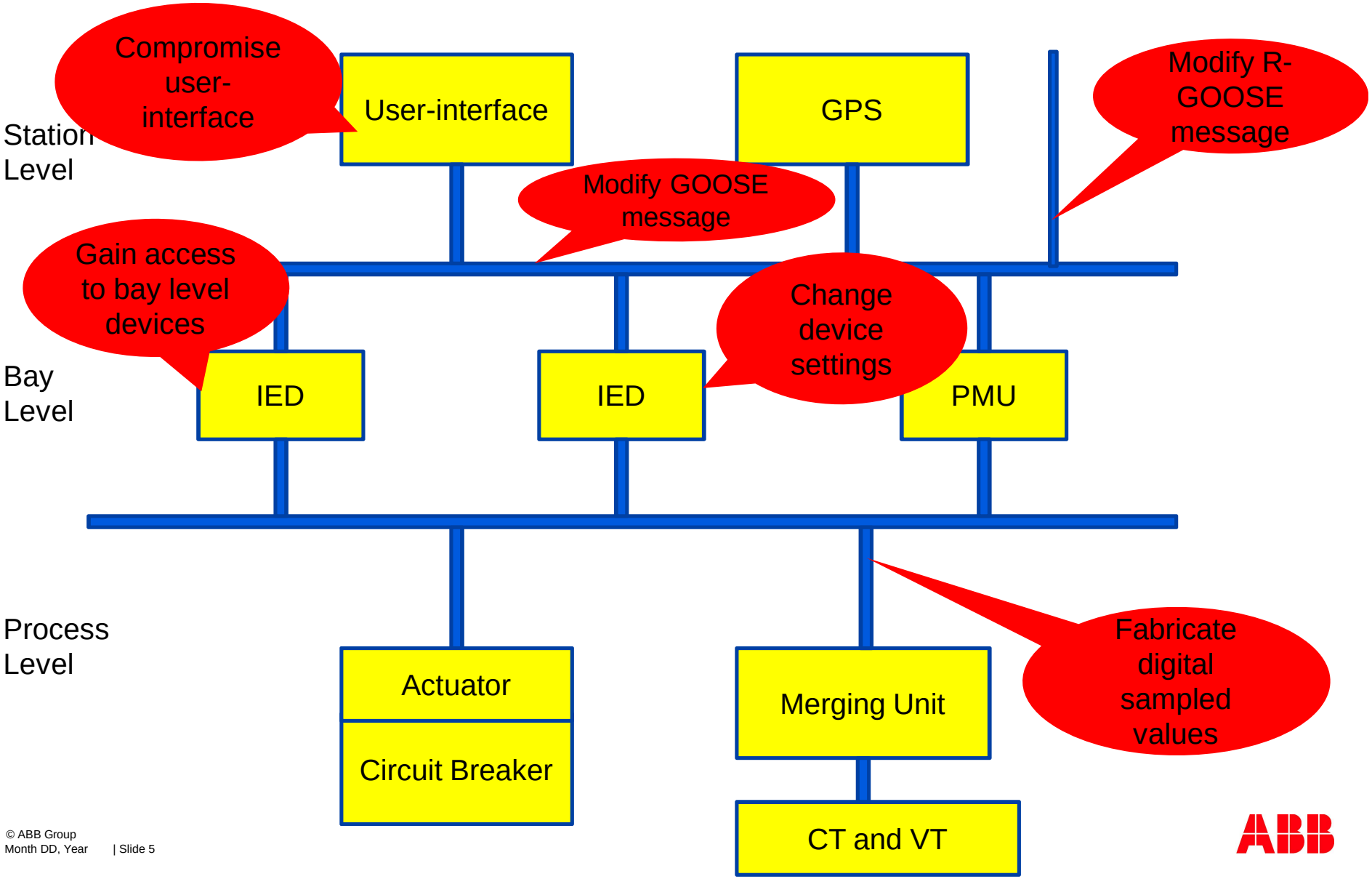
Incident Response Metrics



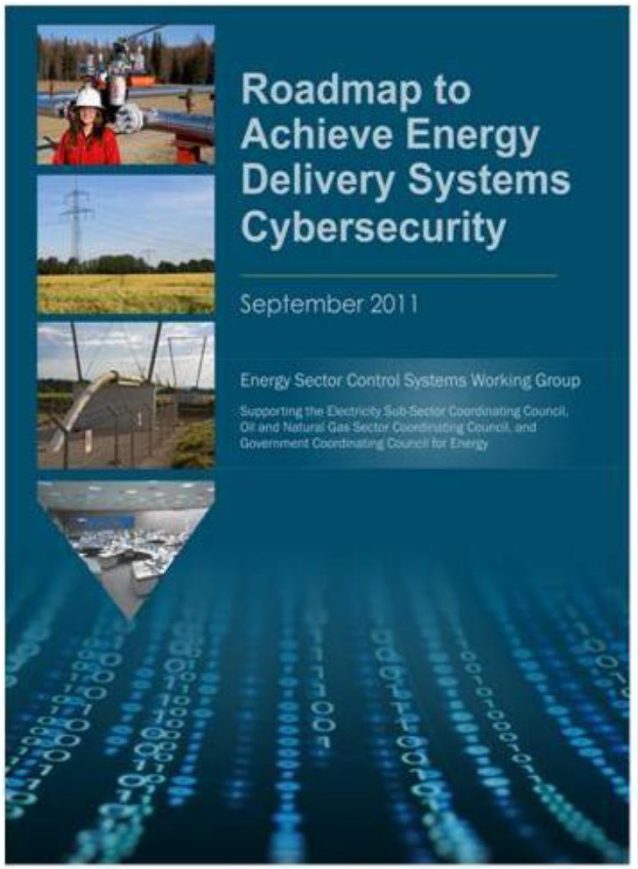
Substations are vulnerable
Loss of a substation could have adverse impact

- Control centers rely on substations and communications to make decisions
- Substations are a critical infrastructure in the power grid (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

Potential Threats in a Substation Network



US Energy Sector's Roadmap
Achieve Energy Delivery Systems Cybersecurity by 2020



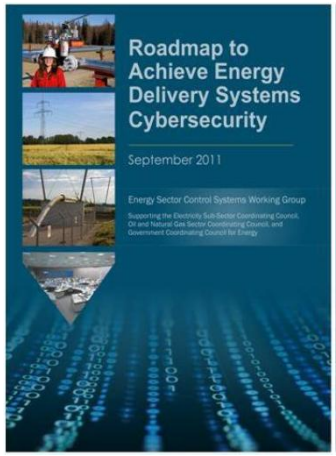
- Roadmap Vision
  - By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
  - For more information go to: www.controlsystemsroadmap.net

DHS

DOE CEDS

Cyber Security for Energy Delivery Systems

DOE Roadmap Milestones Addressed by CODEF
Major contributions on Milestone 3.3



Milestone	Description	Roadmap Strategy	
