Precision Timing Use Cases for Transmission and Distribution Grid Operation

Special Protection Scheme System Stability and 61850 Compromised Time Use Cases—Final Report Prepared for Pacific Northwest National Laboratory

2022 TECHNICAL REPORT

Precision Timing Use Cases for Transmission and Distribution Grid Operation

Special Protection Scheme System Stability and 61850 Compromised Time Use Cases—Final Report Prepared for Pacific Northwest National Laboratory

3002025563

Final Report, October 2022

EPRI Project Manager
C. Hertzog

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

EPRI PREPARED THIS REPORT.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Together…Shaping the Future of Energy®

ACKNOWLEDGMENTS

EPRI prepared this report.

Principal Investigator
C. Hertzog
J. Stewart
G. Drewry

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Precision Timing Use Cases for Transmission and Distribution Grid Operation: Special Protection Scheme System Stability and 61850 Compromised Time Use Cases—Final Report Prepared for Pacific Northwest National Laboratory. EPRI, Palo Alto, CA: 2022. 3002025563.

ABSTRACT

Precision timing vulnerabilities in different time sources and technologies can impact grid operations. The full range of impacts is not fully understood for transmission grids and is only beginning to be explored in distribution grids. This research project created two use cases; one each for Transmission and Distribution Operations to highlight potential vulnerabilities that may now be addressed through testing to determine if time source compromises produce the anticipated impairments and then develop mitigation actions for any identified vulnerabilities.

Keywords

Cyber security
GPS
Precision timing

Deliverable Number: 3002025563

Product Type: Technical Report

Product Title: Precision Timing Use Cases for Transmission and Distribution Grid Operation: Special Protection Scheme System Stability and 61850 Compromised Time Use Cases—Final Report Prepared for Pacific Northwest National Laboratory

---

PRIMARY AUDIENCE: Protection and control engineers, cyber security resources, system operators

KEY RESEARCH QUESTION

Precision timing vulnerabilities in different time sources and technologies can impact grid operations. The full range of impacts is not fully understood for transmission grids and is only beginning to be explored in distribution grids. This research project created two use cases – one each for transmission and distribution operations to highlight potential vulnerabilities that may now be addressed through testing to determine if time source compromises produce the anticipated impairments and then develop mitigation actions for any identified vulnerabilities.

RESEARCH OVERVIEW

The vulnerabilities of technologies that deliver precision timing to applications and systems in the electricity subsector are becoming more publicized, but still trigger skepticism among some electric sector stakeholders. Any dismissal of potential threats can lead to unintended consequences of loss of electricity services, longer restoration times, and threats to health and safety. Use cases are a powerful way to illustrate anticipated degradations in services caused by precision timing source compromises. The two use cases described here – one for transmission grid operations and one for distribution grid operations – help identify potential impairments to operations and offer a logical test plan to determine if anticipated problems do surface, and consistent approach to identify mitigations to precision timing risks.

KEY FINDINGS

- Use cases offer "what-if" scenarios to test with different precision timing solutions in laboratory settings
- Communications protocols like 61850 will require more investigation to ensure that all potential vulnerabilities that could impact grid operations are identified so risks can be understood and mitigations can be developed

WHY THIS MATTERS

Precision timing vulnerabilities in different time sources and technologies can impact grid operations. The full range of impacts is not fully understood for transmission grids and is only beginning to be explored in distribution grids.

HOW TO APPLY RESULTS

These two use case results can now be tested in laboratory settings to confirm or disprove the expected impacts to normal operations. While timing dependencies in transmission operations have been studied for some time, the growing adoption of time-dependent applications in distribution operations increases the need for research to identify any precision timing vulnerabilities and develop risk mitigations. As 61850 is adopted in digital substation deployments, more use cases should be developed and tested and information should be shared with the electricity sector.

LEARNING AND ENGAGEMENT OPPORTUNITIES

- The use cases serve to inform vendor product plans, utility procurement plans, industry association actions, standards development organizations, and governmental agencies actions regarding precision timing resiliency for critical infrastructure.

