CIGRE GRID OF THE FUTURE, SENSOR DATA AND FAULT LOCATION ANALYTICS SESSION 2017.10.24

A Method for Detecting Abnormal Sensor Data Using Multi-terminal Differential Protection Functions

David Coats, Reynaldo Nuqui USCRC

Agenda

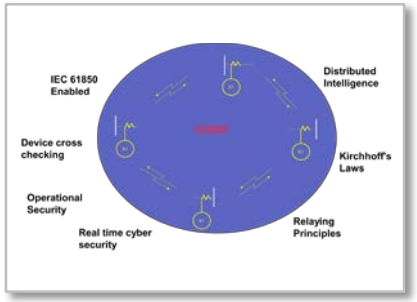
1. Collaborative Defense (CoDef) Project Overview
2. Threat Modeling
3. Multi-Terminal Protection
4. Abnormal Data Detection Method
5. Summary, Conclusions, and Future Projects

Domain Based Collaborative Defense (CoDef)

Collaborative and Distributed Cyber Defense Functions, DoE Funded Research

Objective

- To advance the state of the art in 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.

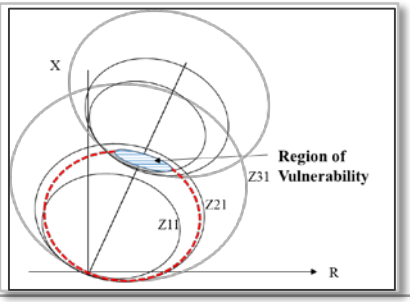


State-of-the-art

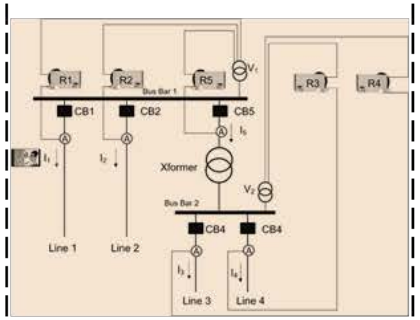
- "Cyber Security through obscurity"
- Security against cyber attacks on protection and control devices is performed at the IT layer.
- Cyber security is reactive and could not block malicious operation of substation switching devices

Innovation

- Inter-device level technology for smart detection of cyber attacks using power system domain knowledge, IEC 61850 and other standard security extensions
- Real time, cyber secure and OT error-proof protection and control solutions for power grids



Technology Objectives



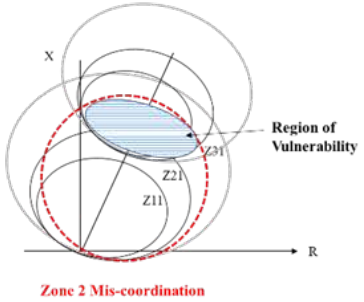


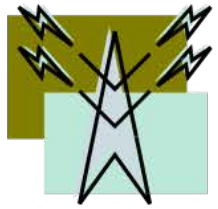
ABB and UI Demonstrators

Research and Design

Development and Validation

Bonneville Power Authority

Ameren Illinois



Utility Demonstration

Substation Automation, High Voltage Relays, Medium Voltage Relays, IEC 61850 Digital Substations, Service

Knowledge Transfer

Phase I | Phase II | Phase III | Phase IV

Cyber-Physical Security Functions

Cyber Attack Scenarios and Security Demonstrations

Attack	Goal of Attack	Cyber Security Function Demonstrated	Implementation Level
Malicious data injection	Malicious tripping of circuit breaker	1. Co-pick – collaborative pickup confirmation (possible w/ in Protective Relays)	Engineering Tools
		2. Trans-pick – transient pickup confirmation (new hardware)	New Development
		3. **Multi-pick – Multi-terminal differential confirmation (possible w/ in Protective Relays)**	Engineering Tools
Unauthorized control of circuit breaker	Malicious tripping of circuit breaker	4. Cyber secured direct control of breaker – M2M communications, simulation assisted	Simulation Assisted
Malicious change in protective relays settings	Mis-coordinate relays	5. Cyber secured IED configuration change – GOOSE confirmation (possible w/ in Relays)	Simulation Assisted, Comm.
GOOSE attack	Malicious tripping of circuit breaker	6. Cyber secured GOOSE – Authenticated GOOSE IEC62351 Implementation (new hardware)	New Development, Standards Based Communication

