SAND2017-13656PE

Exceptional service in the national interest

Sandia National Laboratories

Advanced Cyber-secured Protection Schemes for Renewable-rich Microgrids

Matthew J. Reno

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

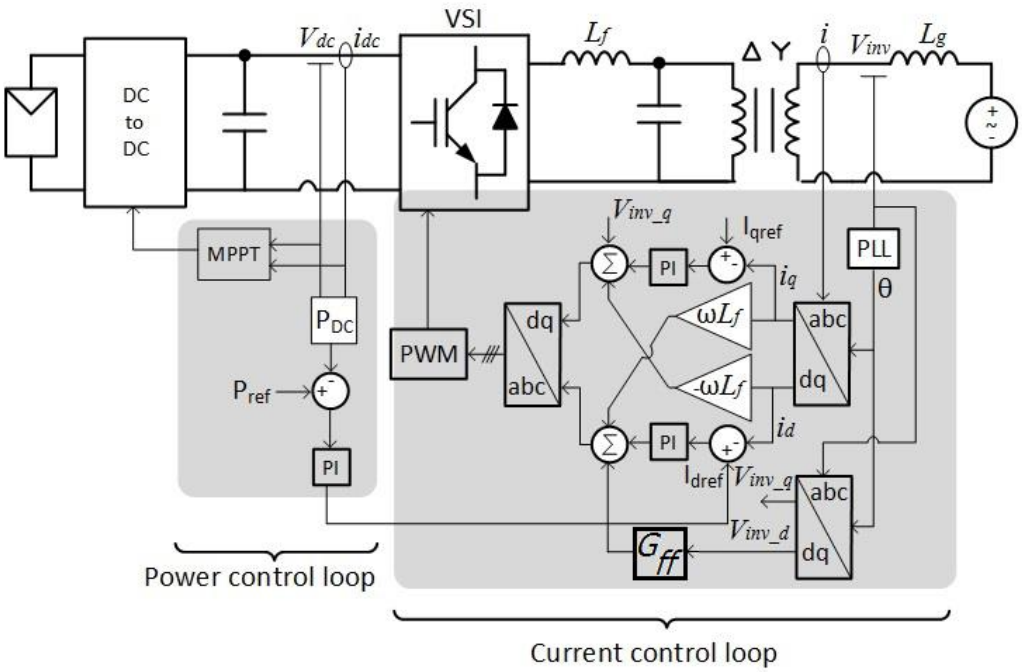
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Outline

- PV Inverter Models for Fault Studies
- Impact of High PV Penetration on Protection Element Design
- Detection of Faults in Microgrids with High PV Penetration
- HIL Protection Analysis
- Cybersecurity of Protection Relays
- FY18 Microgrid Protection AOP

PV inverter models for fault studies

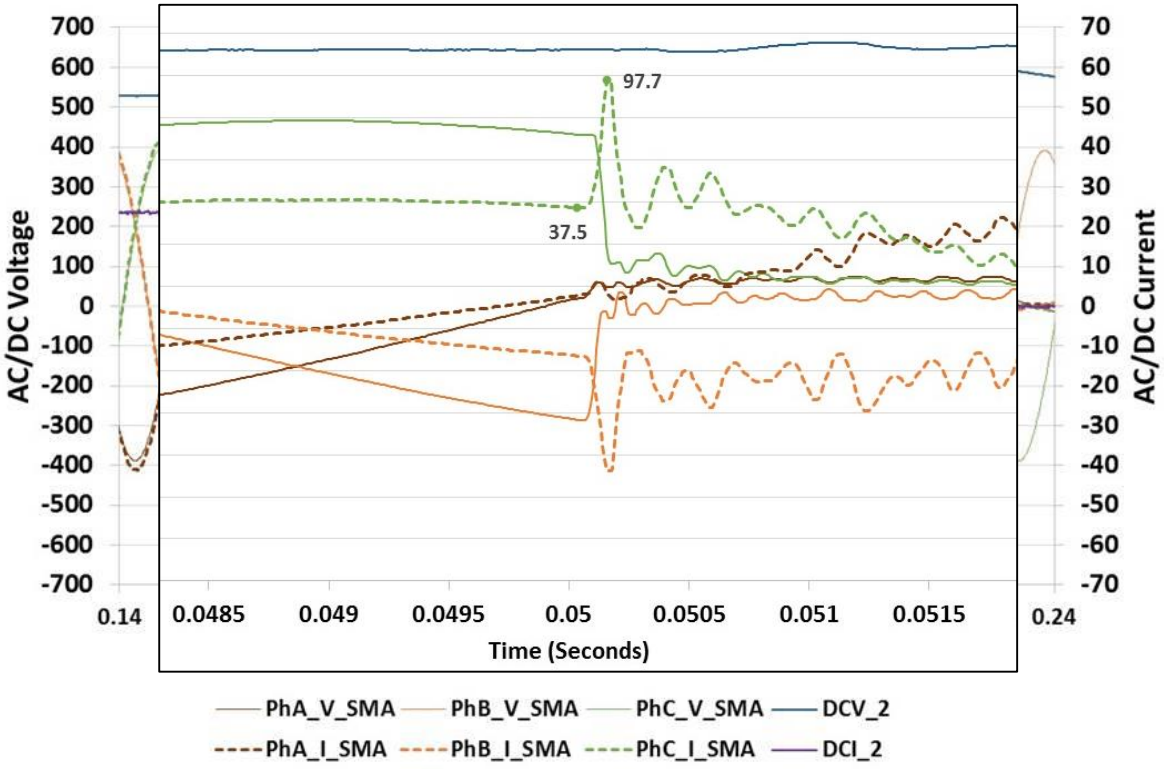


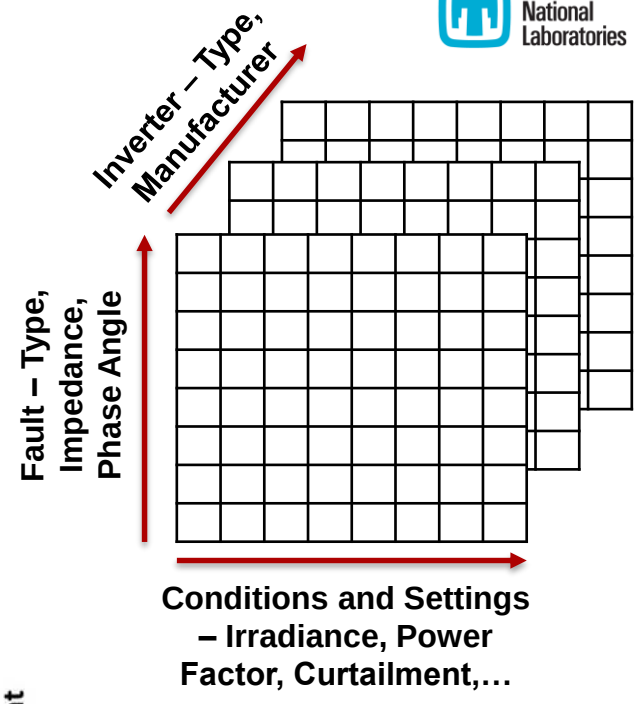
- Developed a comprehensive 3-phase, grid-tied inverter model (in Simulink) suited for fault analysis simulations in microgrids. Main features of the model include:
  - i. MPPT algorithm implementation
  - ii. DQ control scheme for real and reactive power control
  - iii. LVRT algorithm based on IEC standard