EPRI CONTACTS: C. Hertzog, Principal Project Manager, chertzog@epri.com

PROGRAM: P183: Cyber Security for Power Delivery and Utilization

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

ACRONYMS

BES	Bulk Electric System
BRKR	Breaker
CC	Control Center
CIP	Critical Infrastructure Protection
DOE	Department of Energy
GNSS	Global Navigation Satellite System
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
HMI	Human Machine Interface
IED	Intelligent Electronic Device
IEEE	International Electrical and Electronics Engineers
LSE	Load Serving Entity
MMS	Multimedia Messaging Service
MPLS	Multi-Protocol Label Switching
NASPI	North American SynchroPhasor Initiative
NERC	North American Electric Reliability Corporation
PMU	Phasor Measurement Unit
PNNL	Pacific Northwest National Laboratory
PTP	Precision Time Protocol
SCADA	Supervisory Control and Data Acquisition
SV	Sample Value
UTC	Coordinated Universal Time
WAMS	Wide Area Monitoring System
WAN	Wide Area Network

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

The vulnerabilities of technologies that deliver Position, Navigation, and Timing (PNT) sources to the electricity subsector are becoming more publicized, but still trigger skepticism among some electric sector stakeholders. EPRI published the Roadmap For Resilient Positioning, Navigation And Timing (PNT) For The Electricity Subsector[1] in December 2020 to highlight vulnerabilities and impacts on grid operations. Ongoing EPRI research results show that precision timing provided by GPS sources is vulnerable to modifications caused by malicious and inadvertent attacks. Multiple entities including the Pacific Northwest National Laboratory (PNNL) and the Department of Energy (DOE) are investigating precision timing. Other stakeholders such as standards development organizations and the North American SynchroPhasor Initiative (NASPI) also participate in activities to identify risks and mitigations to precision timing in critical infrastructure like electric grids.

This stakeholder community benefits from descriptions of realistic grid operations scenarios that rely on precision timing. Use cases can identify weaknesses and gaps in technologies. Use cases can emphasize the need for standards to resolve issues. Use cases can form the basis of research and tests to help explore the impacts and mitigations of timing failures. These are the research drivers that created this project focused on documenting two use cases for precision timing in utilities.

[1] https://www.epri.com/research/products/000000003002020266

2 METHODOLOGY AND PARTICIPANT OVERVIEW

The project scope was discussed between PNNL and EPRI resources at the project start. The team recognized the importance of recruiting utilities and vendors of timing technologies to assist in the use case development to ensure realistic scenarios were described. With that objective in mind, the project was defined by 3 main tasks:

1. Volunteer recruitment
2. Use case development
3. Use case documentation

Volunteer participation from industry stakeholders was critical to the success of this project. Volunteers from the international stakeholder community were recruited through EPRI's Resilient PNT Interest Group and member utilities; NASPI; IEEE; and various industry publications. Volunteer recruitment kicked off at a Resilient PNT Interest Group webcast in 2021 and continued with email recruitment to the NASPI member list, the Resilient PNT Interest Group member list, and outreach to EPRI's member list.

There were 81 total participants representing 16 electric utilities and independent system operators; 6 universities; 13 vendors and consultants; and 5 research entities participating in the workshops and contributing ideas and feedback crucial to the development of the use cases.

Two use cases were developed in this project. The use case topics were suggested by EPRI researchers in consultation with PNNL to cover both transmission and distribution precision timing scenarios. Timing dependencies are more well-known and documented in transmission operations, but the growing adoption of time-dependent applications in distribution operations increases the need for awareness of precision timing vulnerabilities and risks. The final use cases were identified by group consensus in the first workshops. Each use case was assigned an EPRI lead researcher.

A use case template was proposed to PNNL and approved by them. The template delivers different perspectives on the use case. It includes a high-level flow of the action, the stakeholder roles (which in this setting can mean devices or systems in addition to people), detailed activities at operational and network levels, and regulatory requirements. Then the normal, uncompromised functions are sequentially described. The final section of the use case introduces compromised time signals into these operations and describes expected impacts. These results can now be tested in laboratory settings to confirm or disprove the expected impacts to normal operations.