2.3	Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyberphysical domains commercially available	2	Assess and Monitor Risk
3.3	Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	3	Develop and Implement New Protective Measures to Reduce Risk
4.4	Real time forensics capabilities commercially available	4	Manage Incidents
4.7	Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	4	Manage Incidents

Collaborative **Def**ense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks

§ Objective

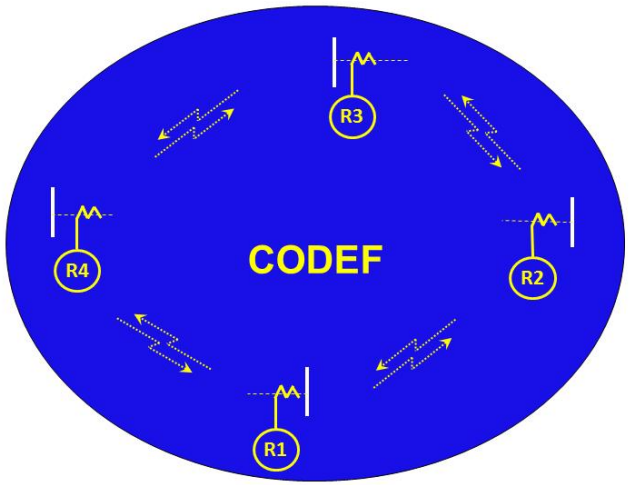
- To advance the state of the art for cyber defense methods for transmission and distribution grid protection and control devices by developing and demonstrating a distributed security domain layer that enables transmission and protection devices to collaboratively defend against cyber attacks.

