Technology Innovation Project

Closing Project Brief

TIP 366: EPRI P183 Supplemental Project: Precision Timing Security Assessment

Context

As utilities install more automated technology in their electric grid deployments, they become increasingly reliant on the timing of actions taken in response to changes in operating conditions. The validity of data often hinges on its time stamp, so accurate timing can reduce spurious data collection and transmission. Advanced grid operations require accurate synchronization to ensure one true time for data exists across the system. Different mechanisms are used as a basis for this synchronization or precision timing. Examples of widely used methods include global positioning system (GPS) signals, Network Time Protocol (NTP), and the IEEE 1588 Precision Time Protocol (PTP).

Increased reliance on timing synchronization comes with risks. A number of utilities, labs, and academic institutions have researched and confirmed vulnerabilities in precision timing that may pose risks to applications used in operations that rely upon highly accurate timing. The potential risks associated with exploitation of these vulnerabilities are unclear and may vary across different utilities.

In addition to this lack of clarity for potential risks created by precision timing vulnerabilities, there is also an absence of field-tested and proven mitigations for many of these vulnerabilities. Existing research on mitigations for vulnerabilities of applications dependent upon precision timing has been, for the most part, confined to the theoretical, and their effectiveness in utility environments has not been widely established.

Description

There were three task focus areas related to security for synchronized operations in electric sector deployments:

1. ***Vulnerability Identification*** – EPRI documents vulnerabilities that exist, their pervasiveness in deployed equipment, and techniques for identifying the vulnerabilities. Results of this task include guidance on testing for the vulnerabilities in existing equipment.
2. ***Potential Risk Assessment*** – EPRI analyzes and prioritizes potential risks to power delivery systems if identified vulnerabilities are exploited.
3. ***Vulnerability Mitigation*** – The final project objective identifies and tests potential mitigations for the vulnerabilities identified. The results of the testing, as well as mechanisms for evaluating the test results, are provided to the project members.

Benefits

This project is a progressive approach for addressing cyber security vulnerabilities in precision timing systems used in mission-critical utility operations. The results provide significant power industry and public benefits, particularly focused on improved power grid reliability and resiliency.

Increasingly integrated synchronized operations lead to improved safety, flexibility, and reliability of the electric supply. The project results help build confidence in sources of sensor data, such as smart inverters, and enable optimal, autonomous management of distributed energy resource (DER) assets in utility grids.

Accomplishments

The results of this project were able to determine:

- What equipment is deployed to provide timing synchronization vulnerable to attacks that could impact synchronized operations?
- What the potential level of risk to power delivery systems for identified equipment vulnerabilities.
- What mitigations are available to reduce the potential for exploitation of vulnerabilities in power systems. And, what is required to implement those mitigations?

Deliverables

The project reported on the presence of vulnerabilities in products used for timing synchronization in the electric sector. Specific deliverables include:

• Report on the presence of vulnerabilities in products used for timing synchronization in the electric sector. Including guidance on testing that can be conducted independently.

• Report on the potential risk of identified vulnerabilities to power delivery systems or operational disruptions in electric sector deployments.

• Guidance for selecting equipment and adopting practices deploying mitigations that will reduce the likelihood of malicious manipulation of system timing infrastructure.

TIP 366: EPRI P183 Supplemental Project: Precision Timing Security Assessment

Project Start Date: May 2016

Project End Date: July 2019

Report

Timing Security Assessment and Solutions
EPRI Supplemental Project Report
3002017347 (available to at www.epri.com)

For More Information Contact:

Technology Innovation Office:
TechnologyInnovation@bpa.gov

Participating Organizations

Electric Power Research Institute (EPRI)
San Diego Gas & Electric,
Southern Co,
Pacific Gas and Electric (PG&E),
Duke Energy,
Salt River Project

Conclusions (from EPRI Supplemental Project Report 3002017347)

RESEARCH OVERVIEW

The project team worked closely to identify the cybersecurity exploits that could be used to test applications that depend on time synchronization. With the support of experts and utility staff and resources in the form of knowledge, laboratories and equipment the project team was able to perform real time hardware in the loop (RT-HiL) testing.

KEY FINDINGS

- All GNSS clocks tested demonstrated vulnerabilities and exploits that could be used against downstream devices that rely on accurate time data.
- Applications tested under this project demonstrated negative impacts to their operation but the complexity to this statement is heavily dependent on exactly how the application is constituted, configured and managed.
- Technologies that claim to protect against some of the known vulnerabilities are still vulnerable. It will become harder to evaluate the effectiveness of mitigations as the level of complexity of some of the devices will increase from current technologies deployed in the field.
- Future systems that rely on time synchronization must be evaluated against attack vectors before deployment. This evaluation can occur in parallel to performance testing.

WHY THIS MATTERS

The energy industry heavily relies and will continue to rely on time synchronization technologies. A coordinated cyber-attack against time synchronization systems could disrupt the operation of applications sensitive to the vulnerabilities found in this research.

HOW TO APPLY RESULTS

Utilities should understand the systems and applications that rely on time synchronization. Utilities should work with EPRI and the industry to evaluate their systems as needed and to engage in the discussion on how to implement mitigation techniques and system design guidelines to prevent mis-operations. Utilities should implement a cybersecurity strategy to reduce the impact of cyber-attacks on GNSS equipment. This strategy should address mechanisms to detect, protect, identify, respond and recover.