The impacts also consider the Department of Homeland Security resiliency impacts[2] to further inform research priorities. These levels are briefly described as:

- Level 0: non-resilient because it may accept unverified inputs or requires manual intervention if damaged
- Level 1: ensures recoverability after removal of a threat
  - Includes ability to securely reload or update firmware, support full system recovery by manual means, and verify that stored data from external sources adheres to established standards
- Level 2: Provides a solution during threat
  - Includes all Level 1 plus must identify compromised PNT sources and prevent their inputs for PNT, and supports auto recovery of individual PNT sources and systems
- Level 3: Provides a solution (with bounded degradation) during threat
  - Includes all Level 2 plus ensures that one corrupted PNT data source cannot contaminate another PNT data source and cross-verifies between PNT solutions from all PNT sources
- Level 4: Provides a solution without degradation during threat
  - Includes all Level 3 plus a diversity of PNT source technologies to mitigate common mode threats

Each use case considered these impacts in the compromised time scenarios. However, detailed resiliency assessments will require testing with different vendor timing technologies to fully determine the variations in recovery speeds in the event of compromise.

The lead researchers developed the content for their respective use cases based on the template. Content development included queries to subject matter experts within EPRI and the volunteer list, online research, and internal discussions. The use case content was then reviewed in a second webcast with the volunteers. This webcast-based review offered volunteers the opportunity to provide feedback in the form of edits and additional content to improve the clarity and accuracy of the use case descriptions.

The concluding task is creation of this report in a document format and a summary presentation.

Use Case 1: Special Protection Scheme System Stability

There were several interesting scenarios in the bulk electric system (BES) but after discussion with the volunteers involved in this project, a realtime operations scenario was selected to highlight the immediate impacts that could be anticipated in this type of cyberattack. This use case examined a realtime wide area monitoring systems (WAMS) application for transmission operations in electric utilities. It focused on the ability to manipulate time for phase angle measurements.

[2] https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf

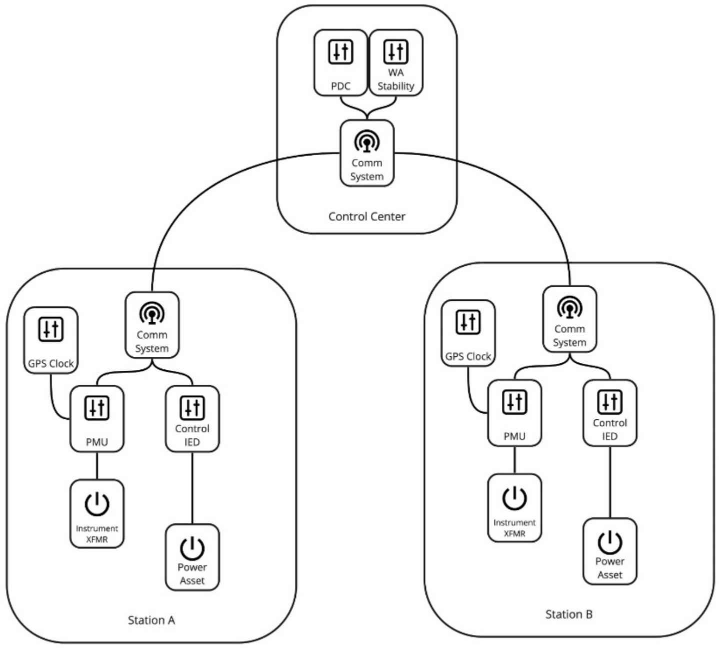

Figure 2-1
Wide Area Monitoring

Certain assumptions were made in this use case:

- WAMS is hosted locally on a phasor data concentrator
- GPS reference is spoofed
- Synchrophasor data from multiple geographically distributed PMUs is aggregated.
- Measurements are aligned using received time stamps.
- Wide Area stability application continuously analyzes aligned data (eg phase angle delta) to identify grid stability event.
- When pre-determined threshold is crossed, control action is initiated to alter grid topology.

The use case consists of a series of tables with content that reflects the stakeholders, influences, and actions for the WAMS scenario in normal and compromised operations.

Stakeholder Matrix

This table identifies the systems, devices, and people engaged in the WAMS scenario. The Phasor Measurement Unit or PMU is high speed compared to SCADA systems and offers a granular look at power system stability. The Phasor Data Collector or concentrator gathers data from multiple PMUs. GPS receiver clocks are assumed to be external clocks and not embedded into any particular device, distributing timing signals to all devices that require it.