Example Application Time-Scale Overview

Timing Plot Comparison

- REL_PTRC:
  - Trip condition logic: actual trip command after actual fault
- REL_Dis:
  - Distance trip command from REL670
- CoPick or MultiPick
  - Confirm from pick-up logical node from 3 to 4 existing relays by GOOSE message, Fiber
  - Multi-terminal protection from 3 terminals proposed confirmation from GOOSE message, Fiber
- TransPick
  - Confirm from Transient conditions approximately quarter to half cycle protection (Commodity Hardware)

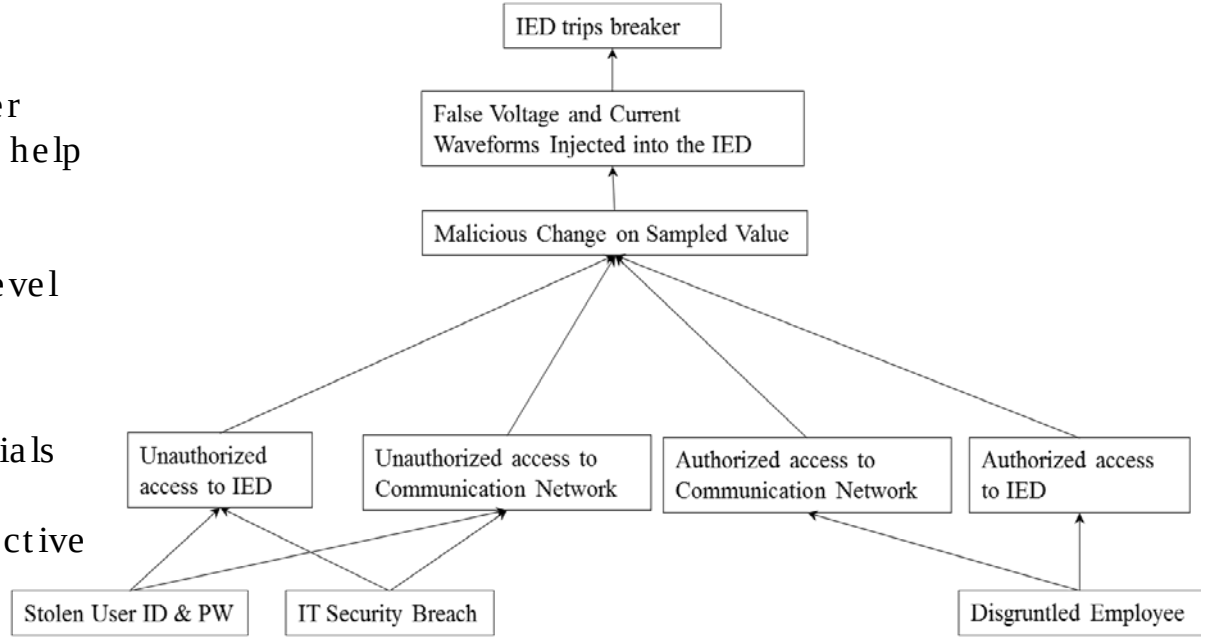
Threat Modeling

Specifications and Assumptions

- In a digital world, "obscurity" is growing increasingly hard to maintain
- Domain based, collaborative, and abnormal data detection cyber security applications are not the first layer of defense but could help
- There are two types of scenarios which form the basis of high level attack models:

Scenario 1: In this scenario, the attacker either steals the credentials (login/ password) and/ or there is a security breach in the IT infrastructure. This leads to unauthorized access to IEDs or Protective Relays and communication network.

Scenario 2: In this scenario, the attacker can be a disgruntled employee, who has the complete knowledge of the system and authorized access to IEDs and communication network.