§ 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

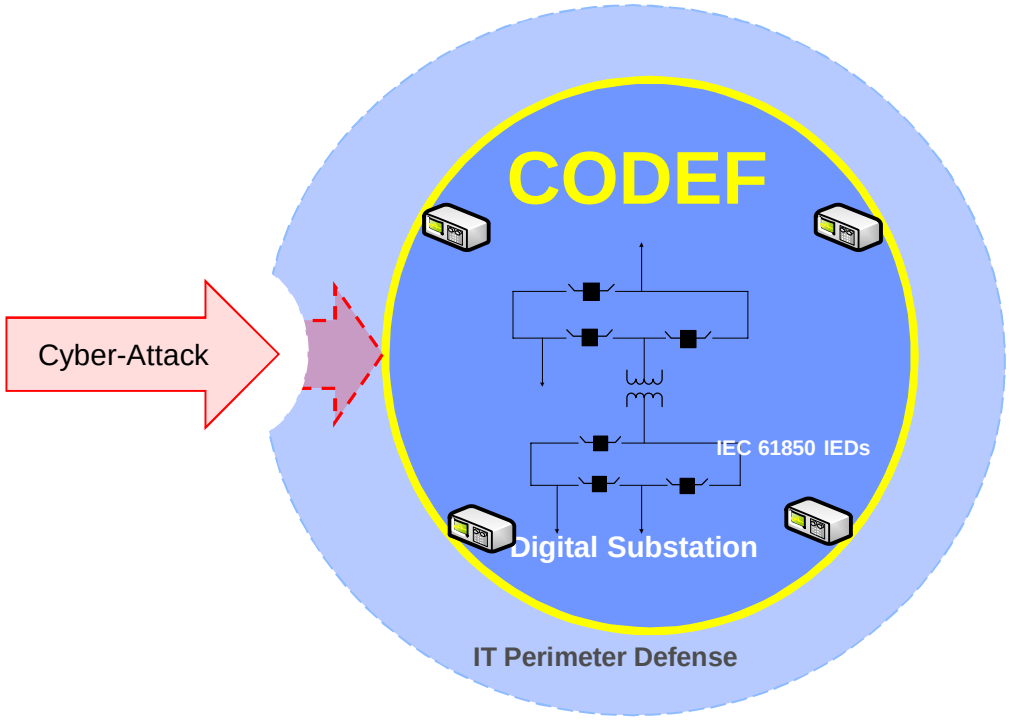
§ Capability to the energy sector:

- 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 Security Features
Distributed, collaborative, cyber and physics-based



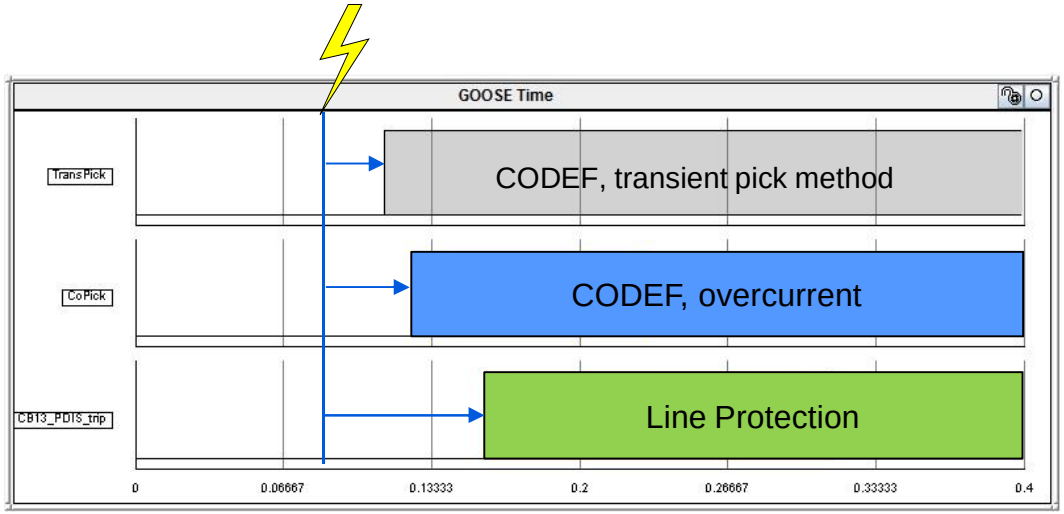
- Distributed intelligence between substation intelligent electronic devices (IEDs)
- Collaborative mechanism for detecting cyber attacks
- *Domain* based cyber security layer for electrical substations and intelligent electronic devices (IEDs)
- Additional cyber-layer for enhanced security

