Resilient Time Synchronization for the Energy Sector

Evaluation of Mitigation Technologies

Gerardo Trevino
Technical Leader Cybersecurity

Workshop on Synchronization and Timing Systems
Virtual Webinar Series
May 13, 2020

Agenda

- Background
- Resilient Time Synchronization for the Energy Sector
  - EPRI Survey Results
  - Supplemental Projects
  - Interest Group
- Next Steps

Background

- GPS is vulnerable* – 3 types
  1. Naturally occurring
  2. Unintentional (interference)
  3. Intentional (jamming or spoofing) – EASY!

GPS is used by the electric sector to provide time data therefore….

energy sector is vulnerable

Background - Moving towards faster response times

More Utility Applications Rely on Precision Timing Enabled by Network-Based Architectures

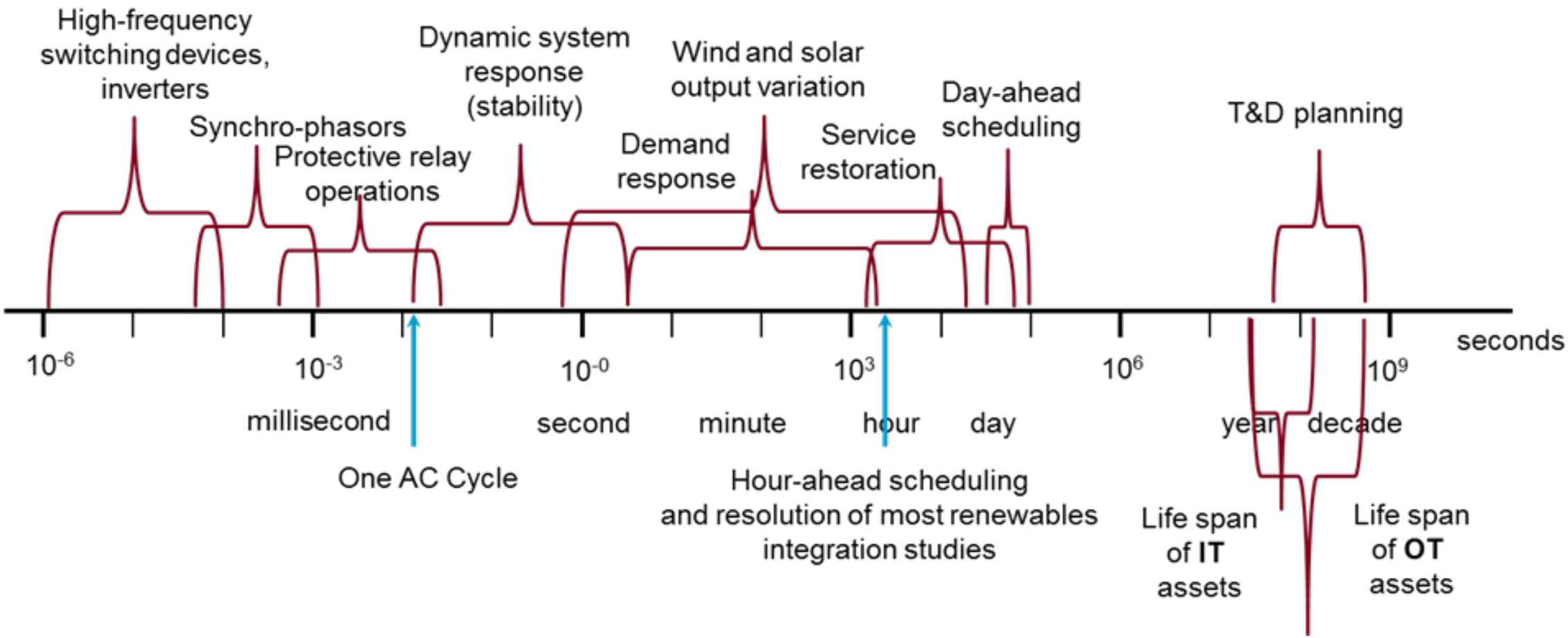
- Substation Automation
- Sampled Values (SV)
- Fault Location
- T&D Relays
- Teleprotection
- Telecommunications networks (i.e. MPLS)
- UAVs
- Synchrophasors (PMUs)
- Network time distribution technologies (i.e. PTP)
- Transition from SONET to modern telecommunications
- New GPS technologies (clocks, detection)