Table 2-1
Stakeholder Matrix

Stakeholder	Type (Resource, system, application, device, database)	Description	Notes
Phasor Measurement Unit	Device	Connect to power grid secondary signals (from instrument transformers) to sample and report measurements at a high rate.	Initial synchrophasor projects relied on dedicated PMU platforms. Over time, PMU functionality has been integrated into multipurpose protection devices.
Phasor Data Collector	Device, application, database	Aggregates measurement streams from multiple PMUs for analysis and forwarding to other applications	PDC aligns measurements based on received time stamp. Some measurements may be disregarded if time stamp diverges too far from expected.
Communications Network	Resource, system	Transport phasor data from PMUs to PDCs and to grid applications	Network must exceed performance requirements for synchrophasor applications
GPS receiver/clock	Device	Local time reference provided by GPS clock at each PMU location	Time synchronization is performed locally using IRIG-B or IEEE 1588 PTP
Wide Area Protection Application	Application	Receives phasor data that has been aligned by PDC, performs analysis, and initiates protection response if warranted	In this scenario, the application is hosted on the PDC
Control IED	System	Receives protection response and operates pre-determined power system assets to mitigate stability issues	Includes communication and local control devices

Technical Step by Step Table

The technical step by step table identifies how the devices interact in normal operations, in this case, stability of the transmission grid. Clocks are geographically distributed and produce a local time signal. IRIG B is one approach that may offer precision, but other time distribution mechanisms, such as PTP may be used. PMUs receive the timing signal from the clock to synchronize its own internal time and tag data for their streaming data that is transmitted to PDCs.

Table 2-2
Technical Step by Step

Stakeholder/Type		Pre-condition	Assumption
GPS Clock (multiple geographically distributed)		Clock determines UTC time and distributes to local PMU	Satellite constellation visible (minimum # required)
Phasor Measurement Units (multiple geographically distributed)			Assumes accurate individual measurements, calibration
Communications Network			Provides data transport while meeting necessary SLA requirements for intended application (latency, jitter, bandwidth, etc..)
Phasor Data Concentrator		Receives phasor data from multiple measurement points at different locations across the grid	Measurements are aligned using embedded time tags to ensure proper reassembly for analysis
Wide Area Protection Application (Hosted on phasor data concentrator)		Receives phasor data from multiple phasor data concentrators located in different regions of the system	Accurate system models and pre-defined control actions for specific grid conditions
Communications Network			Provides data transport while meeting necessary SLA requirements for intended application (latency, jitter, bandwidth, etc..)
Control IED		Wide Area Protection Application has identified specific conditions and initiates a control action	Targeted operation time 2-10 msec after stability event is identified

Data Dependencies Table

The data dependencies table identifies the applications and devices that are dependent on precision time for optimal performance. Inaccurate timing can trigger inaccurate time tags on data. PDCs have limited dependency, because their operations do not require accurate local time from a GPS clock. Data with inaccurate time tags will be disregarded. Similarly, control IEDs that receive inaccurate time signals may cause some regulatory issues.

Table 2-3
Data Dependencies

Computer/system/application activity	Dependency on precision time?	Description	Notes
GPS Clock (multiple geographically distributed)	Yes	Receives RF input from satellite constellation	
Distributes time reference to local phasor measurement units			
Phasor Measurement Units (multiple geographically distributed)	Yes	Receives time reference from local GPS clock. Time stamps local measurements before transmission to upstream phasor data concentrator.	
Phasor Data Concentrator (with System stability application)	Limited	Local PDC time reference should not impact control decisions. Only relative time difference at different PMU locations	

Regulatory Requirements Table

The regulatory requirements table starts with NERC CIP requirements. The low and medium requirements were not examined in great detail, putting more focus in this project on the high criticality assets in the control center to address realtime operations. The last entry for disturbance monitoring is included because precision timing is important to ensure accurate data for forensics analysis of incidents. NERC PRC 002 requires that timestamp accuracy must be within plus or minus 2 milliseconds of UTC.

Table 2-4
Regulatory Requirements

Entity	Mandatory compliance?	Description	Notes
Utility (NERC Registered Entity) – CIP Low Facilities	Yes	Includes PMUs at substations that are classified as CIP Low	Assumes PMU application has real-time (<15 minute) impact to the bulk electric system
Utility (NERC Registered Entity) – CIP Medium Facilities	Yes	Includes PMUs at substations that are classified as CIP Medium	Assumes PMU application has real-time (<15 minute) impact to the bulk electric system
Utility (NERC Registered Entity) – CIP High Facilities	Yes	Includes control center applications such as wide area protection and phasor data concentrators within control center	
Utility (NERC Registered Entity) – Disturbance Monitoring	Yes	Defines precision and accuracy requirements for event records (NERC-PRC)	PRC-002 Disturbance Monitoring and Reporting Requirements

Operations Step by Step – Normal Operations

This description maps out an automated sequence. The GPS clock distributes time references to PMUs, and the aggregated data streams are collected by PDCs. The PDCs may disregard phasor data that is outside of certain tolerance boundaries. This leads to a “sweet spot” for time variance that may impact operations. The C37.118 standard is widely adopted and was used for this scenario.