- Unbalanced Faults:
  - *Inverter is typically interfaced using YG/Delta transformer and does not inject zero sequence*
  - *Feedforward voltage control plays an important role in reducing (eliminating) negative sequence component in the output current*
  - *Ability to inject balanced current under unbalanced grid voltage depends on inverter's design.*
  - *From protection perspective:* output current is essentially balanced and distortion-free. However, a negative sequence component could be present based on inverters characteristics

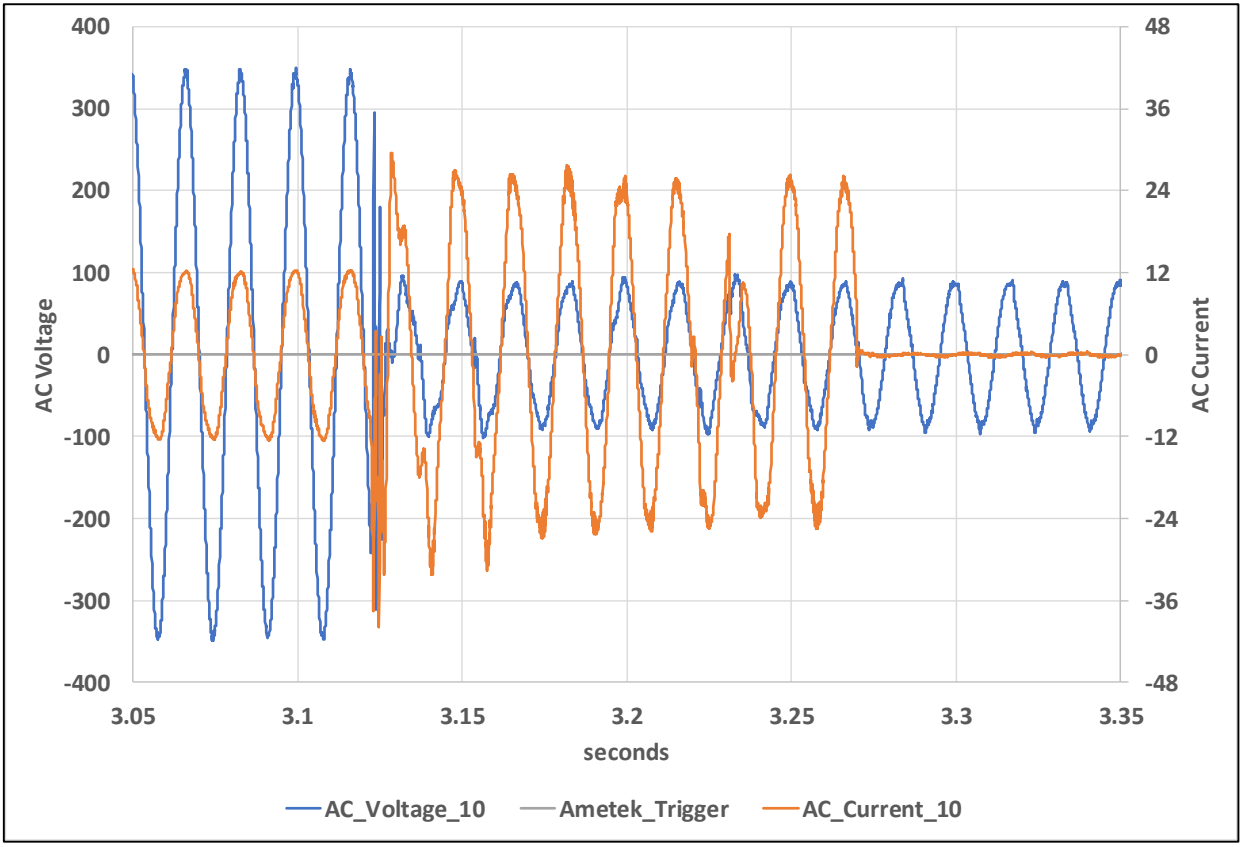
Inverter Fault Modelling

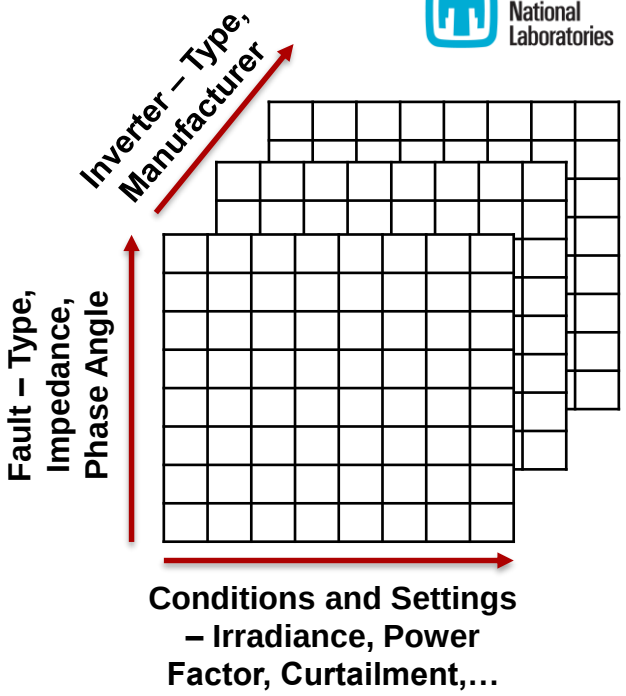
- Validating inverter models using DETL.
- Fault current measurements for different faults, conditions, settings, and inverters