Precision Timing Vulnerabilities

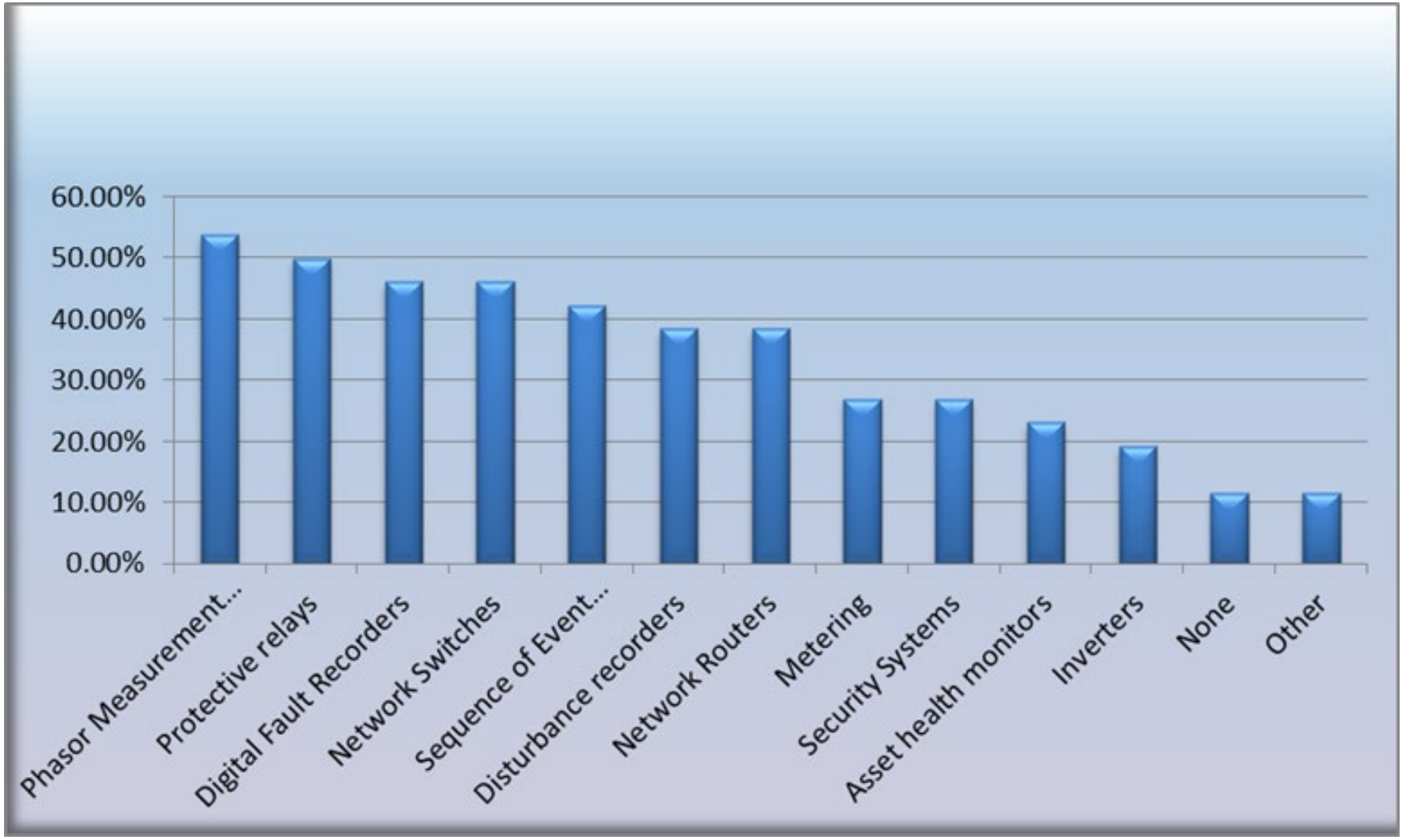
- Timing Drift (natural or intentional)
- Network attacks