Table 2-5
Normal Operations Step by Step

Stakeholder	Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged
GPS Clock (multiple geographically distributed)	1	Acquire GPS reference	Local time acquisition and distribution (multiple locations)	GPS Clock	Phasor Measurement Unit	Local time

Table 2-5 (continued)
Normal Operations Step by Step

Stakeholder	Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged
Phasor Measurement Units (multiple geographically distributed)	2	Synchronize PMU	Synchronize PMU clock with local reference signal (multiple locations)	GPS Clock	Phasor Measurement Unit	Internal PMU samples – time tagged
Phasor Data Concentrator	3	Aggregate PMU streams	Receive PMU data from various measurement points and align using time tags	PMU (multiple locations)	Phasor Data Concentrator	PMU samples (C37.118)
Wide Area Protection Application (Hosted on phasor data concentrator)	4	Identify stability event	Respond based on pre-defined grid stability scenarios	Phasor Data Concentrator	Wide Area Protection Application	
Control IED	5	Reconfigure power system	Operate local breakers/switches to reconfigure grid topology	Wide Area Protection Application	Control IED	Control message (C37.118)

Step by Step Operations – Compromised Time

If the GPS time reference is compromised, the automated step by step reflects the same steps, but with different outcomes. The PMUs receive inaccurate time references, leading to a misalignment of measurements. The PDC will attempt to align measurements (as long as the inaccuracy doesn't trigger outright rejection of data), and the wide area protection application can then issue commands to control IEDs that impact grid stability. It is not difficult to manipulate time but organizing an attack that would be able to manipulate timing without triggering PDC rejection of bad data would require some sophistication. It may be an attack that needs insider information to be most impactful, but an attack could cause some damage to equipment. This scenario can also occur through technology failures—a clock mis-operation can initiate a similar sequence of actions.

Resiliency impacts could not be determined at the use case level without testing conducted with different vendor systems and configurations to assess speed of recovery and other restoration activities. For instance, one vendor's GPS clock may have different recovery capabilities than another vendor's GPS clock. Definitive conclusions would require each use case to be decomposed at a granular stakeholder level and identify key components within systems to determine the resiliency level at any step of a use case.

Table 2-6
Compromised Operations Step by Step

Stakeholder	Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged	Impact to resiliency
GPS Clock (multiple geographically distributed)	1	Acquire Spoofed GPS reference	Local time acquisition and distribution of manipulated time	GPS Clock	Phasor Measureme nt Unit	Local time	Undetermin ed – variable recovery based on deployed component s and systems
Phasor Measurement Units (multiple)	2	Synchronize PMU	Synchronize PMU clock with manipulated time)	GPS Clock	Phasor Measureme nt Unit	Internal PMU samples – time tagged	Undetermin ed – variable recovery based on deployed component s and systems
Phasor Data Concentrator	3	Aggregate PMU streams	Receive PMU data from various measurement points and align using time tags (misaligned)	PMU (multiple locations)	Phasor Data Concentrato r	PMU samples (C37.118)	Undetermin ed – variable recovery based on deployed component s and systems
Wide Area Protection Application (Hosted on phasor data concentrator)	4	Identify stability event	Respond based on inaccurate phase shifts between measurement points	Phasor Data Concentrator	Wide Area Protection Application		Undetermin ed – variable recovery based on deployed component s and systems

Use Case 2: 61850 Compromised Time

There are many potential timing use cases in the distribution grid, but since 61850 is increasingly deployed in digital substations, the researchers decided to focus on this communications protocol to examine precision timing impacts and implications.