Inverter Fault Modelling





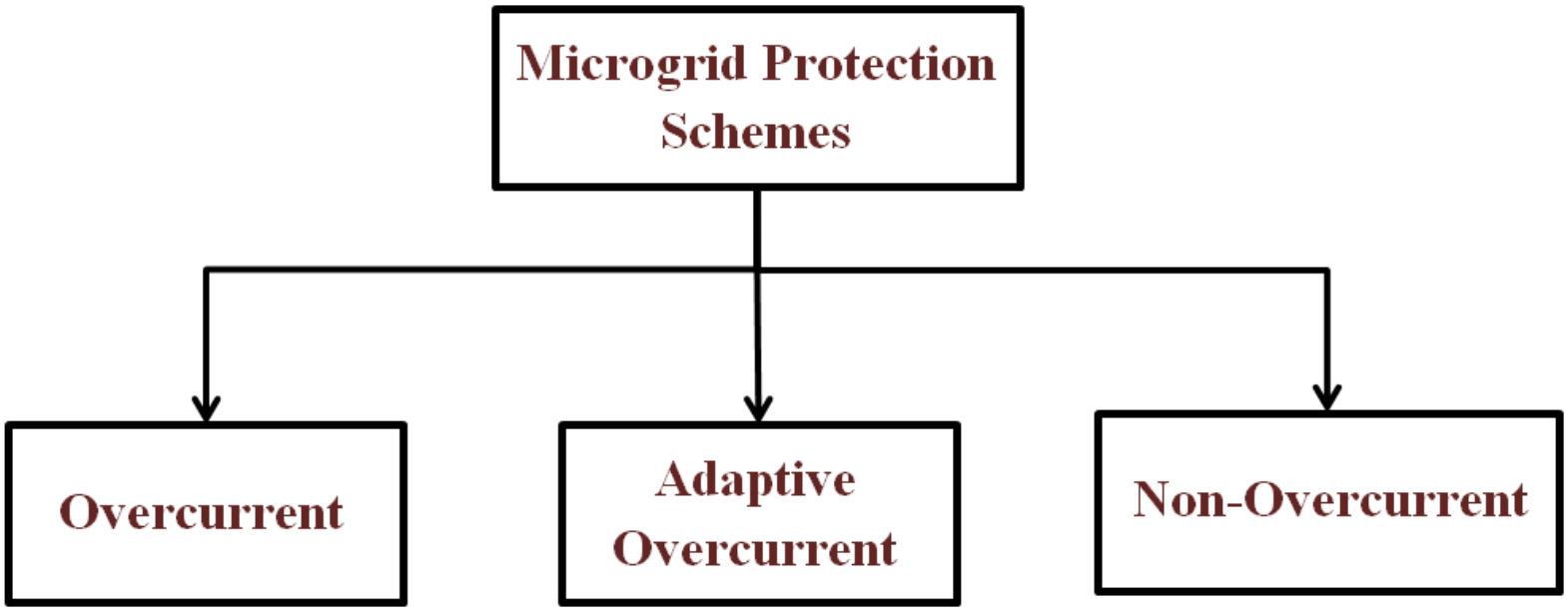
Microgrid Protection Challenges

Sandia National Laboratories

- Variety of sizes, technologies, configurations
  - radial, meshed, dynamic topology
  - difficult to have a "*one size fits all*" solution.
- Islanded and grid-connected modes of operation
  - Significantly different fault levels makes coordination challenging.
  - Fault levels could be very sensitive to generation dispatch thus complicating coordination.
- Inverter-rich Microgrid could have too low fault current
  - Overcurrent might not detect the fault in the first place.
  - High-impedance faults are particularly problematic.

Efficient microgrid protection schemes will also be beneficial for protecting distribution systems with very high penetration of renewable generators.

Microgrid Protection Schemes



Project focus:

1- Cyber security

Project focus:

1- Analysis, development and testing of new protection schemes

2- Cyber security

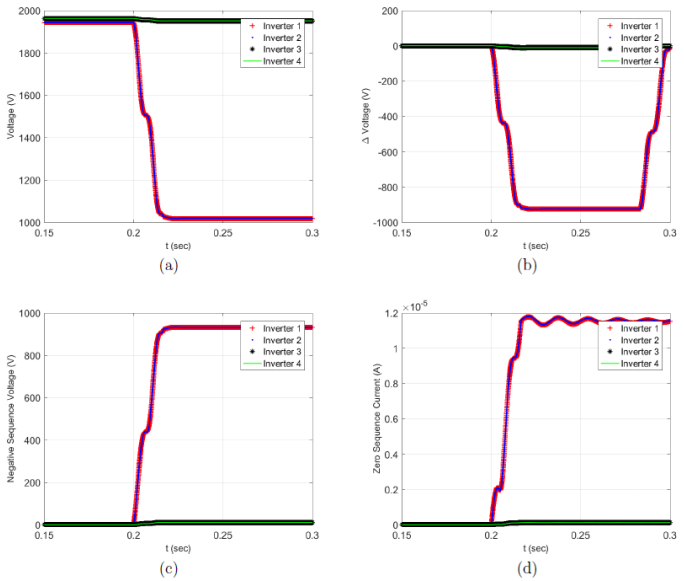
Fault Detection in Microgrids

- Voltage-based Protection:
  - Simple technique
  - Discrimination between faults and normal operation could be hard.
- Superimposed Voltage-based Protection:
  - Based on voltage change at the inverter's terminal
  - Less sensitive to *slow* normal operation voltage changes
- Monitoring Terminal Negative Sequence Voltage and/or Zero Sequence current :
  - Better selectivity between faults and normal operation
  - Sensitive only to unbalanced faults
- Impedance-based Fault Detection
  - Better protection security
  - More expensive

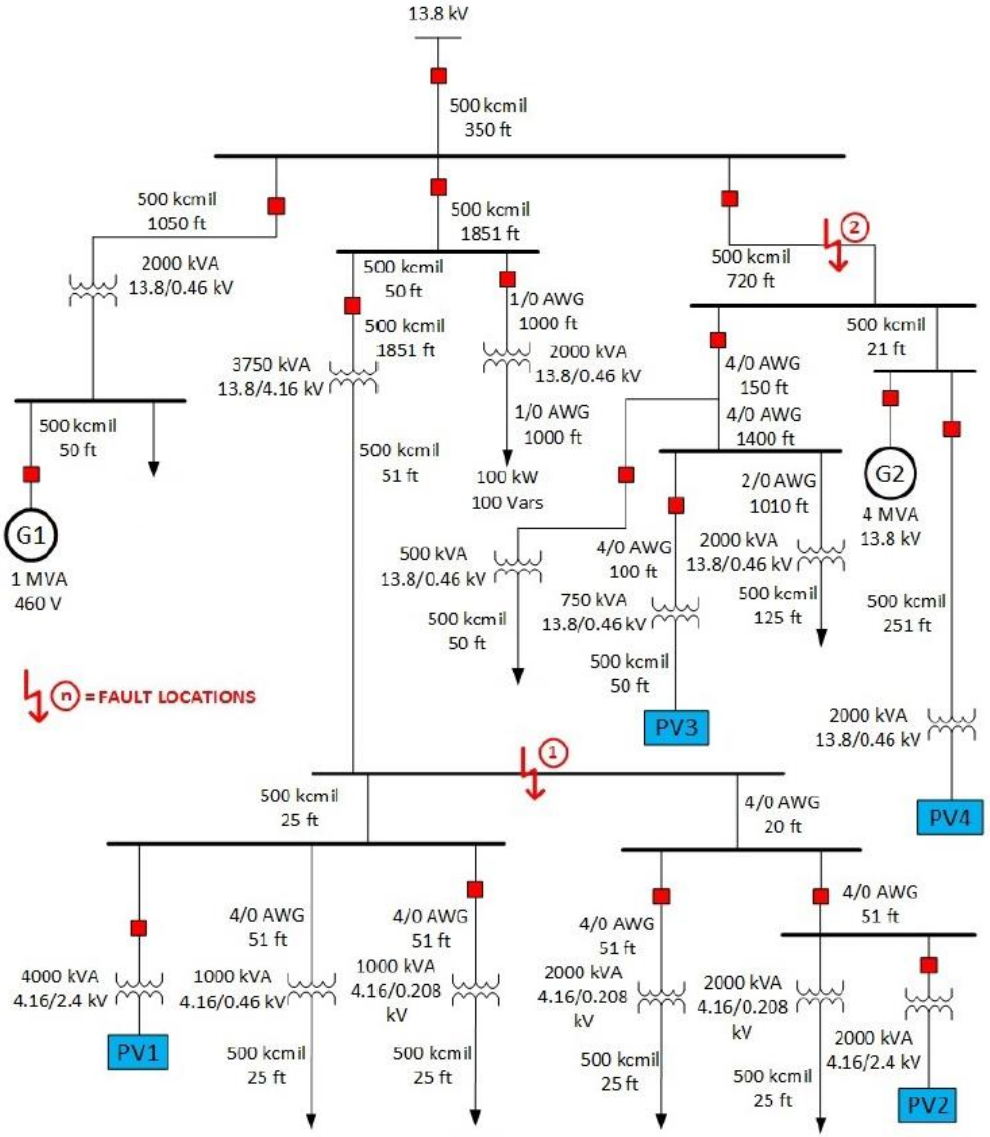
Fault Detection in Microgrids: Simulation Study

Sandia National Laboratories

- Used MIT-LL HIL test feeder
- Tested different fault location, fault types and penetration levels.
- Report compares performance of different fault detection methods.