EPRI Time Synchronization Survey Results

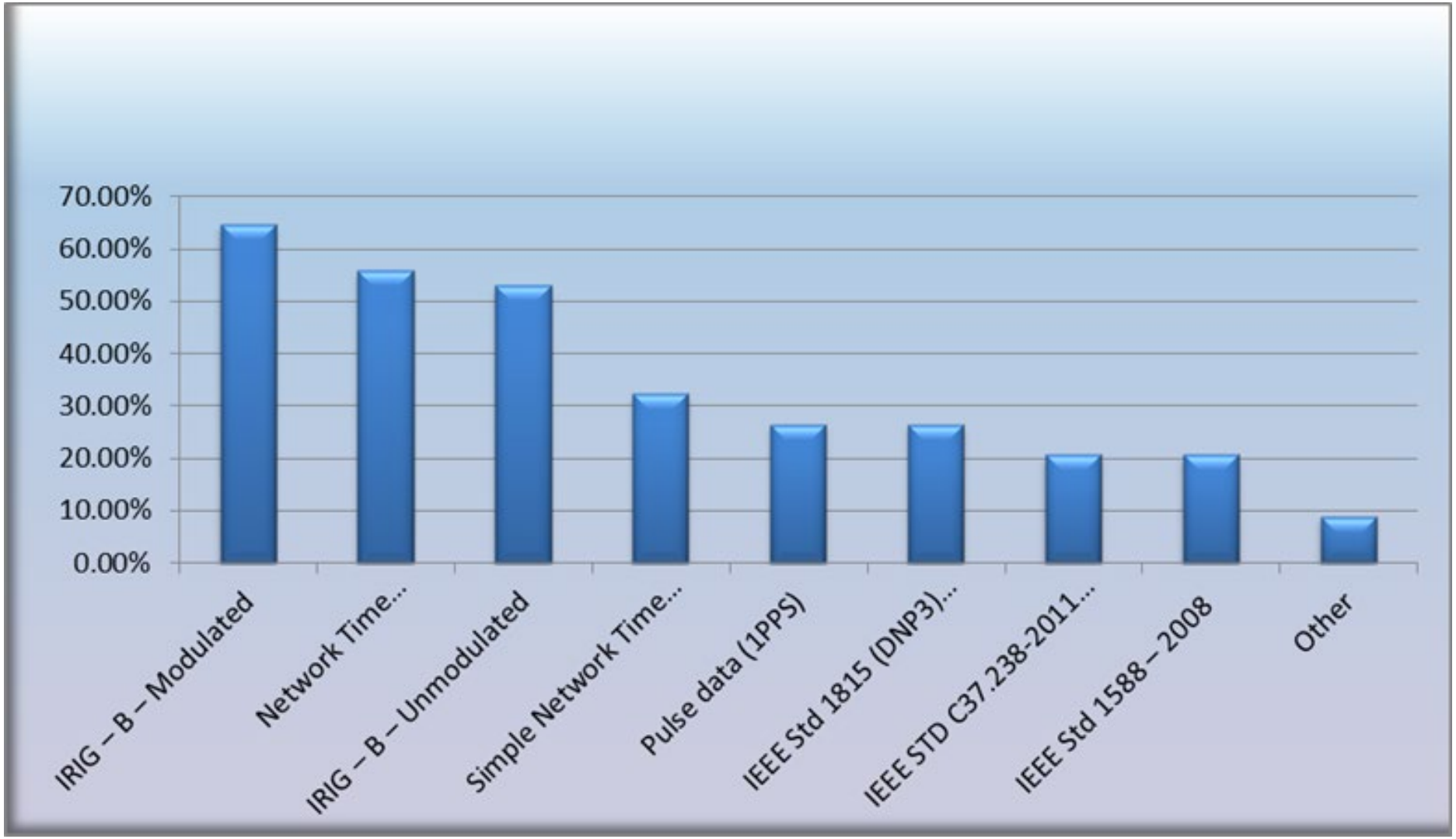
Utility Data Spans a Wide Time Scale



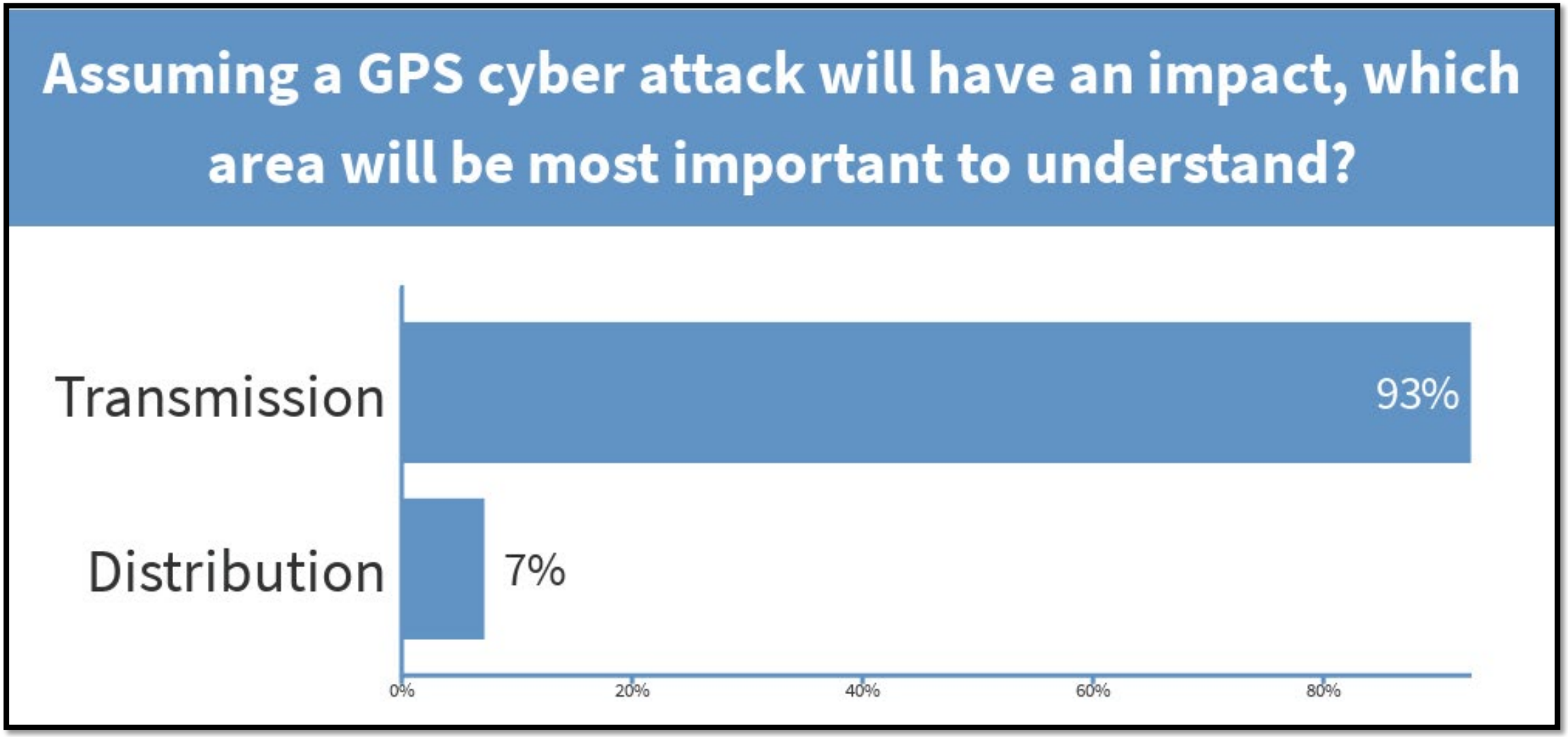
Additional assets planned for connection to the precision time source in the next 5 years