A generic sample value attack model

Abnormal Data Sources

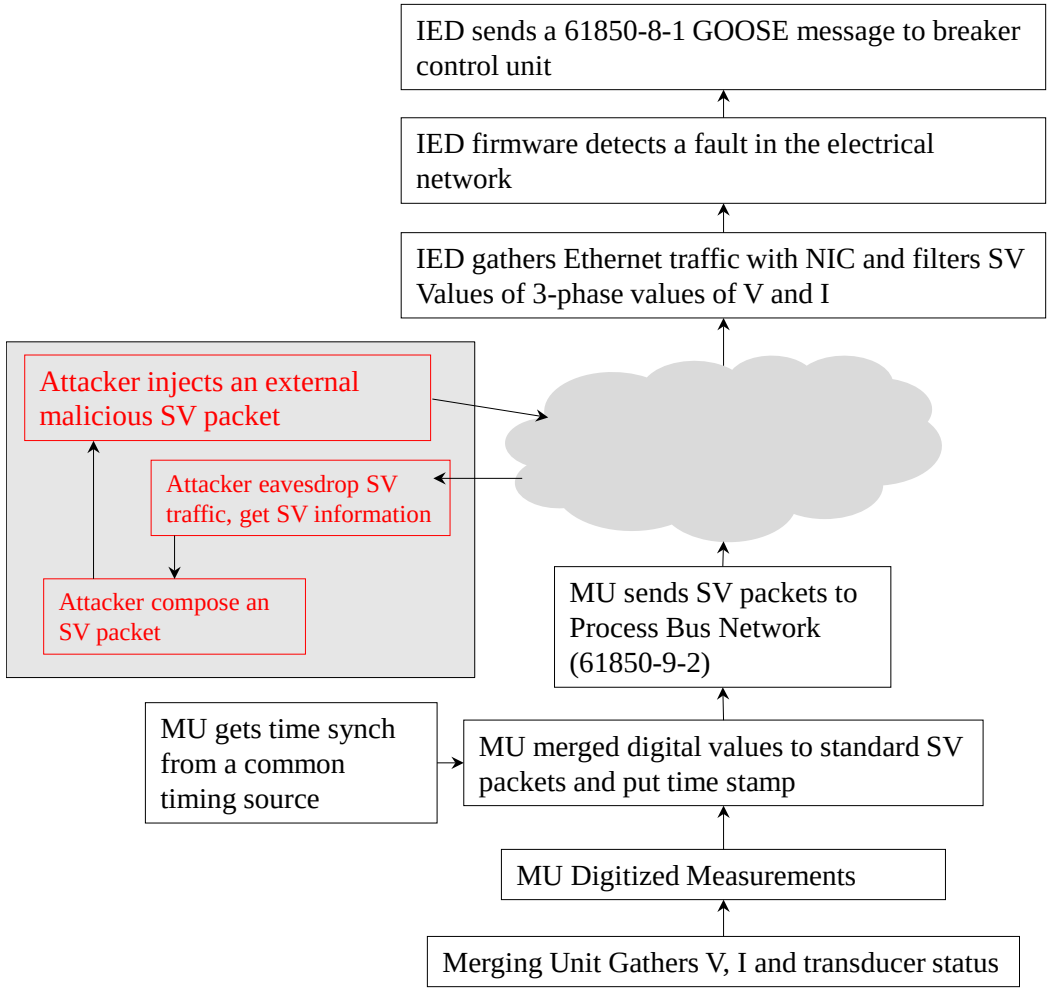
Sample Value Security

Driving Factors:

- Faster protection requires faster measurements
- Distribution and transmission automation push toward digital merging units for measurements
- Increased dependence on timing sources

High Level Threat Scenario

1. The merging unit (MU) gathers voltage, current and transducer status information and digitizes the measurements.
2. MU gets time sync from common time source and digitized measurement merged in sample value (SV) packets. The MU ensures that the number of packets follow IEC 61850-9-2, i.e. 80 samples/ cycle
3. Attacker continuously monitors the SV traffic, composes a malicious SV packets or copies a fault signature, and injects it into the traffic with the correct packet structure and standard format



