



# IEEE P1952: Resilient Positioning, Navigation, and Timing User Equipment Working Group

October 19, 2022

**Jeff Dagle, PE**

Chief Electrical Engineer

Electricity Security Group / Resilience Team

Pacific Northwest National Laboratory




PNNL is operated by Battelle for the U.S. Department of Energy



# Executive Order 13905 Requirements & Timeline

- *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services*
- Sector specific agencies, including DOE, will develop a plan to engage and evaluate use of PNT services
- Secretary of Commerce and Sector-Specific Agencies release initial PNT Profile
- DHS and Sector-Specific Agencies develop a plan to test PNT vulnerabilities
- DHS and Sector-Specific Agencies develop contractual language for PNT in Federal contracts
- DHS and Sector-Specific Agencies submit report to OSTP on adoption of PNT Profiles



Federal Register  
Vol. 85, No. 32  
Tuesday, February 18, 2020

9359

## Presidential Documents

Title 3—	Executive Order 13905 of February 12, 2020
The President	Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1. Purpose.** The national and economic security of the United States depends on the reliable and efficient functioning of critical infrastructure. Since the United States made the Global Positioning System available world-wide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response. Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators.

**Sec. 2. Definitions.** As used in this order:

(a) “PNT services” means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

(b) “Responsible use of PNT services” means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

(c) “Critical infrastructure” means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters.

(d) “PNT profile” means a description of the responsible use of PNT services—aligned to standards, guidelines, and sector-specific requirements—selected for a particular system to address the potential disruption or manipulation of PNT services.

(e) “Sector-Specific Agency” (SSA) is the executive department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

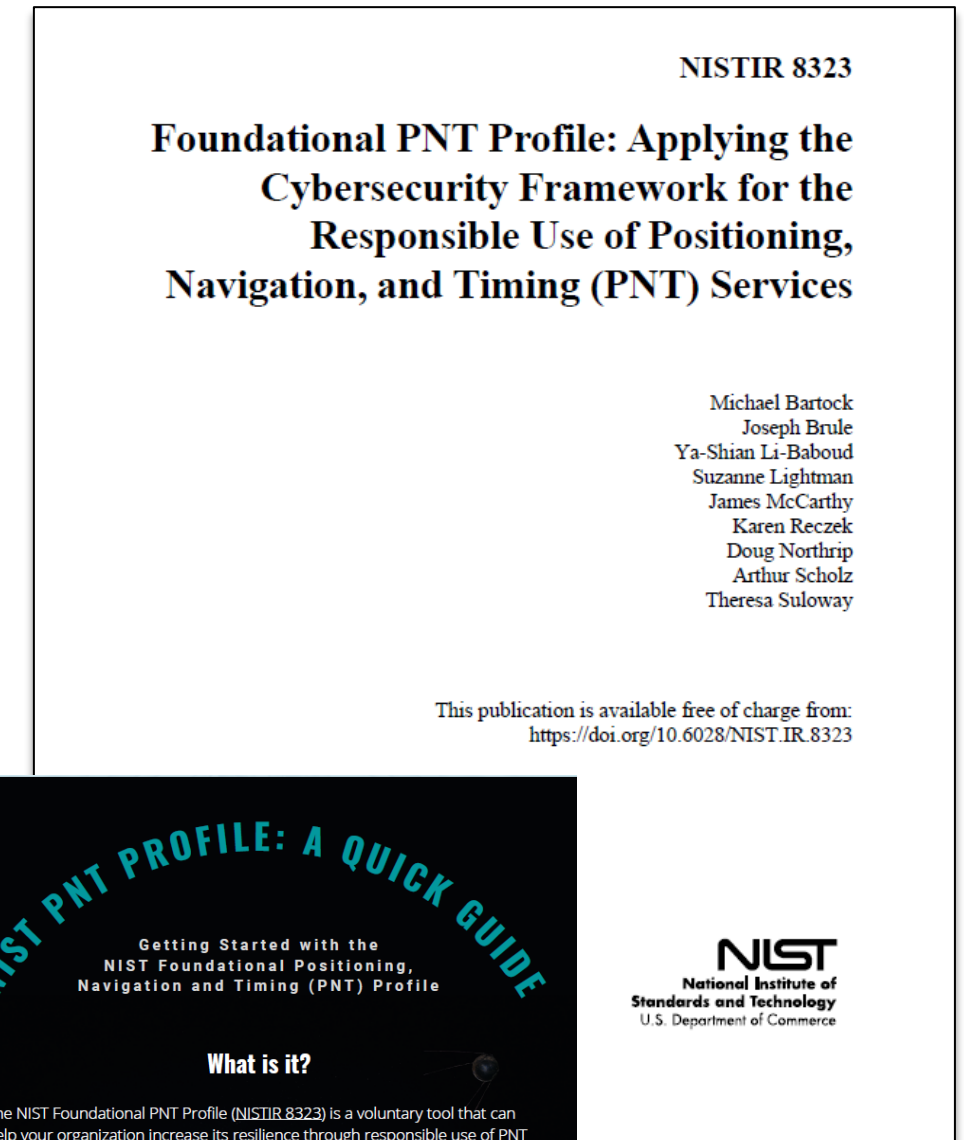
**Sec. 3. Policy.** It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation’s awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services.