Time distribution protocols / signals currently used



EPRI Meeting Poll – Cyber Security Tech Transfer 2018



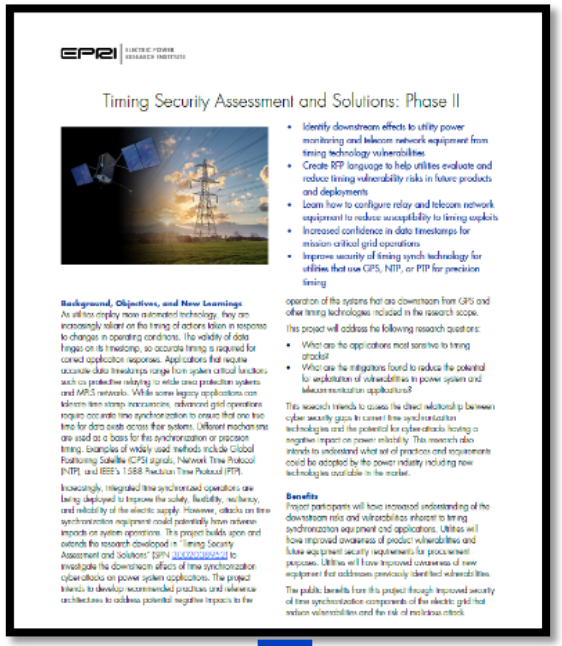
Industry Trends

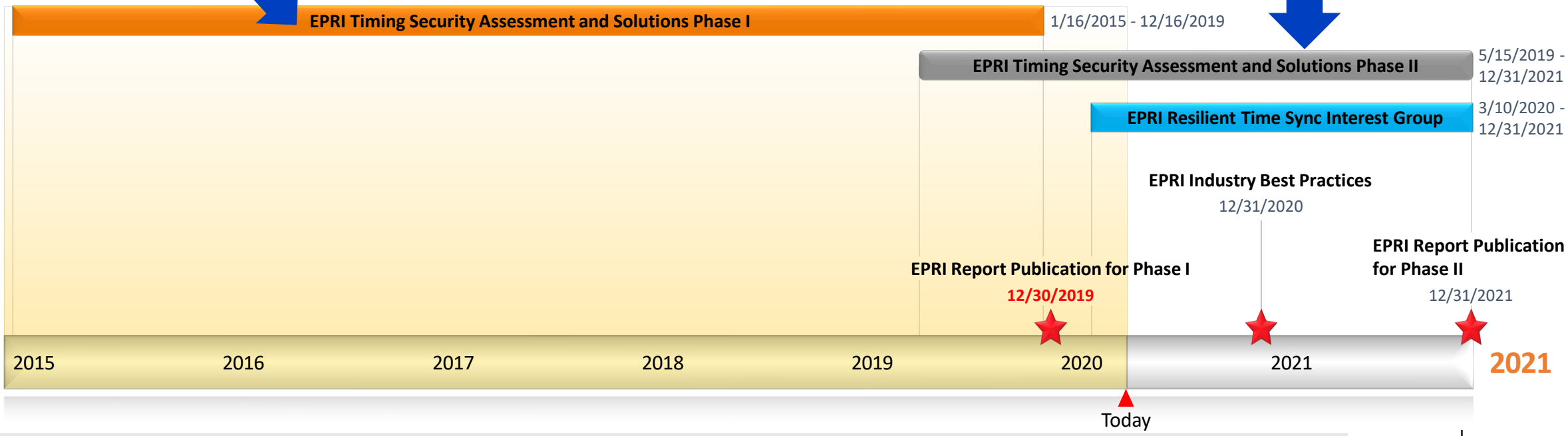
Based on the survey we identified the following trends:

- Over the next five years there is a significant planned increase in the use of the network based precision time protocol (PTP) as defined in IEEE Std c37.238 and IEEE Std 1588.
- Utilities moving away from SONET technologies and incorporating packet based technologies
- Many utilities plan to increase the use of precision time over the next five years for synchrophasor measurement, network routers, network switches, asset health monitors, inverters and security systems.