Man in the Middle or Replay Attack Scenario

Classical Differential Protection

KCL Conditions

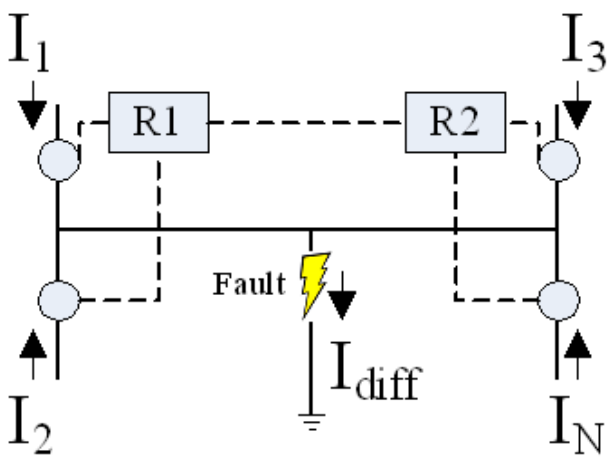
- Typical differential or multi-terminal protection may require dedicated communication paths
- Multiple master configurations: Master-slave, master-master
- Limits introduced in digital systems based on latency and throughput of GOOSE, MMS , etc

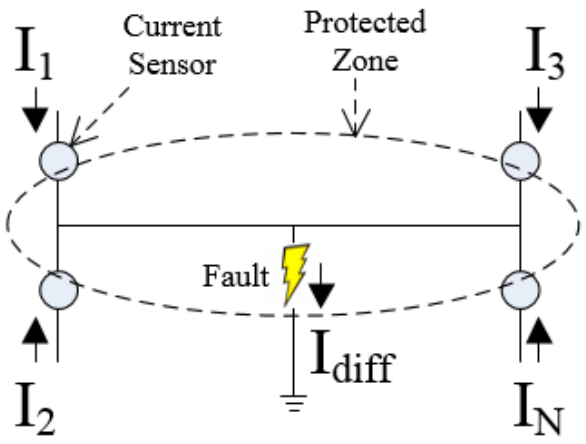
$$I_1 + I_2 + I_3 + \cdots I_N = 0$$

$$I_1 + I_2 + I_3 + \cdots I_N = I_{diff}$$

1. When the sum of all current is zero: No fault is detected in the Protected Zone.
2. When the sum of all current yields a current I_{diff}: A fault is detected in the Protected Zone, and the fault current is I_{diff}.

Current measurements are assumed to be accurate, with additional relay settings for a bias value based on differences in CT calibration