CODEF Project Key Result

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

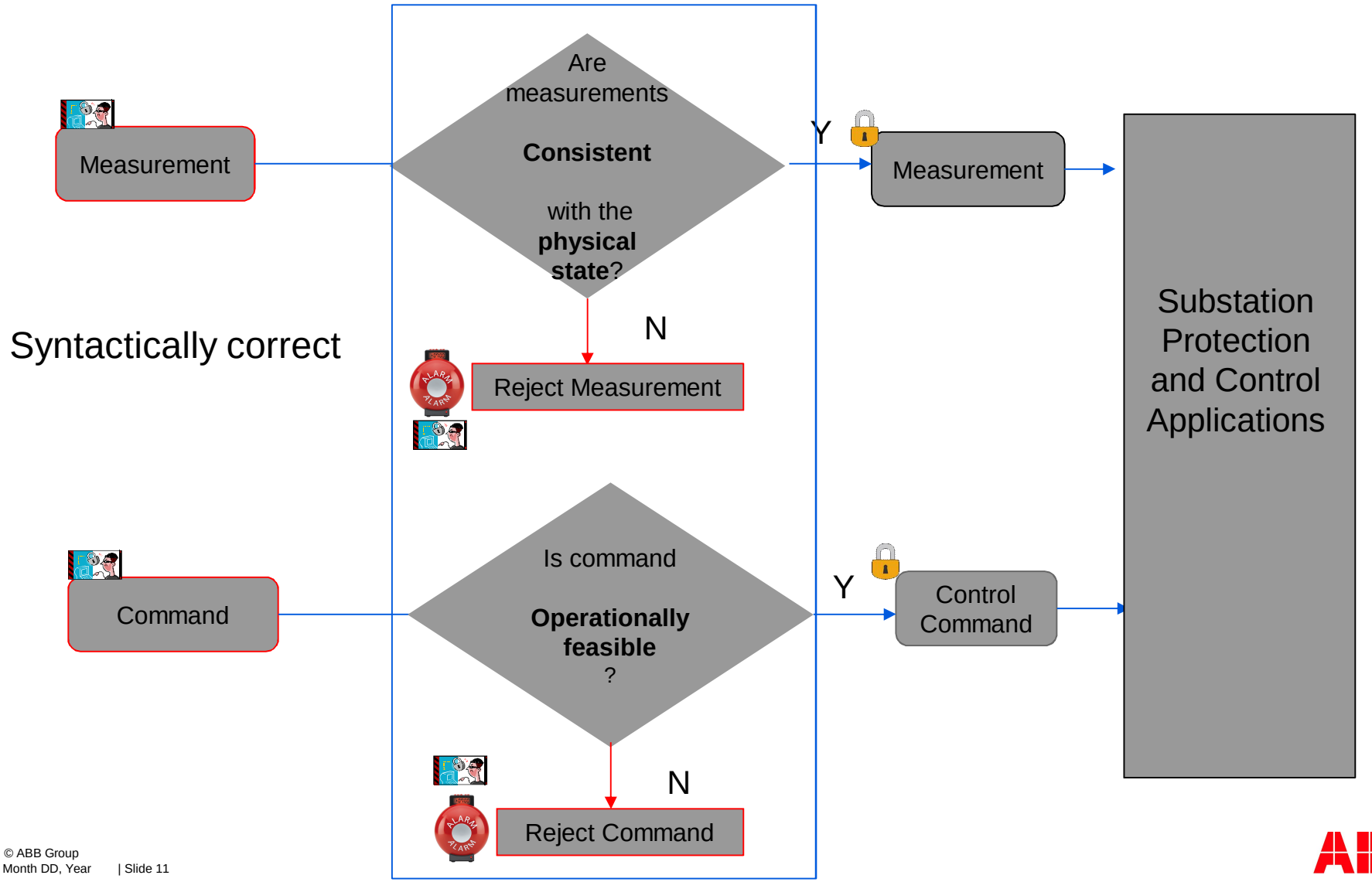
Applications focused on cyber security of electrical substations