Resilient Timing Research


Timing Security Assessment and Solutions


Timing Security Assessment and Solutions: Phase II



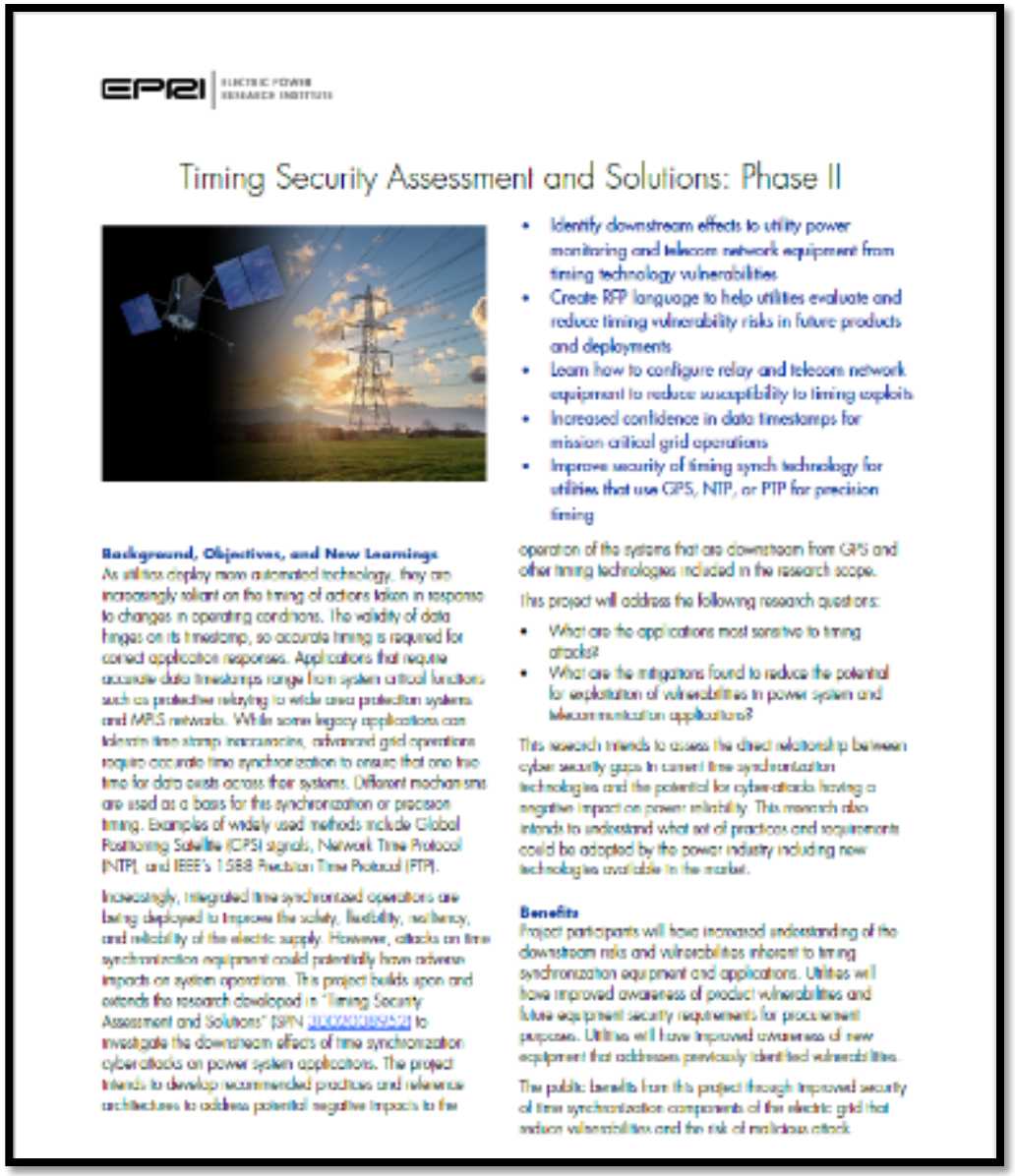
Time Security Assessment and Solutions Project Information

Phase I (2016-2019)

Project Abstract Link:
https://www.epri.com/#/pages/product/3002008952

Phase II (2019-2020)

Project Abstract Link:
https://www.epri.com/#/pages/product/3002016546/



EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Timing Security Assessment and Solutions: Phase II

- Identify downstream effects to utility power monitoring and telecom network equipment from timing technology vulnerabilities
- Create RFP language to help utilities evaluate and reduce timing vulnerability risks in future products and deployments
- Learn how to configure relay and telecom network equipment to reduce susceptibility to timing exploits
- Increased confidence in data timestamps for mission critical grid operations
- Improve security of timing synch technology for utilities that use GPS, NTP, or PTP for precision timing

Background, Objectives, and New Learnings

As utilities deploy more automated technology, they are increasingly reliant on the timing of actions taken in response to changes in operating conditions. The validity of data hinges on its timestamp, so accurate timing is required for correct application responses. Applications that require accurate data timestamps range from system critical functions such as protective relaying to wide area protection systems and MRLS networks. While some legacy applications can tolerate time stamp inaccuracies, advanced grid operations require accurate time synchronization to ensure that one true time for data exists across their systems. Different mechanisms are used as a basis for this synchronization or precision timing. Examples of widely used methods include Global Positioning Satellite (GPS) signals, Network Time Protocol (NTP), and IEEE's 1588 Precision Time Protocol (PTP).

Increasingly, integrated time synchronized operations are being deployed to improve the safety, flexibility, resiliency, and reliability of the electric supply. However, attacks on time synchronization equipment could potentially have adverse impacts on system operations. This project builds upon and extends the research developed in "Timing Security Assessment and Solutions" (SPN [illegible]) to investigate the downstream effects of time synchronization cyber attacks on power system applications. The project intends to develop recommended practices and reference architectures to address potential negative impacts to the operation of the systems that are downstream from GPS and other timing technologies included in the research scope.

This project will address the following research questions:

- What are the applications most sensitive to timing attacks?
- What are the mitigations found to reduce the potential for exploitation of vulnerabilities in power system and telecom communication applications?

This research intends to assess the direct relationship between cyber security gaps in current time synchronization technologies and the potential for cyber-attacks having a negative impact on power reliability. This research also intends to understand what set of practices and requirements could be adopted by the power industry including new technologies available in the market.