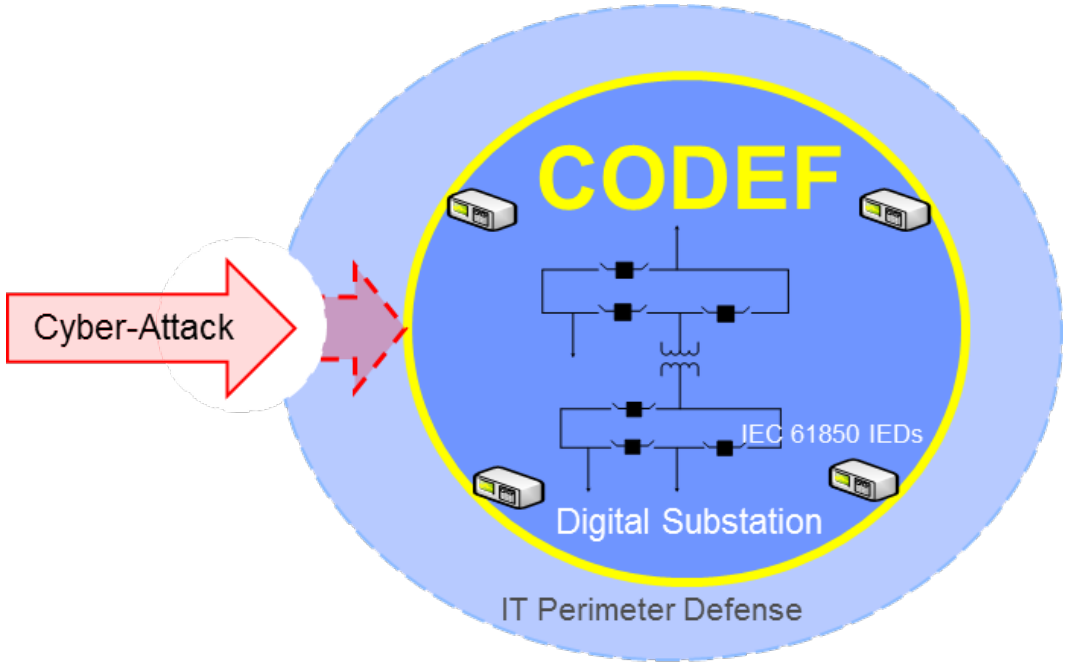




Multi Terminal Logic Goals

Collaborative and Distributed Cyber Defense Functions for Transmission and Distribution

1. Fast Operation
   - Fast acting protection methods chosen (overcurrent, differential)
   - Take advantage of digital merging units and high speed communication
2. Security
   - Multiple locations
   - Multiple sensor streams
   - Established physical principles (KCL)
   - Supplemental to IT and OT best practices
3. Readiness
   - Typical Markov Decision Logic utilized for protective relays
   - Interoperability provided with in communication standards
   - Minimal development required
   - Targets existing engineering and configuration tools
4. Compatibility
   - No dedicated hardware
   - Can use existing protection functions
   - Confirmation and collaboration functions available through IEC61850 logical nodes



Abnormal Data Detection Logic

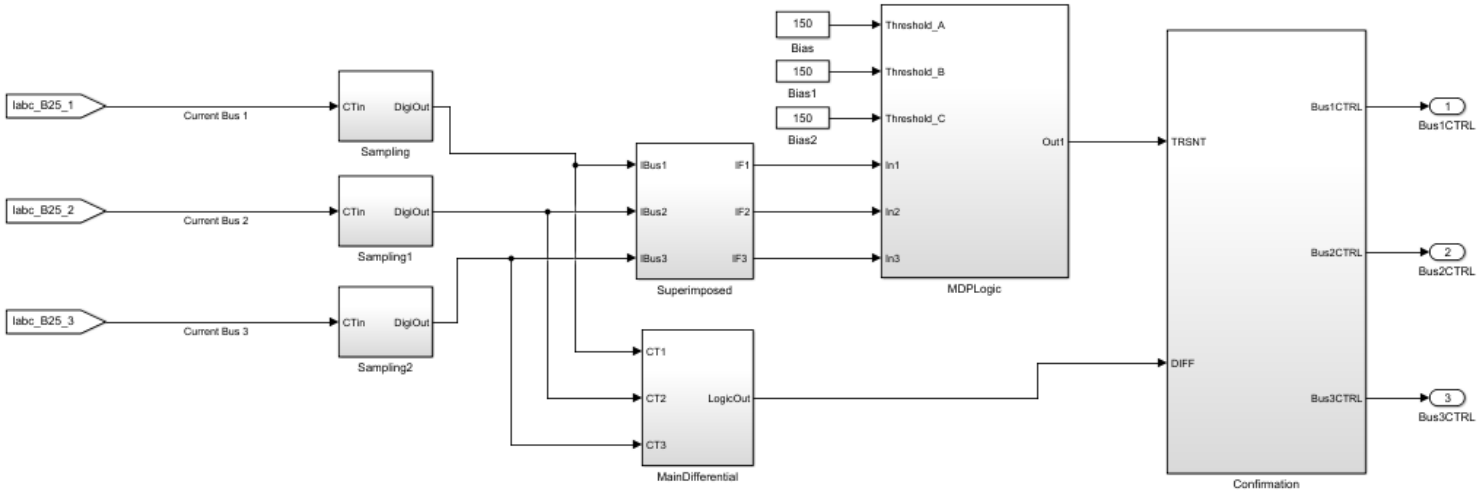
Collaborative and Distributed Cyber Defense Functions for Transmission and Distribution