2



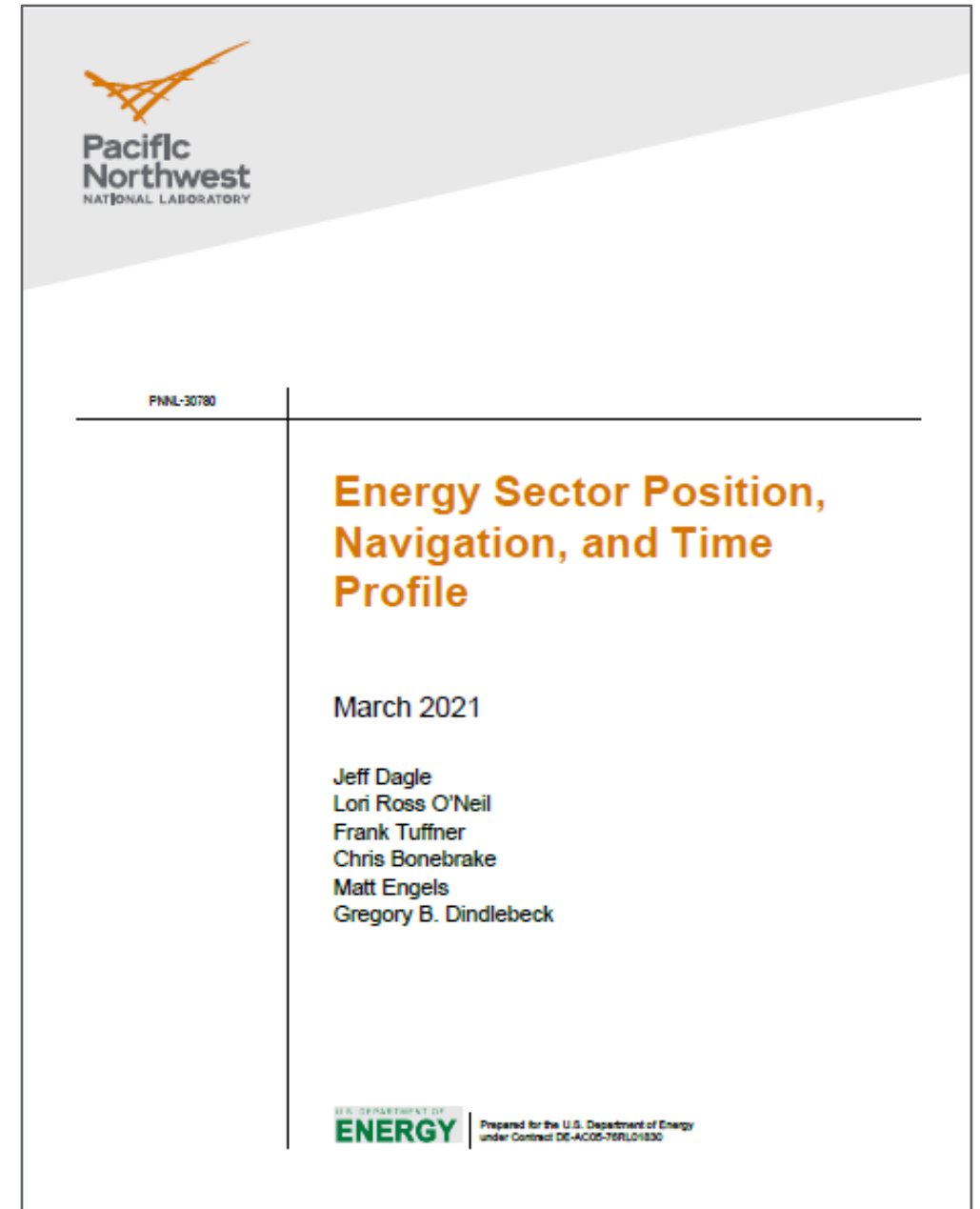
# DHS and NIST sector neutral PNT Profile