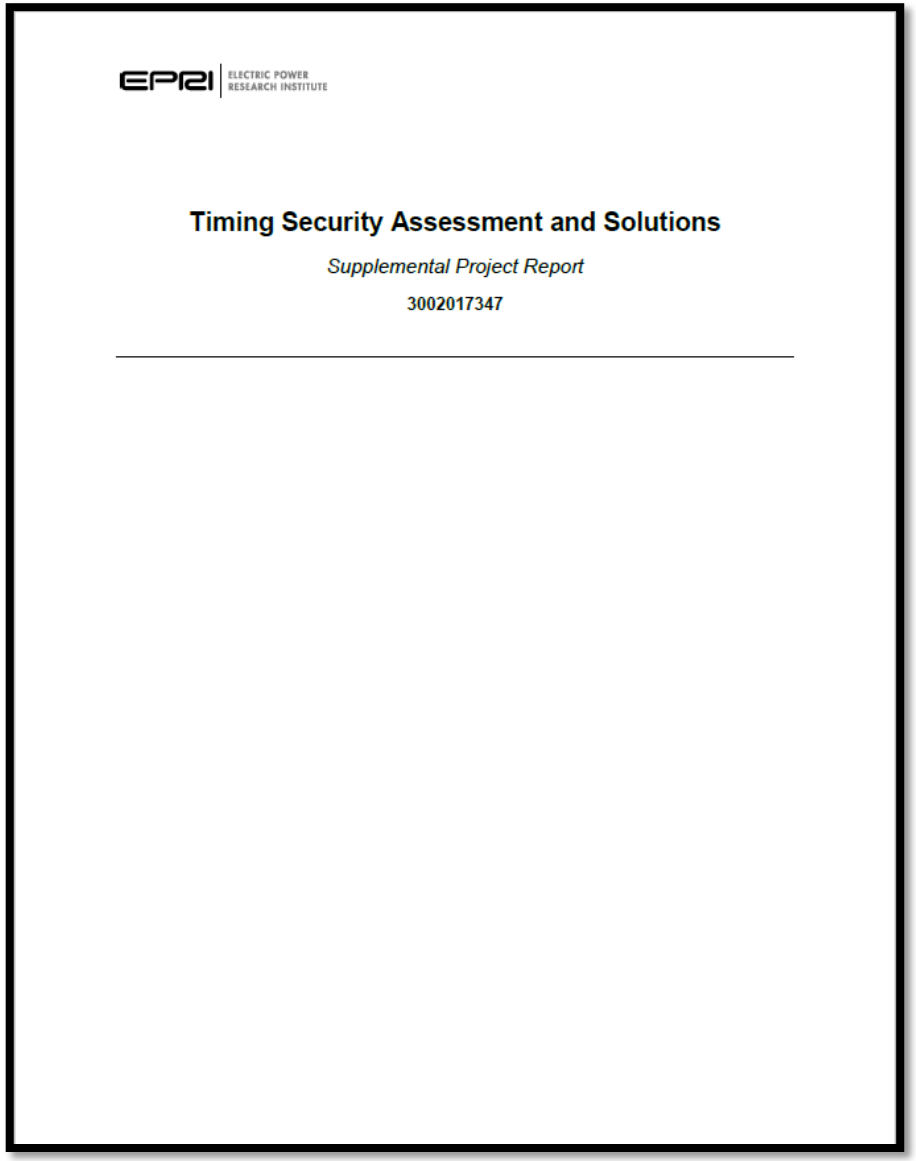
Benefits

Project participants will have increased understanding of the downstream risks and vulnerabilities inherent to timing synchronization equipment and applications. Utilities will have improved awareness of product vulnerabilities and future equipment security requirements for procurement purposes. Utilities will have improved awareness of new equipment that addresses previously identified vulnerabilities.

The public benefits from this project through improved security of time synchronization components of the electric grid that reduce vulnerabilities and the risk of malicious attack.

Timing Security Assessment Report

- Product ID: 3002017347
- **KEY FINDINGS**
  - Future systems that rely on time synchronization must be evaluated against attack vectors before deployment. This evaluation can occur in parallel to performance testing.
  - **LIMITED TO PROJECT FUNDERS**