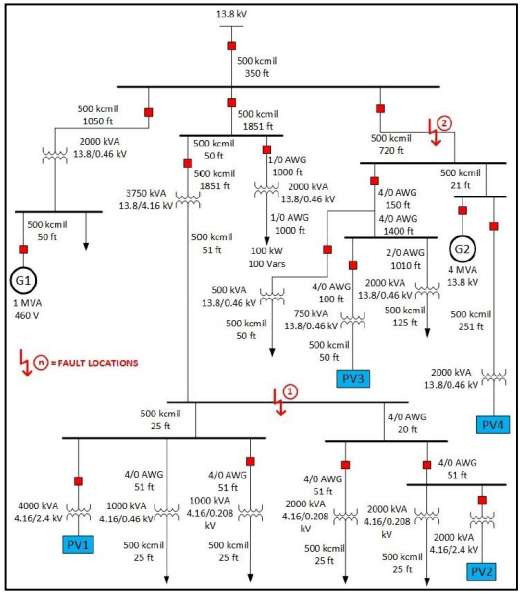


Relays Performance for a phase A to phase B fault at location 1 under grid connected mode (a) Voltage Relay (b) Superimposed Voltage Relay (c) Negative Sequence Voltage Relay (d) Zero Sequence Current Relay

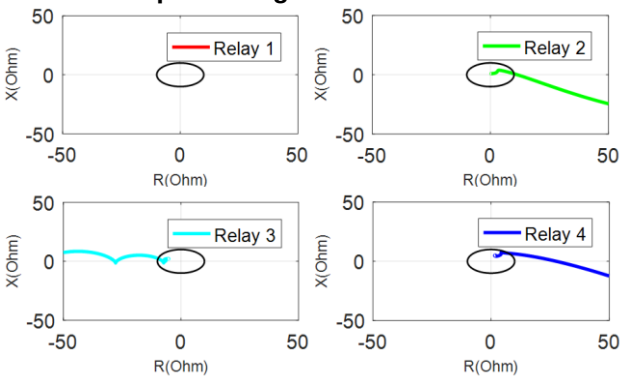


Communication-Assisted Impedance-Based Microgrid Protection

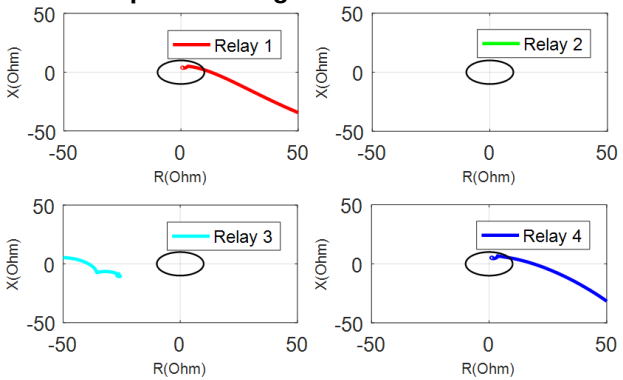
- The proposed scheme depends on monitoring impedance trajectories to detect the occurrence of faults and utilizes directional elements to determine the direction of faults
- Communications between feeder relays are utilized to exchange permissive and blocking signals in order to locate and clear the fault
- Published at PES GM



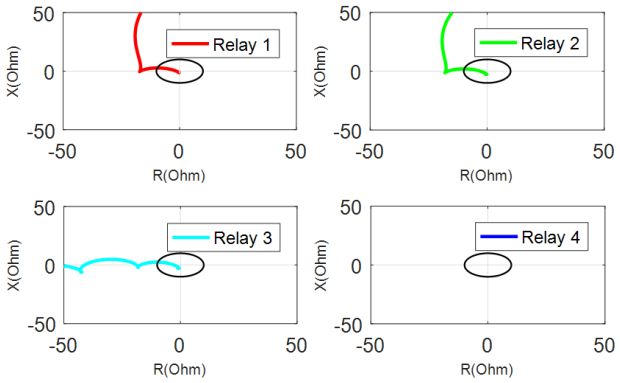
Impedance trajectories during a 3-phase to ground fault at F1



Impedance trajectories during a phase A to ground fault at F2

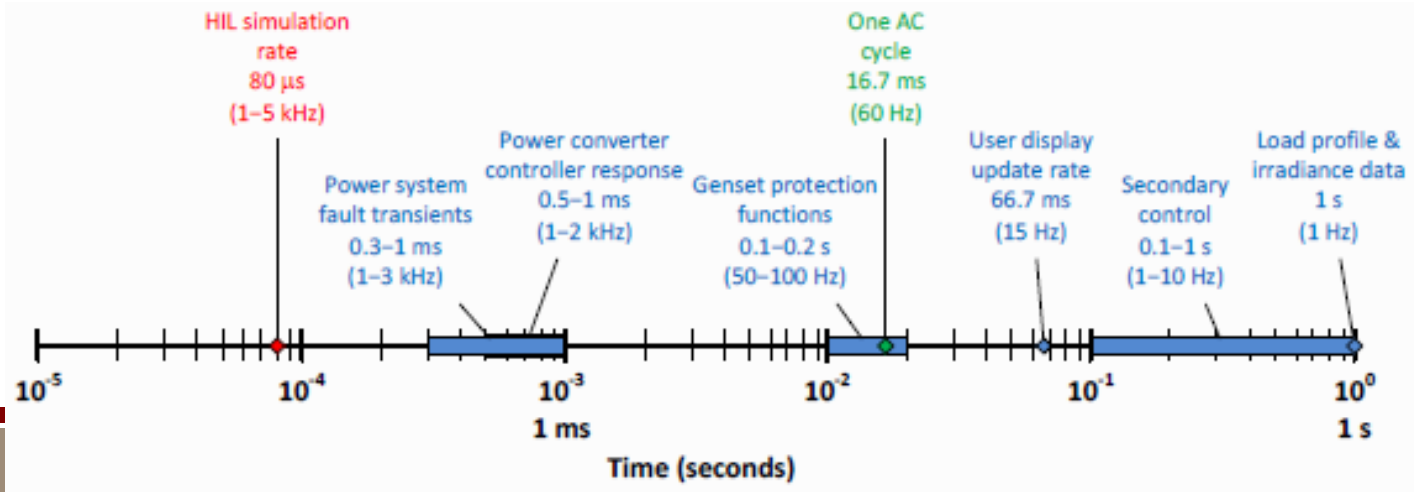


Impedance trajectories during a 3-phase to ground fault at F4 under islanded mode



Protection HIL Setup (Opal-RT)

- HIL testing is an excellent solution for advanced protection studies
  - Real-time simulation increases testing speed for complex cases
  - Using real devices removes concerns about dynamic inverter models
  - Model-based testing methodology can study specific utility systems and realistic testing scenarios
  - It is scalable and flexible and allows adaptation to various study complexity, power system size, and new protection schemes
  - Develop and validate new protection algorithms using HIL simulation
  - For communication-based protection, the communication hardware, protocols, and delays can be tested directly