- Technical Challenge
  - Speed – cyber security solutions must not delay protection actions



Fault confirmation faster than existing object protection

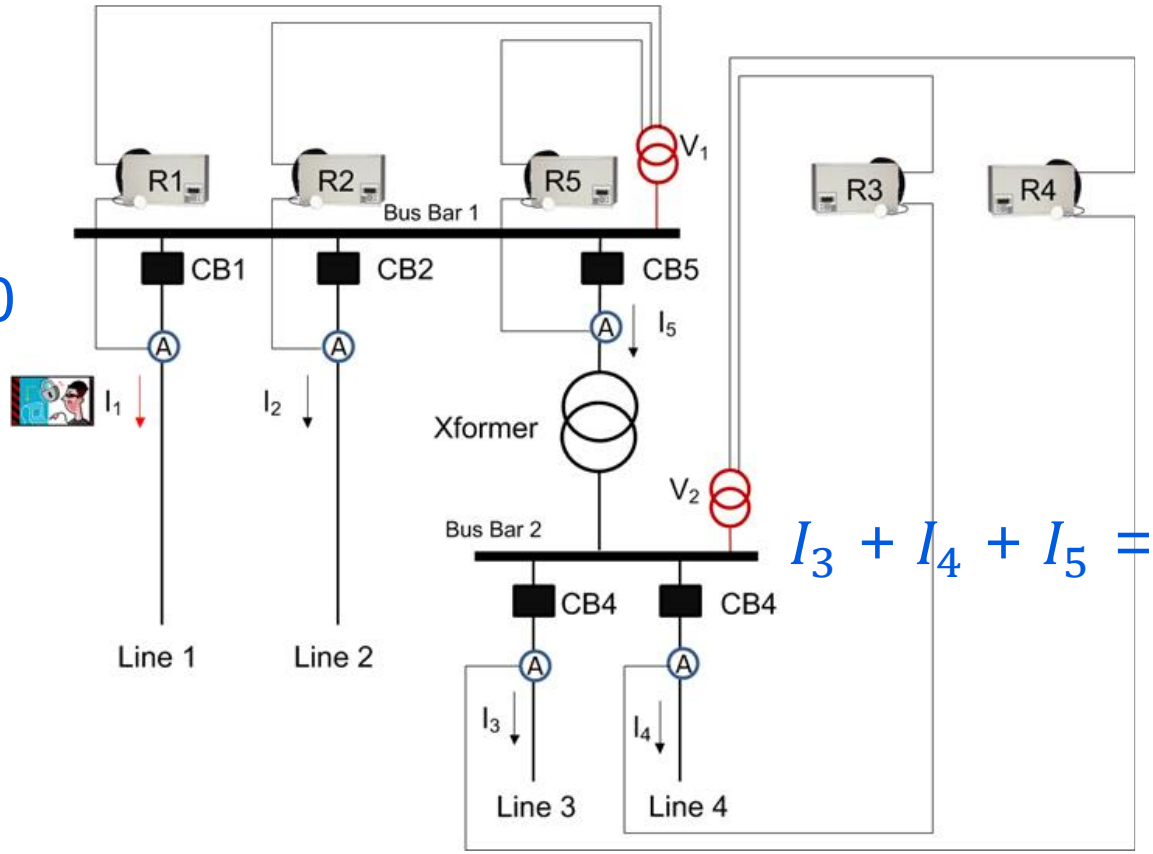
Technical Approach
Use physics to block malicious cyber attacks



