Reynaldo Nuqui

ABB

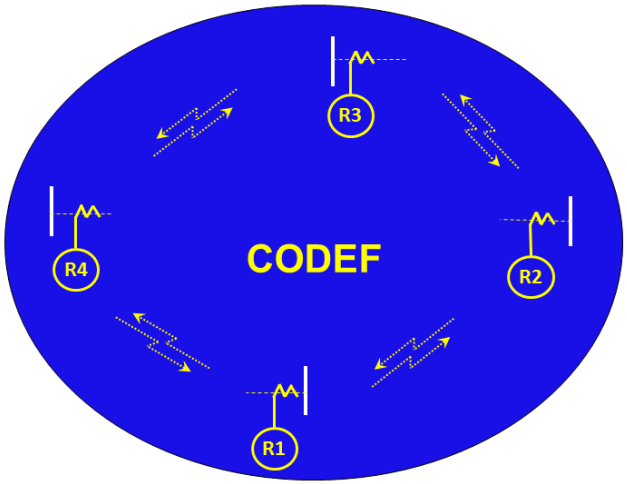
Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: Collaborative Defense 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
    - Project start: January 2014
    - Distributed Security Enhancement Layer Design
    - Distributed Security Enhancement Layer Implementation
    - Security Demonstrator
  - 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



- **Total Value of Award (MUSD): 3.70**
- **% Funds expended to date:** 9.3%
- **Performer:** ABB
- **Partners:** University of Illinois, Negotiations with a utility partner are underway

Advancing the State of the Art (SOA)

- **Current "state of the art"**
  - "Security through obscurity"
  - Security against cyber attacks on protection and control devices is performed at the IT layer.
- **Advancing the cybersecurity of energy delivery systems**
  - What is new?
    - Real time cyber security that is aware of power system operations
    - Novel technical approach that will be designed, tested and demonstrated in an IEC 61850 based substation; leveraging vendor, university and utility knowledge and competences.

Advancing the State of the Art (SOA)

- **Advancing the state of the art**
  - The project will develop a technology that adds a domain based security layer against cyber attacks. Its domain nature utilizes the physics of the protected system to block cyber attacks against itself.
- **Benefit to the end user**
  - The approach will mitigate the incidence and direct impact of successful cyber attacks on power grid infrastructure, resulting in a power grid that is hardened against cyber attacks.

Challenges to Success

Challenge	Severity	Impact	Mitigation Plan
Algorithm implementation	High	Identified IED platform is difficult to adapt for project goals	Leading PI has frequent communication with ABB IED business partner (BU); plan to bring BU resources on-board if the issue is foreseen
Demonstration site	Low	Demo in utility delayed	Negotiations with a utility partner
IED computational platform	High	IED could not host the CODEF algorithms	Code the algorithms in an add-on computational platform

- Challenges are well identified and mitigation steps are in place

Progress to Date

- **Major Accomplishments**
  - Milestone 1: Completed
  - Threat Models Defined and Tested.
    - Attacks on voltage and current sampled values, GOOSE messages, and relay settings were modeled. A subset of these threats were tested and verified in hardware in the loop demonstrator.
  - Milestone 2: Completed
  - Distributed Security Enhancement Layer Designed.
    - Power system domain based security algorithms were designed and ready to be coded within the IEC 61850 synthesizer.

Next Steps for this Project

TASKS DESCRIPTION

1. IMPLEMENT THE SECURITY ENHANCEMENT LAYER

-Implement the security enhancement layer for GOOSE and (substation level) IEC 61850 Process Bus Data

2. DEVELOP AND IMPLEMENT IED ALGORITHMS INTO COLLABORATIVE DEFENSE SECURITY LAYER

-Implement inter device cross checking for secure configuration using domain principles and semantics and detecting malicious direct control commands

3. POWER SYSTEM DOMAIN BASED IED SECURITY ALGORITHM VALIDATION

-Implement IEC 61850 simulator embodying security enhancement layer. Validate performance of security enhancement layer