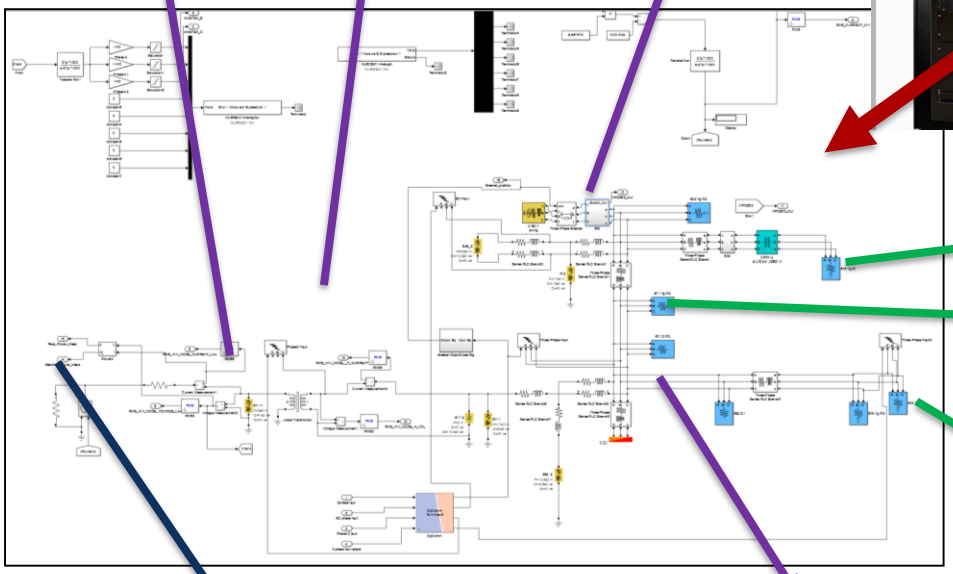
Protection PHIL Setup (Opal-RT)