1. Continuously calculate the superimposed component currents (I_{1F} through I_{NF}) from the current measurements (I_1 through I_N)

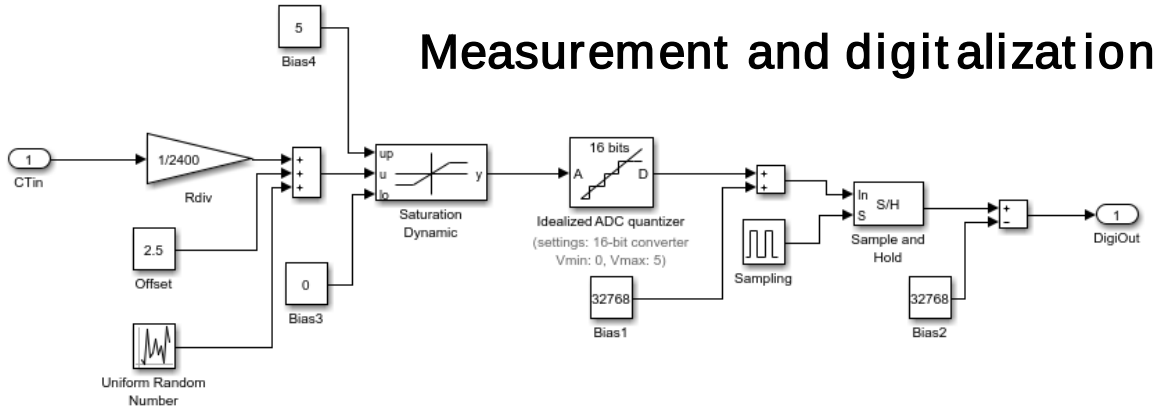
2. Calculate the differential current, I_{diff}

3. If I_{diff} and a majority of the N superimposed component currents (I_{1F} through I_{NF}) are greater than predefined thresholds, confirm internal fault

4. If I_{diff} and only one of the N superimposed component currents, for example only I1F, are greater than predefined thresholds, a sensor failure was detected and the sensor that measures I_1 was the failed sensor.



Measurement and digitalization of CT inputs



Simulation Setup and Test Cases

Simulated Measurement System:

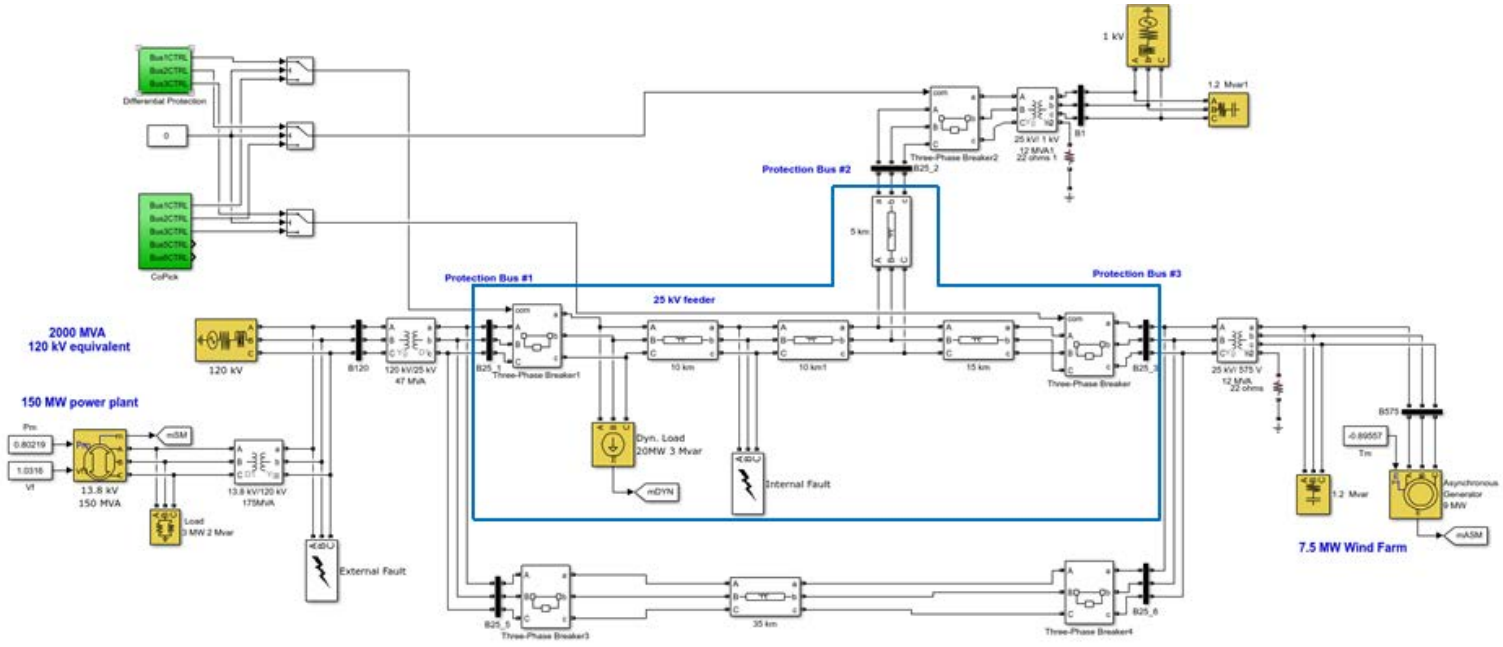
1. Ideal quantization with randomized noise
2. Modelled current transformer saturation limits and gain settings
3. Time synchronization