A 61850 substation with transmission and distribution assets is subjected to GNSS/GPS interference. The substation relies on two GPS-enabled clocks to provide redundant time synchronization information to all substation devices. The GPS clocks have limited internal capabilities to detect problems with GPS signals. Primary communications between the control center and the substation are delivered via MPLS over fiber. The station MPLS router is configured with the primary and secondary time sources set to the local GPS clocks. It is also configured with a tertiary time source of recovered PTP from an adjacent substation. The substation fiber connection represents a node in a fiber ring and rests between two other substation nodes on the ring. SCADA control between the substation and control center utilizes the MMS protocol. There is some routable GOOSE and sampled values (SV) between the substation and the adjacent substations and control center. A local firewall also receives time information from the local GPS clocks.

Both GPS clocks provide time to both the station bus and process bus to avoid the potential for failure of one clock causing a synchronization failure between the two buses. One clock is assumed to be a primary time source and the other is the redundant backup. PTP recovered across the network is a tertiary time source, but only used in the event of a complete loss of both local time references.

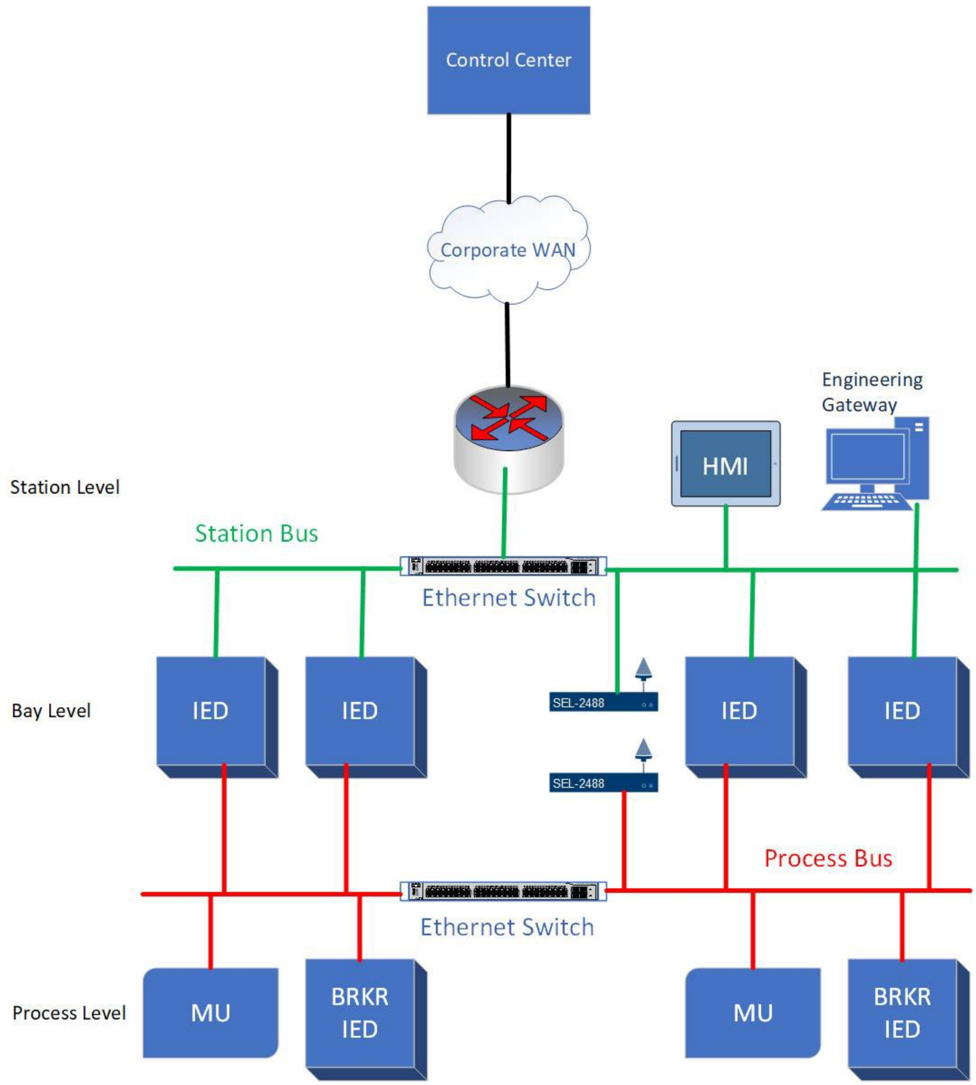

Figure 2-2
61850 Communications

The first scenario is that timing synchronization failure happens between the substation and all devices across the WAN when a utility operator attempts to operate a breaker using MMS. The GPS reference time clocks are both operational and reporting high accuracy but are being spoofed and the time reference no longer is in synchronization with UTC. Timing synchronization between the local devices in the substation is maintained.