- February 12, 2021 NIST releases NISTIR 832:  
*Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*
  - Along with a 3-page Quick Start Guide
- Follows NIST Cyber Security Framework:
  - Identify, Protect, Detect, Respond, Recover
- Intended for all 16 critical infrastructure sectors
- Each Sector-Specific Agency is expected to develop their own PNT Profile that builds on NISTIR 8323, addressing the unique needs of their sector
  - DOE is responsible for the Energy Sector's PNT Profile



# DOE's Energy Sector PNT Profile Focus

- Addresses the unique needs of the Energy Sector
  - Electricity, oil and natural gas subsectors
- Profile focuses on timing. Positioning and navigation do not need precise time in electricity subsector.
  - The Department of Transportation will address position and navigation aspects that may relate to asset management, field crew deployment, drone operations, etc.
- Profile focuses on electricity applications in the microsecond ( $\mu$ s) class of timing precision and accuracy
- Less accurate timing needs, which can be met via networks (NTP) or radio (e.g., WWVB), are declared out of scope
  - We determined that the oil and gas subsector does not require precise time in the  $\mu$ s accuracy



# Energy Sector PNT Profile

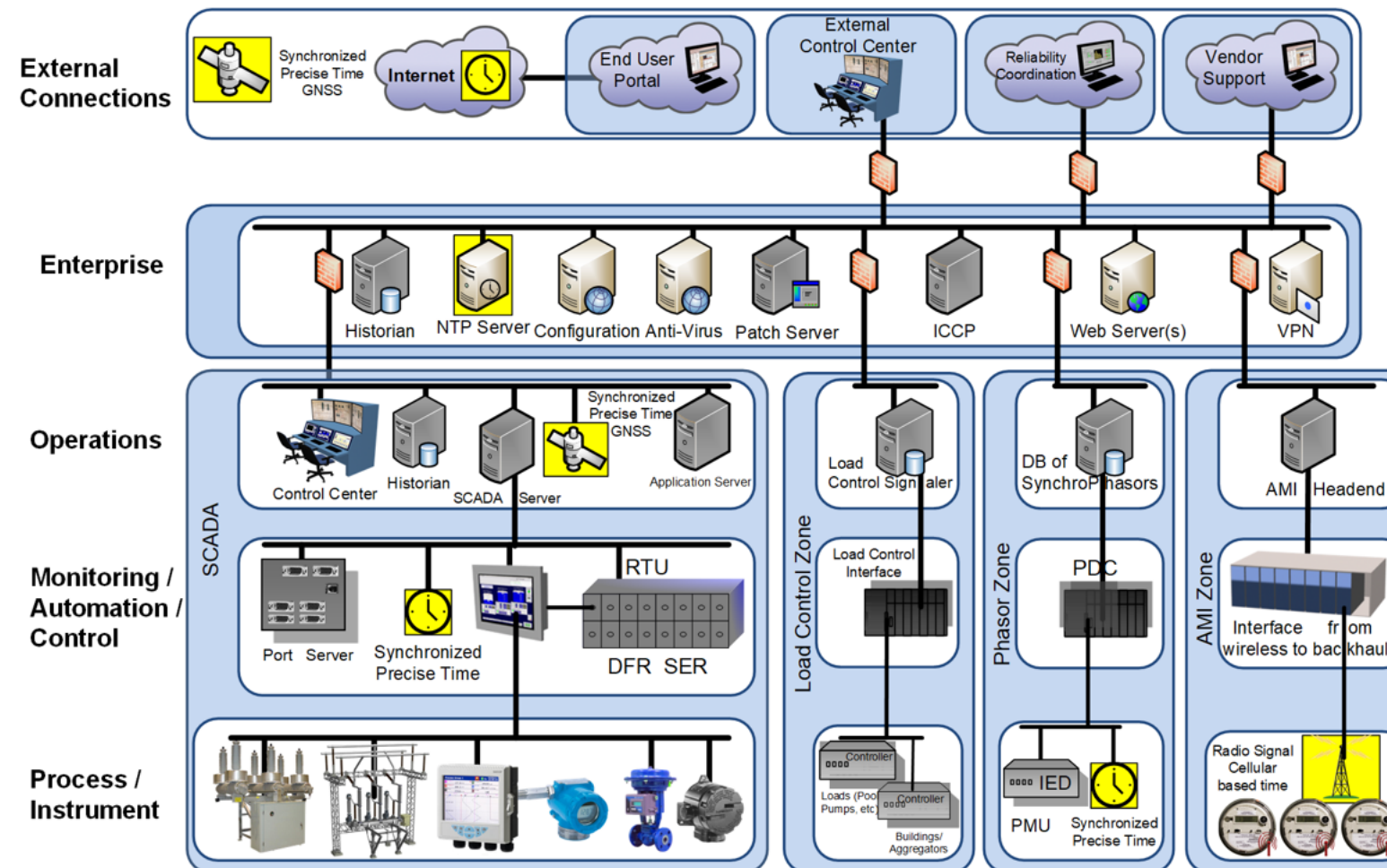
- Follows the NISTIR 8323 approach of NIST Cybersecurity Framework
  - [Identify] Current PNT Landscape in the Energy Sector
  - [Protect] Current Protection Landscape
  - [Detect] Threats and Consequences
  - [Respond & Recover] Mitigations
  - Next Steps