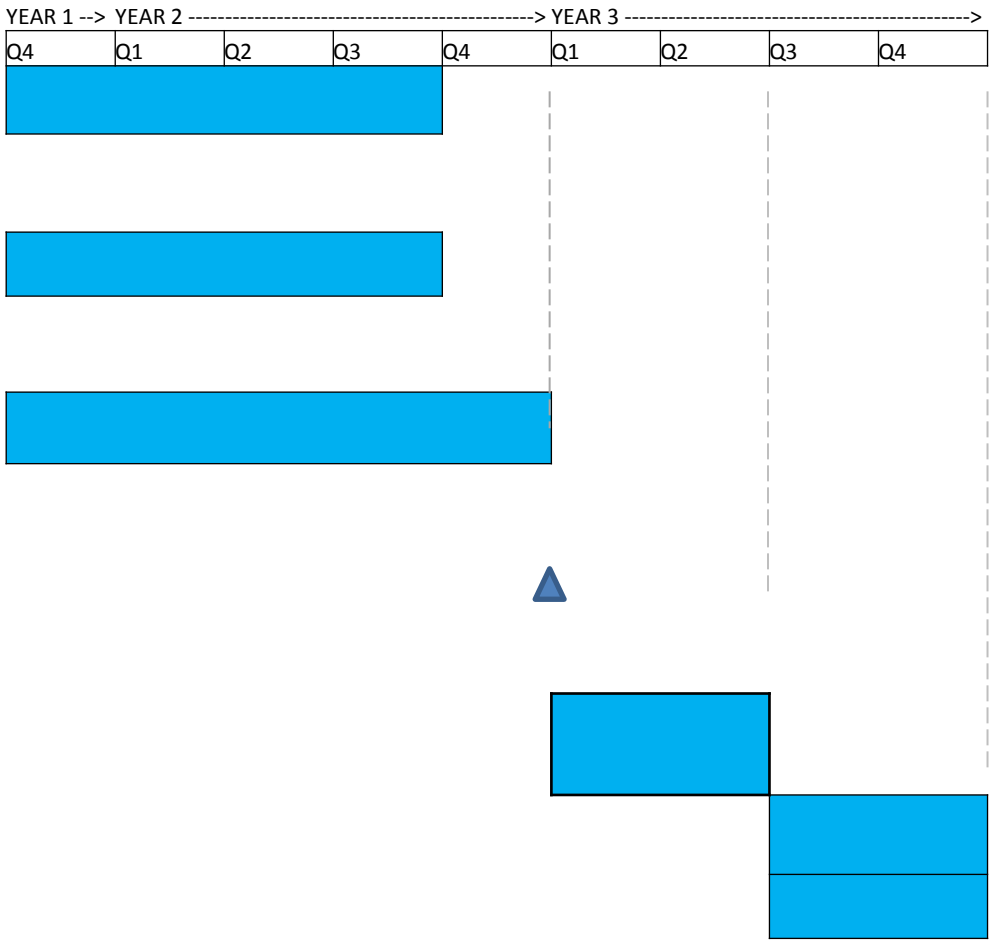
GO/NO GO Decision

4. DEMONSTRATION

-Set up hardware demonstration in utility environment, demonstrate and validate timing claims of security enhancement layer

5. INTEGRATE COLLABORATIVE DEFENSE ALGORITHMS IN ABB PRODUCT LINE

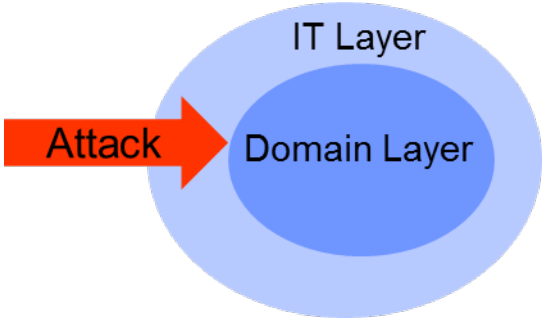
6. PROVIDE RECOMMENDATIONS TO IEC AND OTHER STANDARDS



Collaboration/Technology Transfer

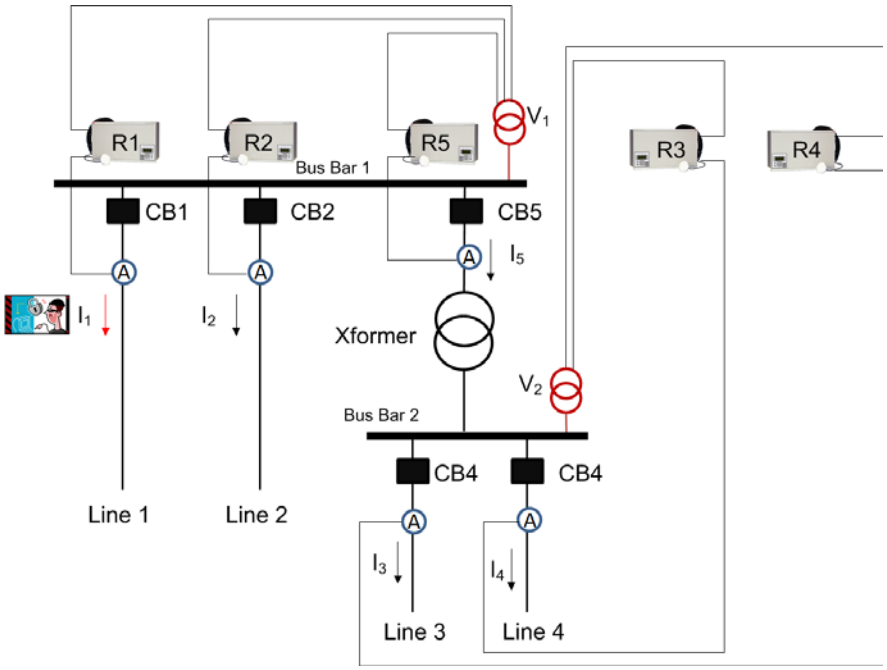
- **Targeted end user for the technology or knowledge: Asset Owner**
- **Plans to gain industry acceptance**
  - Demonstration
    - Demonstrate the system in a utility test bed environment and validate the timing and security aspects of the collaborative defense to include the following:
  - Knowledge Transfer
    - Integrate the developed/validated IED algorithms on collaborative defense into the ABB P&C product lines
    - Provide recommendations to IEC and other standards organizations