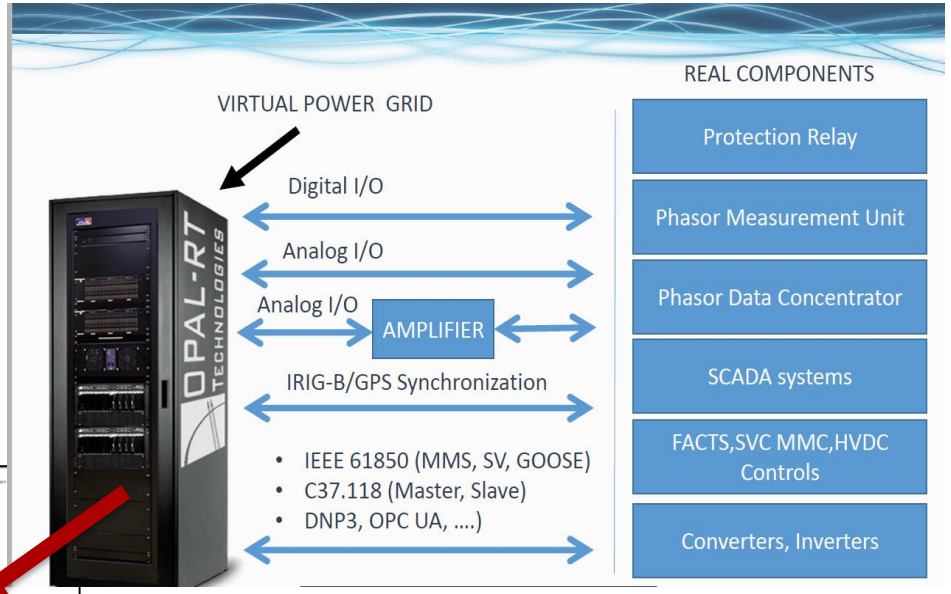
Sandia National Laboratories

SEL 487

SEL 321

SEL 351

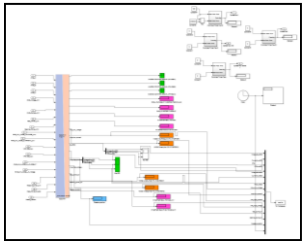




Fronius Single-Phase Inverter

SMA 3-phase Inverter

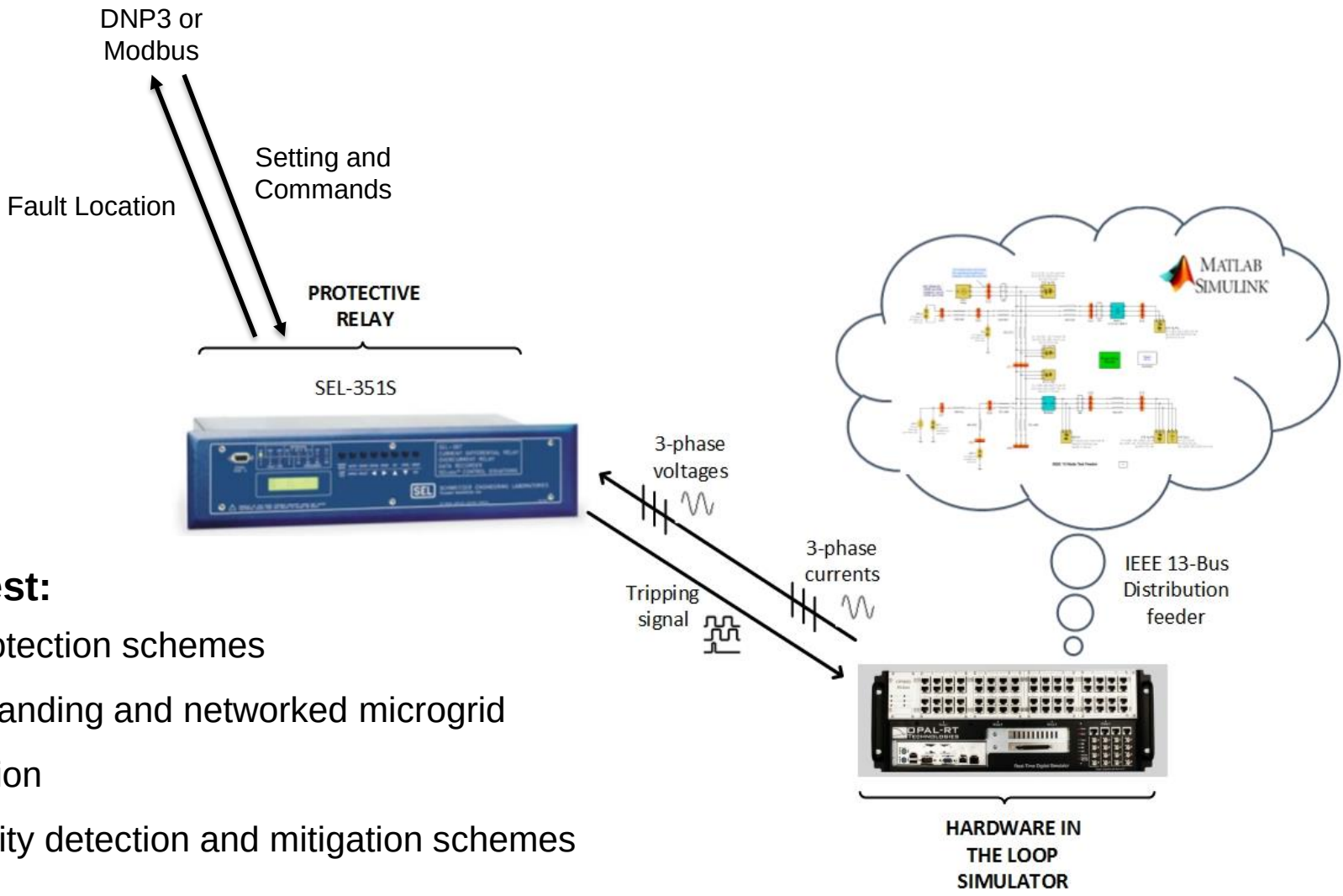
Simulated Inverters



Grid Simulator

Virtual Protective Devices

Protection PHIL Communication Layer

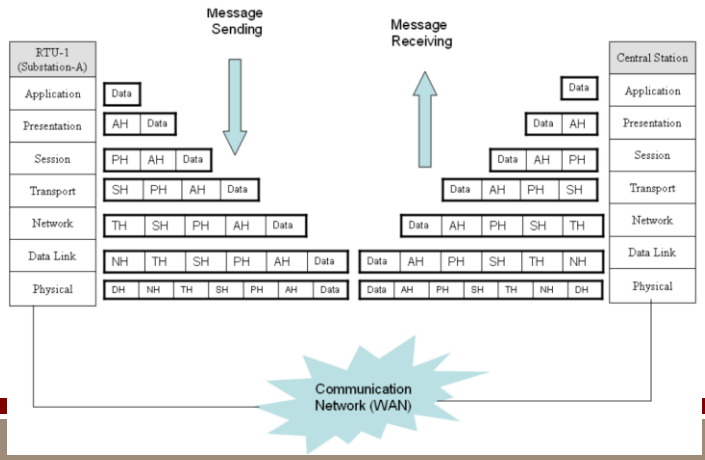


Ability to Test:

- Adaptive protection schemes
- Microgrid islanding and networked microgrid reconfiguration
- Cyber security detection and mitigation schemes

Protection Cyber Security

- Cybersecurity is a key challenge to making protection settings adaptive
- Cyber security of **power system protection** in general is very critical to the reliability of the bulk power system.
- Cyber security is reliant on the communication type and protocol: DNP3, Modbus, IEC 61820, etc.
- Key questions for cyber security design:
  - What should we measure to detect adversary activity
  - How can we provide layered security
  - How to develop general cybersecurity specifications for relays



Many of the protocols are layer-based, as defined by the Open Systems Interconnection (OSI) model. Each layer is a collection of similar functions that provides services to the layer above it and requests services from layers below it

Cyber Vulnerability Assessment of Protection Devices

Sandia National Laboratories

- Conducted vulnerability assessment of protection devices to ensure: confidentiality, message integrity, authentication, authorization, access and availability.
- Security testing validates the intended application and functionality of the device.
- Findings and the report from this assessment advise the industry on best security practices and provide recommendations for interconnection, interoperability, and communication protocol standards development.
- Security Report - Tests
  1. Network Reconnaissance
  2. Packet Replay and Authentication of Data
  3. Man in the Middle Attach (MiTM)
  4. Denial of Service (DoS)
  5. Vulnerability Scans and Patched Software Information
  6. Submit Modified Firmware
  7. Maintained Logs
  8. Password Handling

Cyber Security for Protection

Sandia National Laboratories

- Presently, the prevalent measures being incorporated include firewalls, intrusion detection systems (IDSs), and security gateway devices (SEL 3620)
- However, some gaps include:
  - Cyber security standards exist but are in various stages of development; need to isolate and address technical problems to finalize them
  - Need to merge technical countermeasures and management/organizational issues into comprehensive standards
  - Sandia report titled, "Cyber Security Gap Analysis for Critical Energy Systems (CSGACES)" identified various gaps in ICS cyber security and ranked them
- Device-level security mechanisms are key for protecting field devices and creating multi-layered cyber security solution

Device-Level Security

Sandia National Laboratories

- Low-level analysis-enabled and out-of-band security devices would be significantly useful for field device cyber security
  - Particularly for detecting zero-day exploits and attacks in progress
  - Detect intrusion before damage is incurred
- Improve cyber security posture of the protection with layered approach, pair device-level solutions with network defense such as intrusion detection systems (IDSs) and firewalls
- Report investigates two potential device-level solutions:
  1. **WeaselBoard, developed by Sandia National Laboratories**
  2. **Power Fingerprinting, developed by PFP Cybersecurity**

WeaselBoard

- WeaselBoard (WB), a modular PLC backplane analysis system designed at SNL, addresses the need for ICS cyber security that can detect attacks in progress
  - Zero-day attacks provide no warning or attack signatures; cannot use conventional signature-based approaches
- Developed for programmable logic controllers (PLCs)
- Enables low-level analysis at PLC firmware/hardware level, at the backplane
  - Inspects the physical pins and analyze traffic across them of single PLC as well as between PLCs

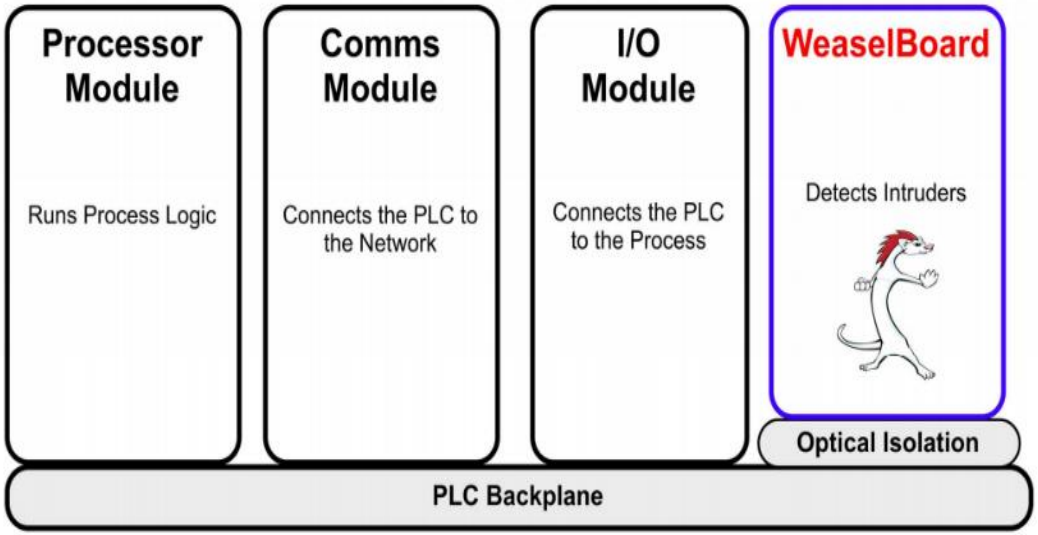
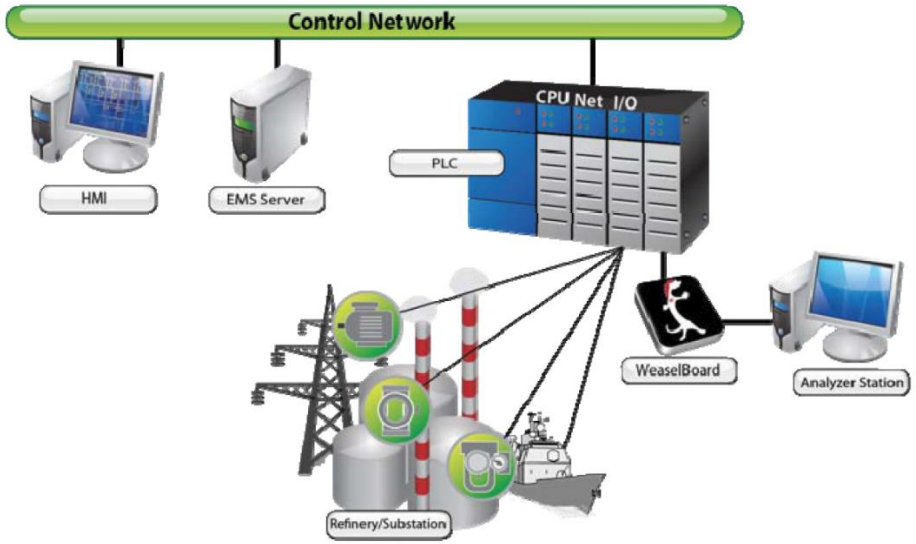