# Energy Sector PNT Profile - Identify

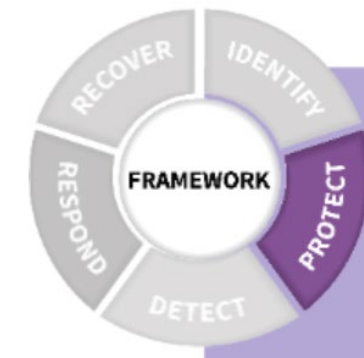


## [Identify] Current PNT Landscape in the Energy Sector





# Energy Sector PNT Profile - Protect



## [Protect] Current Protection Landscape

- PNT-related Standards in Energy Sector
  - Precision Time Protocol (IEEE 1588-2019)
  - Time Tagging for Intelligent Electronic Devices (IEEE C37.237-2018)
  - Inter-range Instrument Group Timecode (IRIG-B)
  - Substation Automation (IEEE/IEC 61850-9-3-2016, IEEE C37.238-2017)
  - Synchrophasors (IEC/IEEE 60255-118-1-2018, formerly IEEE C37.118.1)
  - Data Transport/Aggregation Standards
  - Disturbance Measurement Requirements (NERC PRC-002-2)
  - Oil and Natural Gas Sequence of Events Records
- Practical PNT Protection in the Energy Sector
  - Firmware Management
  - Multiple Local Redundant Time Sources
  - Resilient GNSS Antennas
  - Multi-Band GNSS Time Sources
  - Multi-Constellation GNSS Time Sources
  - Backup Offsite Time Source