EPRI ELECTRIC POWER RESEARCH INSTITUTE

Timing Security Assessment and Solutions

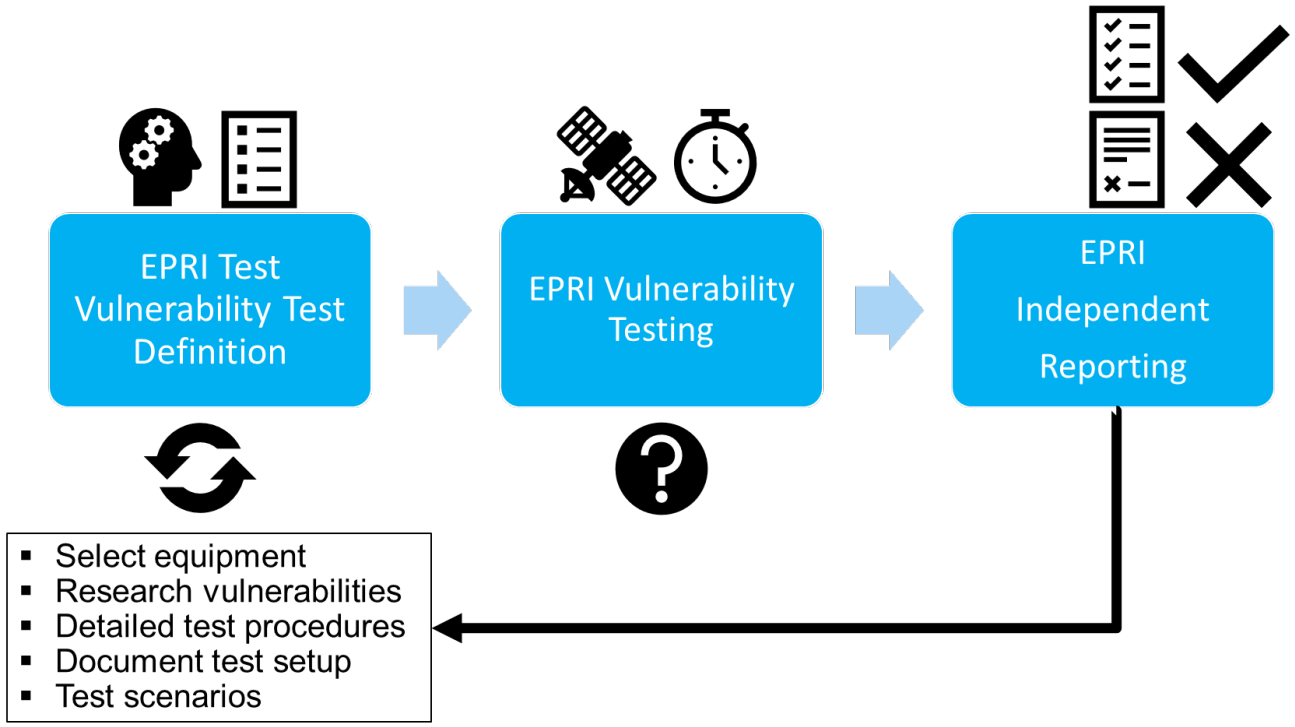
Supplemental Project Report

3002017347

Phase II Project Approach

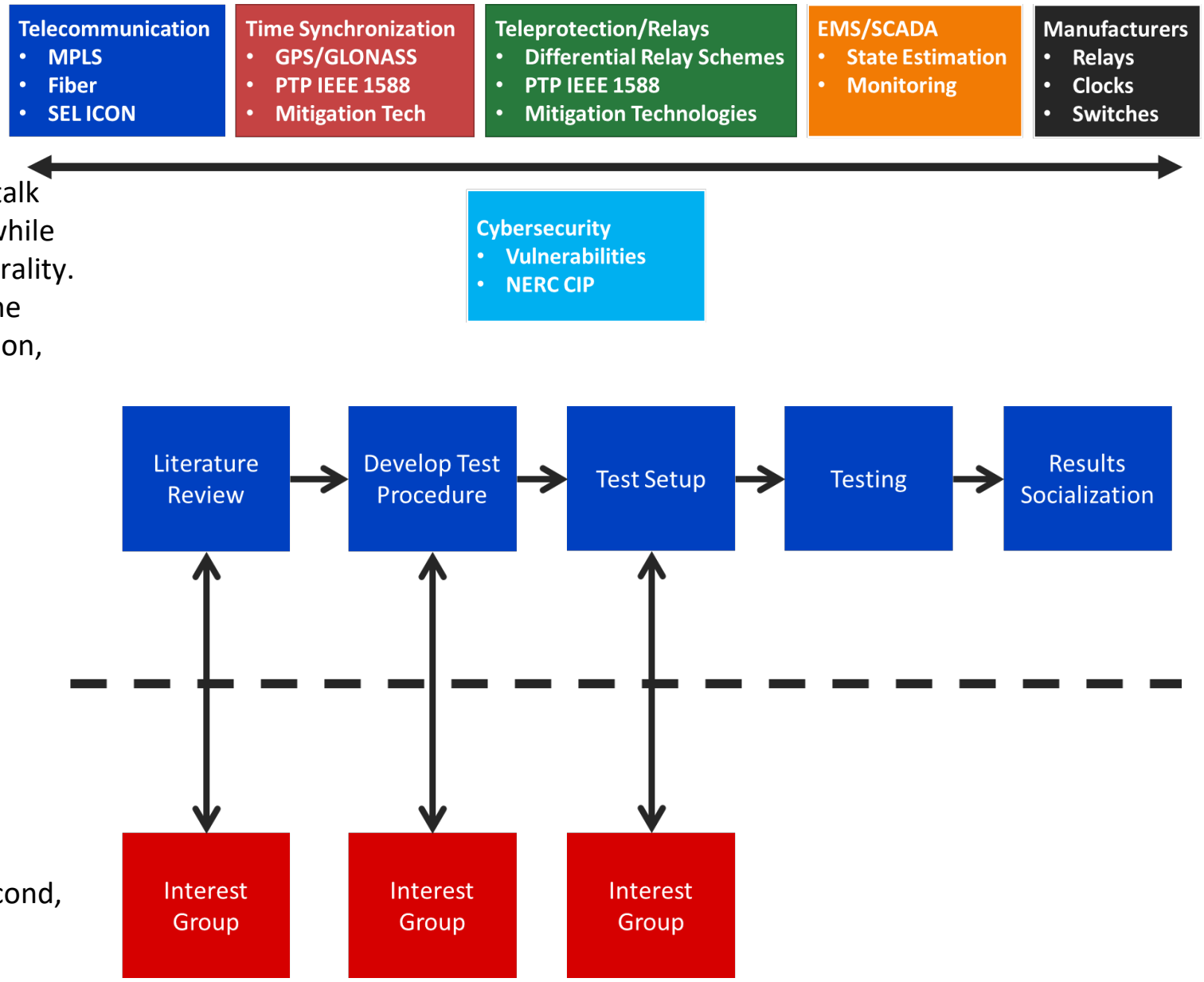
There are six (6) tasks planned for this project:

1. Review publicly available literature in relation to time synchronization vulnerabilities, technologies, and future states to help inform test plan development. Review will be summarized in the final report
2. Develop a test procedure document (to be included in report)
3. Implement a test setup in EPRI's Knoxville Cyber Security Laboratory or the project funder lab
4. Perform tests according to test procedure
5. Develop final report
6. Project management and socialization

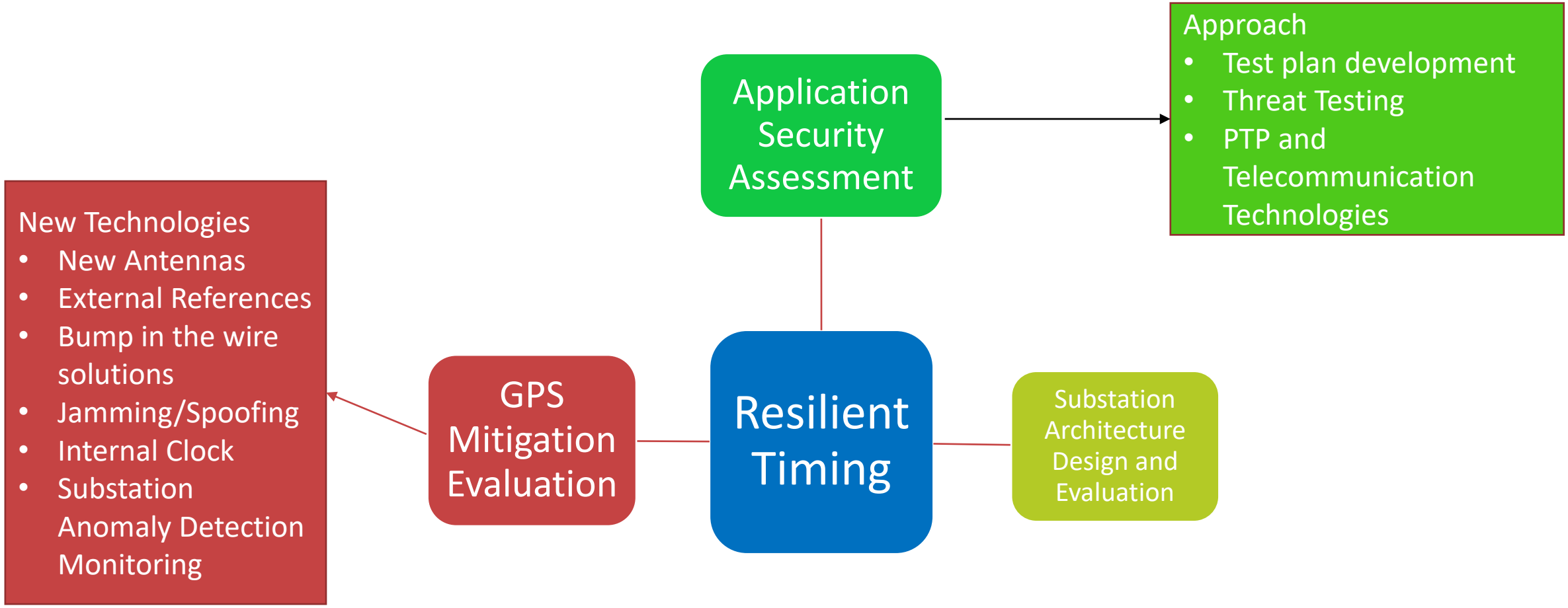


Resilient Time Synchronization for the Energy Sector Interest Group

- **Objective**
  - Create a virtual forum for utilities to share experiences, talk about tools and techniques and explore research topics while maintaining impartiality, independence, and vendor neutrality. EPRI provides this forum without charge as a service to the industry and to promote the importance of reliable position, navigation and time (PNT) data in the energy sector.
- **Who Should Participate?**
  - Anyone who works with PNT or depends on PNT data
  - Utilities, vendors, governmental and industry groups
- **Structure of meetings**
  - Time: 1-hour total
    - One (1) Vendor/Academic presentation and Q&A
    - One (1) Industry Update and Q&A
    - Related announcements (i.e. issues, events, leap second, best practices events etc.)



Phase II - Tasks preliminary direction



Next Steps

- EPRI intends to evaluate mitigation technologies and develop test plans according to technology approaches (i.e. antennas, GPS backup etc)
- EPRI intends to evaluate applications that may be impacted by time synchronization errors
- EPRI intends to test 2020-2021

Together...Shaping the Future of Electricity

Gerardo Trevino
Technical Leader
Cybersecurity