Kirchhoff's Laws must be satisfied

Violation could constitute a cyber attack on the measurements

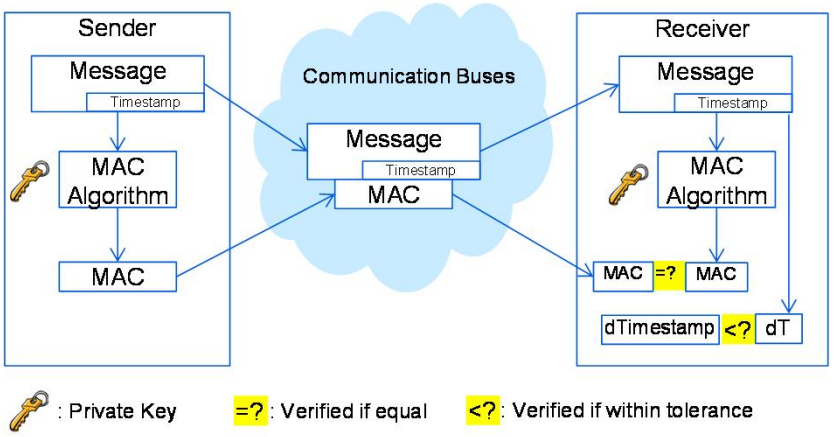
$$I_1 + I_2 + I_5 = 0$$

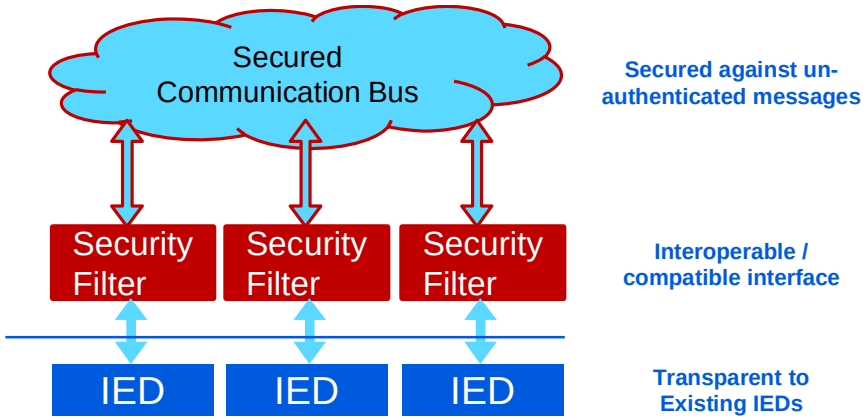


$$I_3 + I_4 + I_5 = 0$$

Technical Approach
Cyber Layer – Security Filter

- Bump-in-a-wire device
- Designed according to draft IEC 62351-6 Ed. 2
- Galois Message Authentication Code (GMAC)128 bit
- Key distribution handled according to draft IEC 62351-9 Ed. 2 (GDOI)
- Modes of operation:
  - Filtering – block all compromised packets
  - Supervisory – thresholds to block packets
  - Advisory mode – alarm only





Cyber Physical Test Beds & Demonstration Platforms

Hardware in the loop testing is key to evaluating speed of solutions

Development and testing platforms

ABB Raleigh

University of Illinois

Demonstration Platforms

BPA

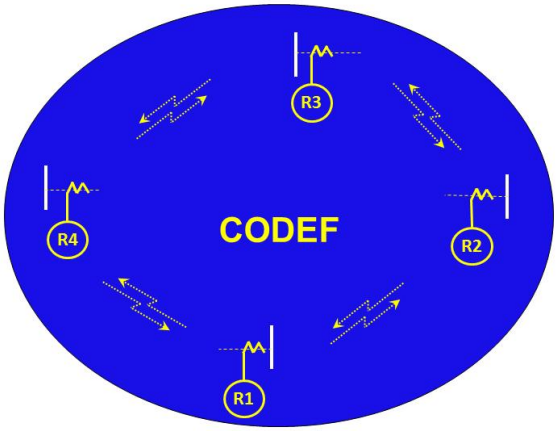
Ameren-Illinois

BPA CODEF DEMONSTRATION MAY 12, 2016

AMEREN CODEF DEMONSTRATION held on MARCH 30, 2016

CODEF
Conclusions

- Class of power system-aware cyber security functions that are distributed, collaborative, and domain-based.
- Designed to reinforce existing IT based solutions and also to provide another security layer in case of breach of IT security layer
- Detects and blocks malicious attempts to control circuit breakers and malicious device configuration settings
- CODEF functions were validated in an IEC 61850 digital substation simulator and in the utility environment



Power and productivity
for a better world™