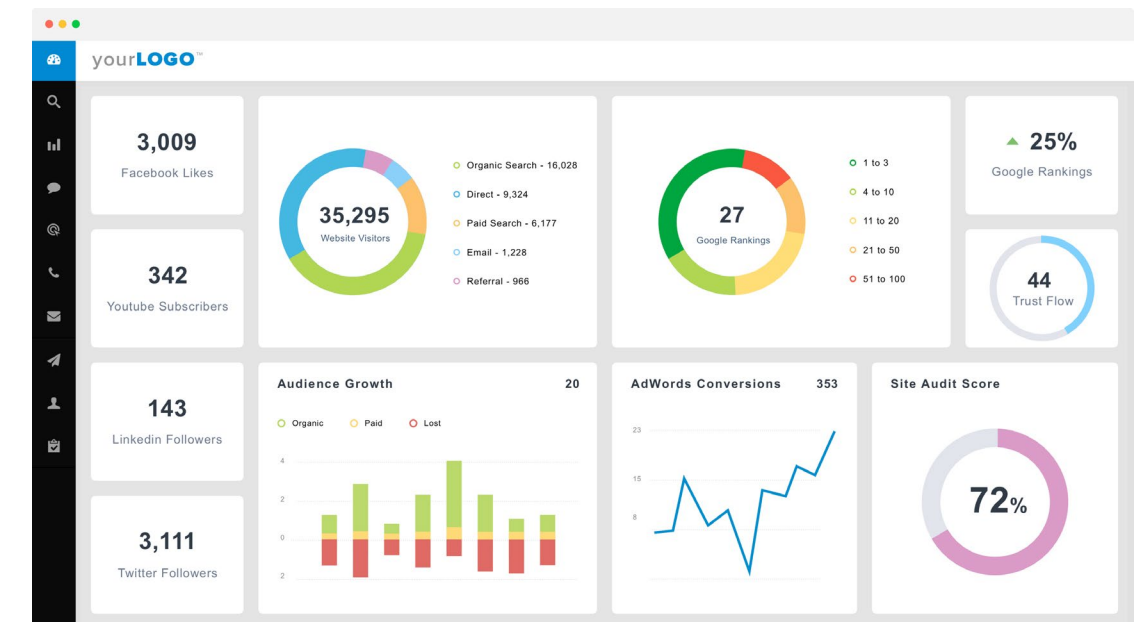


# Energy Sector PNT Profile - Detect



## [Detect] Threats and Consequences

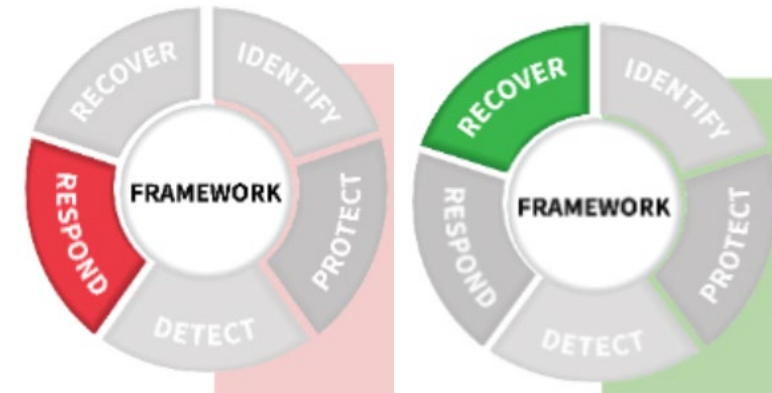
- Detecting Timing Attacks
  - Time Distribution Mediums
  - GNSS Attacks
  - Network-Based Time Attacks
  - Redundant Time Sources
  - Hardware/Software Attacks
- Reporting of Detected Attacks
  - Syslog and Simple Network Management Protocol
  - Security Information and Event Management



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



# Energy Sector PNT Profile Respond & Recover




## [Respond & Recover] Mitigations

- Response Plan
- Communications
- Analysis
- Mitigations

### Response & Recovery Plan

Company



Logo  
Name

### ANNUAL TEST PLAN

**CONTINUITY OF OPERATIONS**

REPORT DATE	PROJECT NAME	PREPARED BY
Date	Project	Name

**STATUS SUMMARY**

To get started right away, just tap any placeholder text (such as this) and start typing to replace it with your own.

**TAB 1 F TOP**

TASK	% DONE	DUE DATE	DRIVER	NOTES

**EXERCISES**

CATEGORY	SPENT	% OF TOTAL	ON TRACK?	NOTES

**TESTS**

ISSUE	ASSIGNED TO	DATE

Company Name

### COMMUNICATIONS PLAN

# IEEE P1952: Standard for Resilient Positioning, Navigation, and Timing (PNT) User Equipment

**Scope:** This standard specifies technical requirements and expected behaviors for resilient Positioning, Navigation, and Timing (PNT) User Equipment (UE).

The scope is limited to the reception, ingestion, processing, handling, and output of PNT data, information, and signals.

The scope does not include standards relating to the characteristics of PNT sources.

Based on technical requirements, the standard defines different levels of resilience to enable users to select a level that is appropriate based on their risk tolerance, budget, and application criticality.