Simulated Protection Systems:

1. Simplified differential multi-terminal detection
2. Logical Markov decision process verifying differential protection with the superimposed current

Test Conditions:

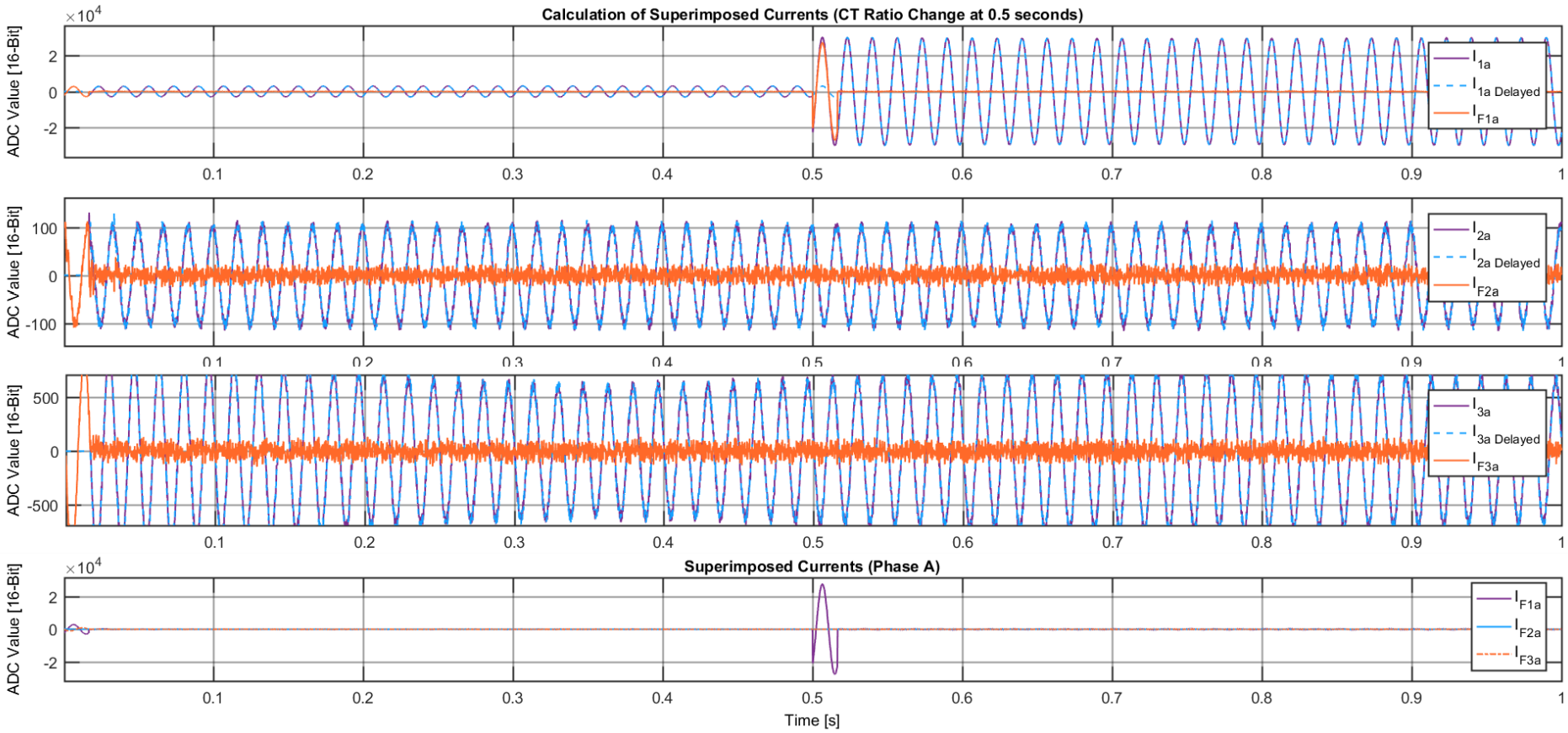
1. Internal fault within the protection zone
2. External fault close to the grid connection
3. Measurement fault caused by a sudden, unauthorized change in CT ratio or falsified current measurement