Image Sources: SNL, 2017

WeaselBoard Solution Approach

- WeaselBoard is a modular device that is composed of a main CPU board and a PLC-specific adapter board
  - Adapter board allows connection different types of PLC and shows promise in extending to relays
- Custom protocol, WeaselTalk, designed to extract and transfer data and send commands to the WeaselBoard
  - Protocol assumes UDP is underlying protocol and physical media is Ethernet
- Data is received by a computer, the analyzer station, to both reverse engineer the PLC backplane and detect malicious activity



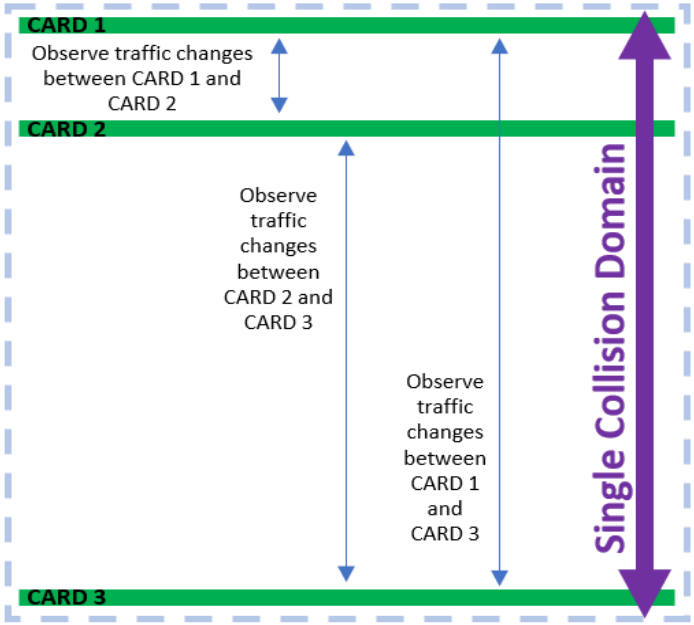


Image Sources: SNL, 2017

Implementation Process

Sandia National Laboratories

Reverse Engineer (RE) Backplane

- Need to RE backplane due to lack of available pin role and interaction information
- Must identify individual pin behavior with multimeter and characterize physical layer
- Analyze backplane traffic to understand and reconstruct communication protocol
- With RE knowledge, design circuit board to capture, parse, and interpret signal traffic to detect real-time attack activity

Detect Malicious Activity

- Detection analysis is performed by classifying the backplane traffic using a rule-set and a Bayesian classifier
- Rule-set is dependent on process-specific limits and causes an alert when predetermine, malicious behavior is observed
- Bayesian classifier identifies known system states to identify traffic related to bad states; it is trained with previous data packets

Obtain Results

- Results offer detection capabilities as well as design analysis (e.g., optimal configuration)
- Able to detect/identify:
  - *Changes in sensor values*
  - *Changes in process control settings*
  - *Changes to ladder logic*
  - *Information about module configuration*
  - *Updates to firmware*
  - *Updates to process control programs*

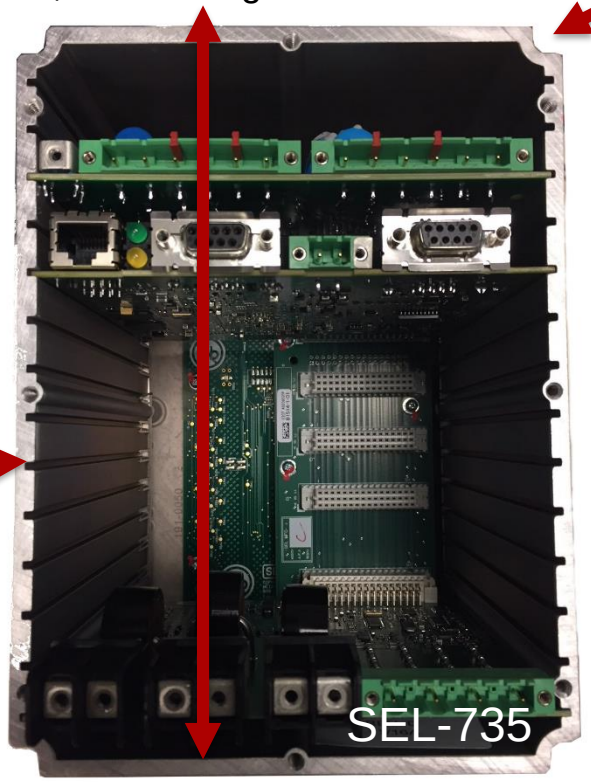
Investigating SEL-735 and SEL-487E

Sandia National Laboratories

Power Quality and Revenue Meter and Transformer Protection Relay

Both have backplanes!