This standard applies to UE that outputs PNT solutions, including PNT systems of systems, integrated PNT receivers, and PNT source components (such as Global Navigation Satellite System (GNSS) chipsets).

# IEEE P1952 Use Case Subgroup

Initial areas of focus:

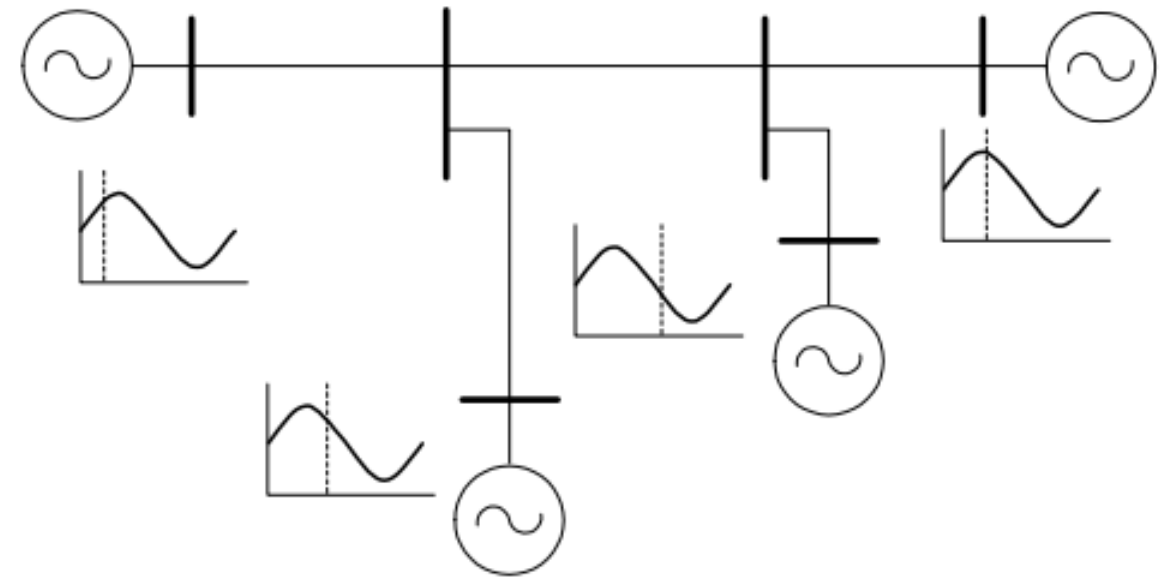
- Energy Sector
- Communications Sector
- Transportation Systems Sector
- Financial Services Sector