Domain Based Security Layer
In a nutshell



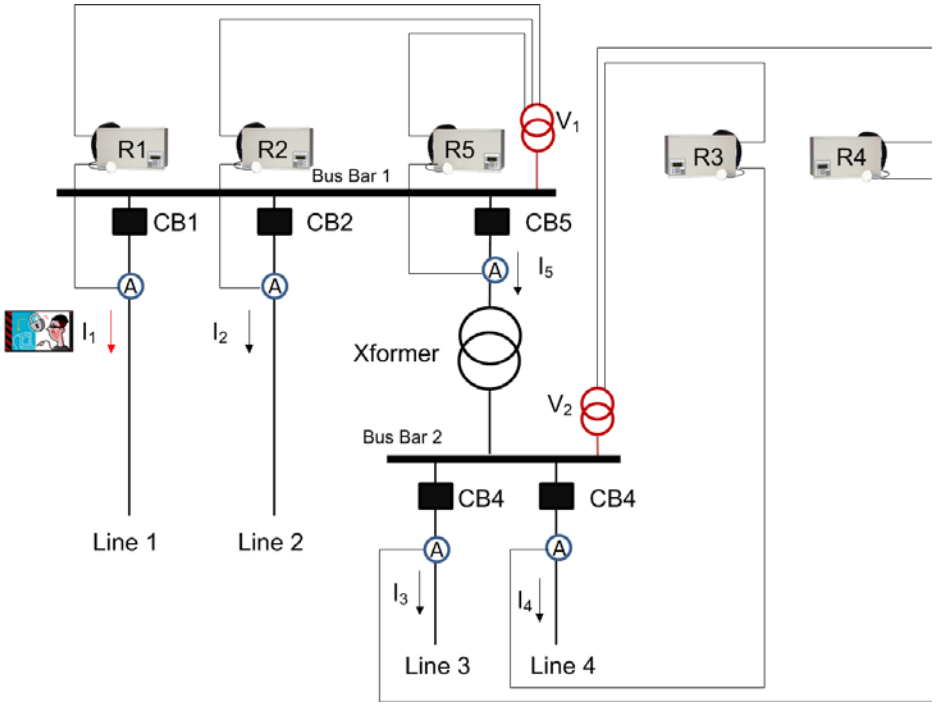
- **Using power system domain principles to detect and block a cyber attack**
  - An attacker has breached the IT security layer
  - An attacker injects spurious data into the protection network
    - Corrupts the voltage and current sampled values
    - An authorized employee deploys wrong settings to protection device(s)
    - Executing malicious control commands (through GOOSE or direct Circuit Breaker control)
- **IEDs collaborate in confirming the validity of changes based on their own measurements**
- **IEDs vote as a group to effect a change in the IED configuration**

Threat Example



- **An attacker gains access to the utility substation network**
- **The attacker injects false current signals to relay R1**
- **Relay R1 will calculate a fault current and sends trip signal to CB1**
- **CB1 trips resulting in a successful attack**

Distributed Domain Based Security Layer Example



$$I_1 + I_2 + I_5 = 0$$

$$I_3 + I_4 + I_5 = 0$$

- **Check if Kirchhoff's Current Law is violated on relays R1, R2, and R3**
- **Check if voltage signal at bus bar indicates a fault condition**
- **Relays collaborate and arrive at a consensus**
- **Relays send a blocking signal to R1 if an attack is discovered**

Towards a Widely-Accepted Cybersecurity Solution for Energy Delivery Systems

- **Real time cyber security that is aware of power system operations**
- **Physics of electrical systems is a reliable gauge for detecting cyber attacks**
- **The solution is easily implementable in a digital substation and modern day IEDs**