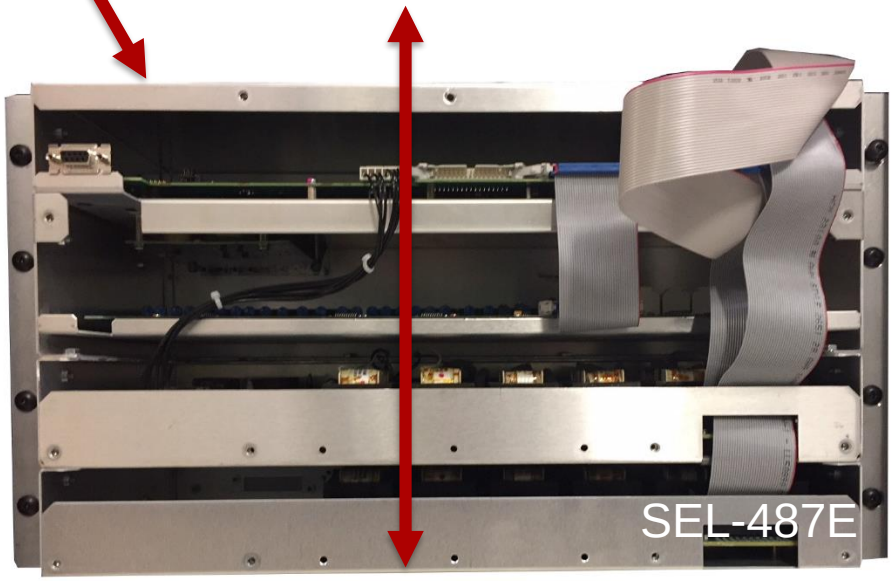
Yes, is on a single collision domain



Similar design to typical 751 feeder protection relays

WeaselBoard can be slid into empty slot---straightforward implementation

Could not readily test single collision domain requirement

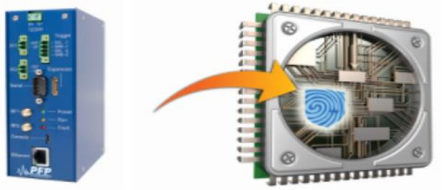


May not have empty card slots, could require “board-on-board” design

Possibly more intensive implementation

Vendor support would significantly aid RE of both device backplanes

Power Fingerprinting



a b

Sandia National Laboratories

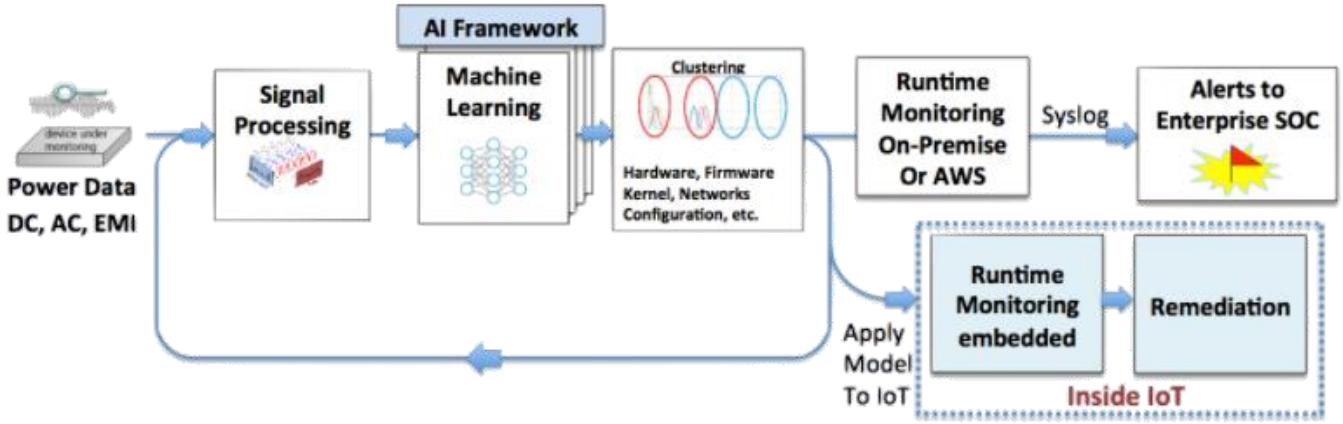
- Power Fingerprinting (PFP) was developed by PFP Cybersecurity and provides an innovative solution for intrusion detection for a variety of electronic devices
- PFP analyzes the power consumption and electromagnetic emissions from a device to assess its integrity
  - Can also detect zero-day exploits and attacks in progress
  - Was demonstrated to detect Stuxnet before it became active

Key Characteristics	
	Can be implemented as an air-gapped module (a), and thus, can retrofit an existing system; doesn't require electrical contacts or software install
	Focuses on physical layer and low-level activity, utilizes simple power analysis
	Has potential to be very cost-competitive, especially if embedded in target device (b)
	Enables Managed Security Service Provider (MSSP) capabilities for Internet-of-Things (IoT) by chip and IoT industries
	Is versatile in application, can analyze any hardware/firmware combination
	Does not require extensive knowledge of network or system target device is within, unlike traditional IDS

Image Source: PFP Cybersecurity, 2017

PFP Solution Approach

- The PFP module utilizes analog signals (AC, DC, EMI) to determine if unauthorized modifications have compromised the integrity of an electronic device or not
- Can detect unique power consumption and EM emission patterns of any hardware/firmware combination



- Identifies abnormal/compromised emissions using signal processing, machine learning, and clustering techniques
  - Trained with data from different execution states of target device/system
  - When anomaly detected, a preset policy for certain scenarios is deployed (remedial actions such as reset or disconnect commands) to restore system to normative state
- Can detect compromises without attack signatures, such as memory attacks and side-channel attacks

Image Source: PFP Cybersecurity, 2017

PFP Application to Protection Relays

- In collaboration with SRNL, PFP Cybersecurity demonstrated on protective relays, specifically SEL-751A
  - Detected changes in logic, or execution states, within relay using only EM emissions
- PFP is suitable for relay security and could be deployed in a modular manner, similar to WeaselBoard

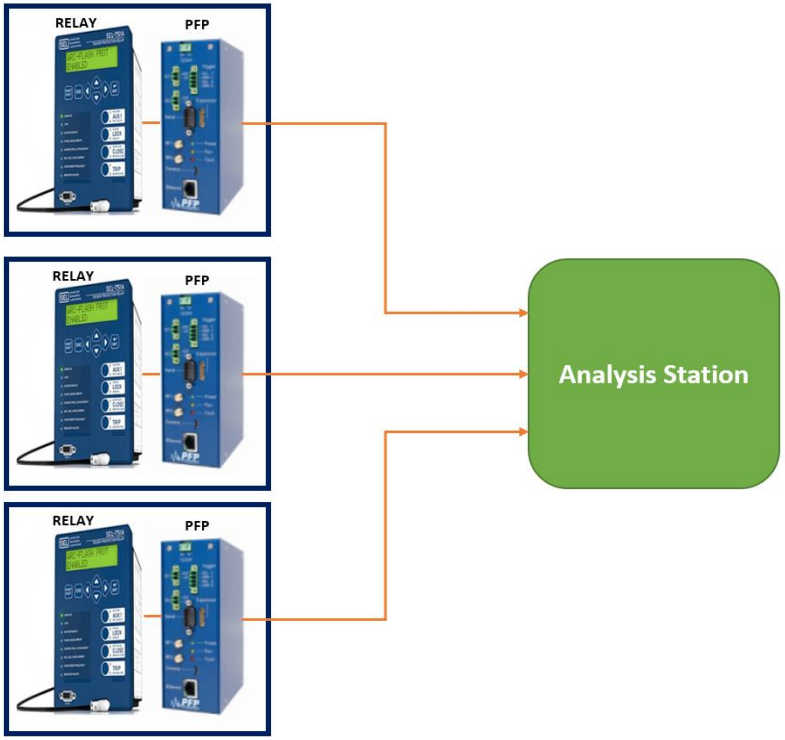
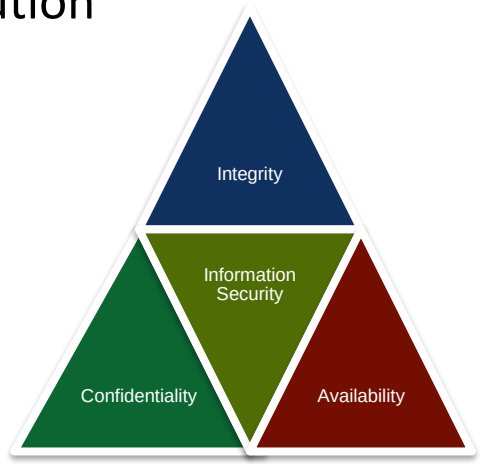


Image Source: PFP Cybersecurity, 2017

General Relay Cyber Security

- Cyber security best practices must be applied to entire protection system
  - Need to ensure authentication, authorization, and accounting (AAA) by using strong password policies, role-based access control, logging, etc.
  - Need to ensure CIA triad: confidentiality, integrity, and availability through measures such as encryption and integrity checks
- Multi-layer security approach must be taken
  - Device-level security that leverages low-level analysis provides powerful security capabilities, including detection of attacks in progress
- Addressing cyber security of field devices, such as protective relays, can inform and develop design for a holistic and defense-in-depth cyber security solution



FY18 Microgrid Protection AOP

Sandia National Laboratories

- SNL and ORNL will collaborate on a holistic approach to address distribution system and microgrid protection design under high inverter-based DER penetration
  - Develop, validate, and demonstrate highly reconfigurable protection schemes including adaptive overcurrent and non-overcurrent schemes
- Fault location schemes for systems with high DER penetration
- Protection schemes for DC microgrids
- Involvement in IEEE PSRC committees and working groups
- Application of microgrid protection into Networked Microgrid OD&D Project

QUESTIONS?

Sandia National Laboratories
Matthew J. Reno
mjreno@sandia.gov