Initial area of focus: stationary precision timing applications



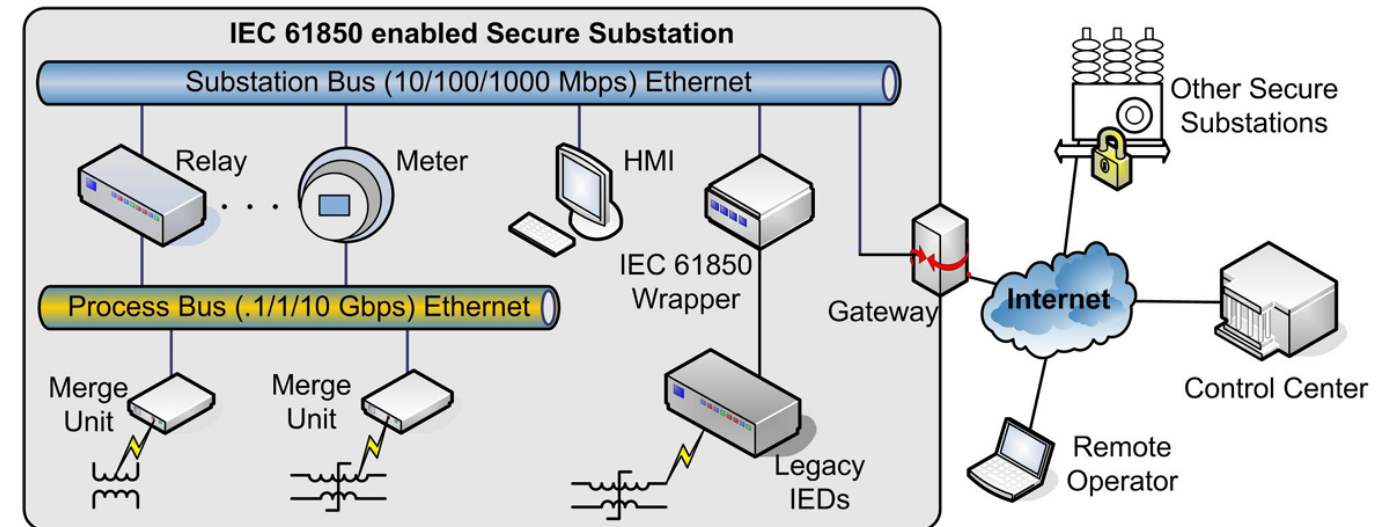
# Synchrophasors

- Time-synchronized voltage and current measurements that includes the phase angle for the fundamental system frequency across a wide area
- Accuracy requirements (directly related to timing precision) are governed by IEEE and IEC standards
  - IEEE/IEC 60255-118-1-2018 (replaces IEEE C37.118.1)
  - Accuracy required: tens of microseconds
- The resilience consequences are highly dependent on how the measurements are being utilized:
  1. Feedback control (including protection)
  2. Feed-forward controls (e.g., state estimation)
  3. Situational awareness and visualization
  4. Off-line applications (e.g., event and engineering analysis)
- The criticality of these measurements have been increasing over the past several years



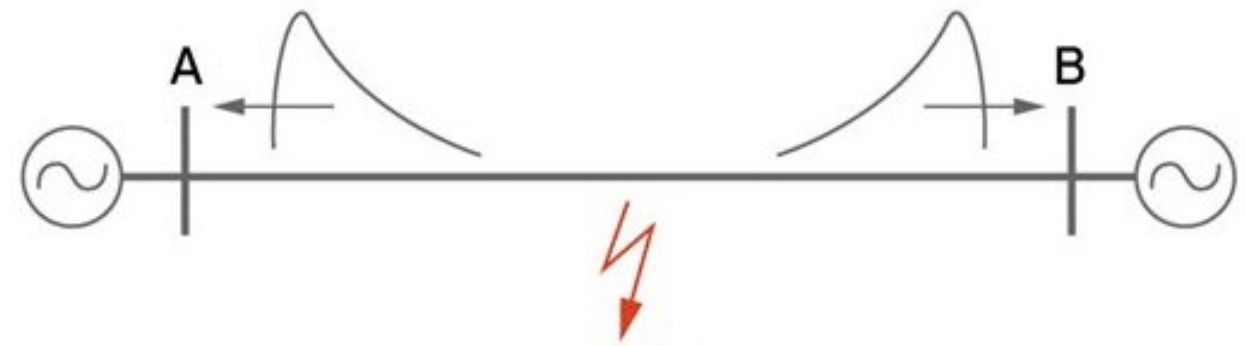
# Sampled Values

- Deployment of IEC 61850 for substation automation applications (emerging in North America) defines a protocol for information exchange between intelligent electronic devices and merging units with digital representations of analog quantities (e.g., voltages, currents)
  - Mostly intended for localized applications within a substation
- Time accuracy requirement: application-dependent, on the order of microseconds
  - IEC 61869-9 defines accuracy requirement  $\pm 1$  microsecond
- The protocol includes a description for sampled value measurements
  - Publisher/subscriber approach for sending time-stamped messages
- Global synchronization is necessary when information is coming from multiple clocks
  - Local applications may be possible without a global time reference
- Mis-operation of this scheme could have impacts on smart substation applications, including false operation of circuit breakers, etc.