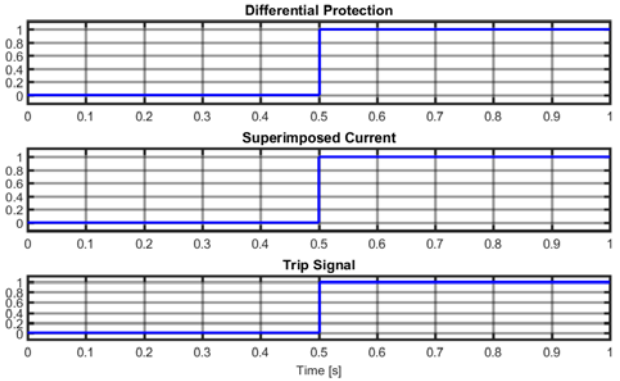
Example tapped line with multi-terminal protection and DER integration

Multi-terminal Collaborative Defense Confirmation

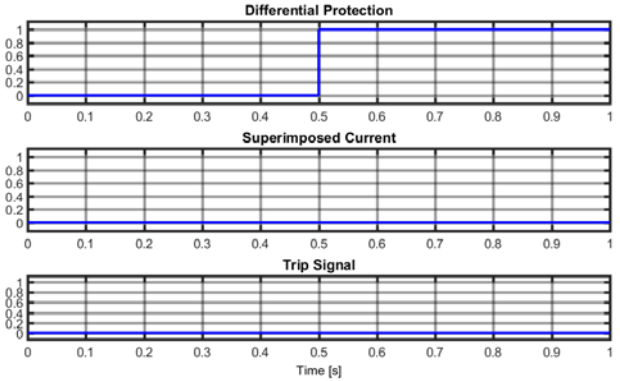
Results - Fault caused by unauthorized change in CT Ratio



Confirmed Trip



Unconfirmed Trip



Summary and Conclusions

A multi-terminal differential protection scheme allows for detection and identification of sensor anomalies in measurement devices

Enabled by IEC61850, logical variables verify that each terminal in the protection zone sees a given internal fault and provide normal operation of differential protection

The method is fast, interoperable with existing systems/ protection, and provides an additional cyber-physical defence layer

As more digital merging unit devices emerge, they support new communication and confirmation methods that could operate within protection timing requirements

Efforts in Collaborative Defence at ABB have been continued in two separate programs targeting Microgrids and HVDC applications partnering with UIUC, Duke Progress, and Bonneville Power Administration

Questions?