# Traveling Wave Fault Location

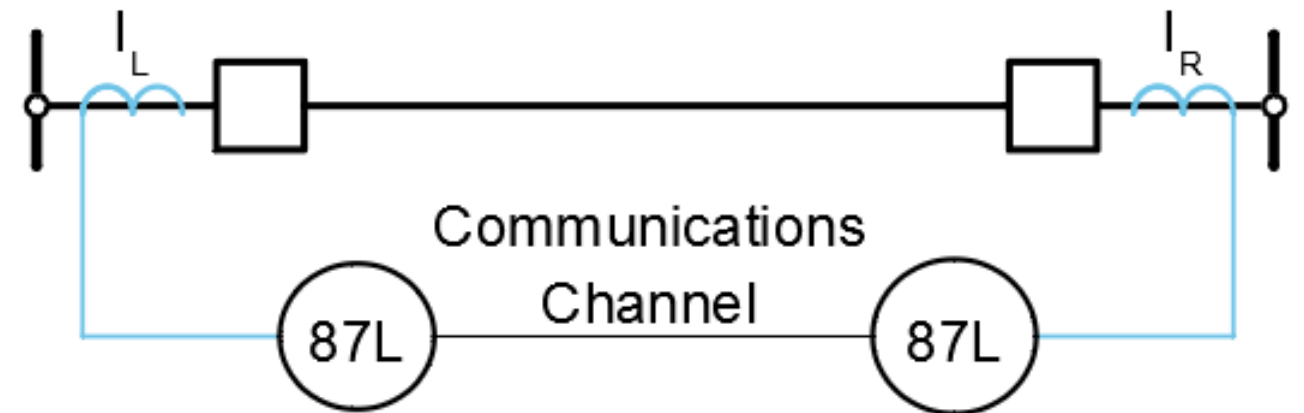
- Advanced protection scheme that determines the location of a transmission line fault by comparing the arrival time of the fault-induced transient at each terminal
- The scheme requires precise time synchronization, each nanosecond of error results in approximately 0.3m uncertainty resolving the location of the fault
  - Traveling waves propagate at approximately 98% of the speed of light
  - Accuracy requirements: approximately 500 ns to resolve within a tower-tower span distance
- Traveling wave location and/or protection schemes require synchronization between each end of the line (achieved through dedicated fiber optic links), accuracy to global time is less consequential





# Line Current Differential Protection

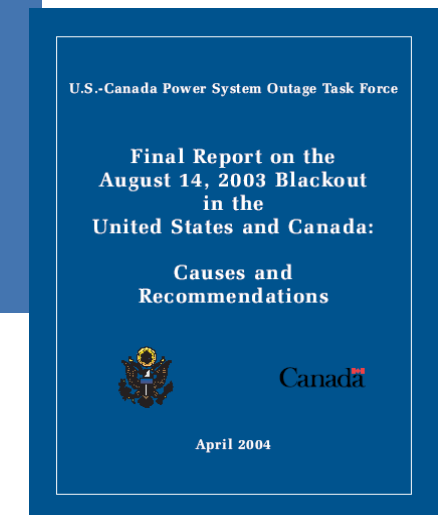
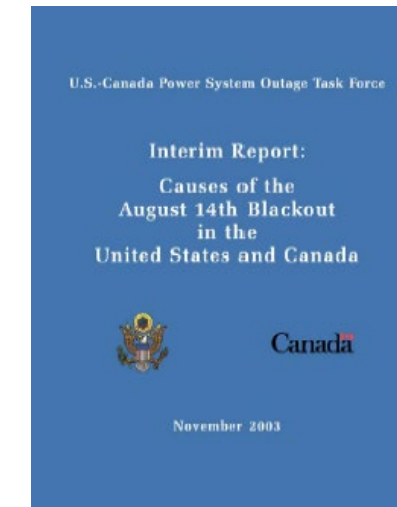
- Protection scheme that utilizes highly reliable and low latency communications links between substations
- Compares time-stamped current measurements on each terminal of a transmission line, and operates protection scheme when a line fault is determined based on mismatch
- The scheme depends on reliable time synchronization between substations
- There are schemes that depend on timestamp accuracy (typically resolved to the microsecond)
  - Potential for mis-operation with clock error



Line differential relays (device 87L) compare the local line current ( $I_L$ ) and remote line current ( $I_R$ ) to determine whether a line fault (i.e., short circuit) has occurred.

# Disturbance Measurement

- Accurately determining the sequence of events is critical for event analysis (i.e., event analysis, or blackout investigations)
  - When multiple utilities are involved, time-aligning the data is critical
- In North America, the North American Electric Reliability Corporation (NERC) Protection and Control (PRC) reliability standard NERC PRC-002 requires better than  $\pm 2\text{ms}$  accuracy with respect to Coordinated Universal Time (UTC)
- Other jurisdictions also require adherence to this requirement



# Thank you