The second scenario on local disparity is that timing synchronization failure happens between the station and process bus because these devices are synchronized to different time sources. One of the two reference clocks in the substation has a failure that results in loss of the GPS reference for timing synchronization. Misconfiguration or physical wiring problems result with the devices on the two buses using different reference clocks for timing synchronization.

Stakeholder Matrix

The stakeholder matrix is high level, focused on stakeholders that could have time sensitivities. SCADA is listed primarily because of the severity of potential impact if communications is interrupted or impacted. Transport systems carry different sensitivities to time synchronization issues. The emulation of TDM circuits across MPLS networks can be impacted if routers are not synchronized to a common reference. Handoff between adjacent SONET rings may be impacted if they don't have a common time reference. A number of newer clocks have advanced capabilities to use the recovered time from other geographically dispersed satellite clocks to identify sources that are out of synchronization with the rest of the network. Digital fault recorders and historians may not directly impact services but may make it difficult to align and understand what's going on when comparing data from multiple sites if the time stamps are not in synchronization.

Table 2-7
Stakeholder Matrix

Stakeholder	Type (Resource, system, application, device, database)	Description	Notes
SCADA	System	Supervisory control and data acquisition system	
Transport network system for WAN (MPLS, SONET, Carrier Ethernet, etc..)	System	Network transport between substation and other external entities	Routers for WAN access
IED	Device	IEDs used for monitoring, protection and control	
Merging Units	Device	Merging units used to aggregate data from CT, VTs, NCITs, etc. and transmit data to IEDs	Typically use SV
Satellite clocks	Device	GPS/GNSS enabled clocks for time reference and synchronization	Can act as PTP grandmaster clocks, some have advanced capabilities to detect time synchronization issues
Ethernet switches	Device	Ethernet switches for local substation communications	
Substation HMI	Application	Human machine interface for local visibility and control.	Localized SCADA terminal. May have security controls limiting local operations.

Table 2-7 (continued)
Stakeholder Matrix

Stakeholder	Type (Resource, system, application, device, database)	Description	Notes
Engineering Gateway	Device	Machine used as local/remote resource for engineering access to substation hardware (IEDs, etc.)	
Digital fault recorders and historians	Database	Stores copies of event data for later review	

Data Dependencies Table

The 87L functionality is well documented to be vulnerable to time synchronization failure. Previous EPRI research and demonstrations at member utilities in the presence of vendors have caused failures in the protection circuit when operating in channel-based mode. In that research, the network transport, an MPLS router, used a local GPS clock for time reference. When synchronization with the rest of the network was impaired, channel latency, jitter and packet loss began to occur. Time synchronization issues could also impact the ability for services requiring cryptographic handshakes to successfully establish a session.

Table 2-8
Data Dependencies

Computer/system/application activity	Dependency on precision time?	Description	Notes
IEDs	Yes	Relays and other intelligent electronic devices used for reporting, protection and control	Rely on time synchronization for accurate timestamping of data. Impact can vary depending on functions being performed by IED. 87L, Sample Measured Value (SMV), Synchrophasor, digital fault recorders all impact differently.
Transport Network router (MPLS, etc.)	Yes	MPLS or another transport technology used to establish WAN connection back to control center (CC).	Time synchronization issues may impact communications channels. Previous research and experience has shown that a lack of time synchronization can cause asynchronous latency, jitter, and packet loss in channels (if not an entire loss of communications)

Table 2-8 (continued)
Data Dependencies

Computer/system/application activity	Dependency on precision time?	Description	Notes
Local HMI	Unknown	Local HMI available to techs within the station house	Suspect time synchronization difference between station and process bus could potentially cause issues
Engineering Gateway	Yes	Remote gateway for engineering access to local hardware	Lack of time synchronization could cause failure of cryptographic handshakes
SCADA	Yes	Supervisory control and data acquisition is centralized at CC location(s).	Time synchronization failure could cause loss of communications between CC and substations.
Merging Units	Yes	MUs used for aggregating data from CT, VTs, NCITs, etc.	Assumed MU is using SV communications and timestamping of data would be impacted by timing synchronization issues
Digital fault recorders & Historians	Yes	Recording of event data for later review	Time synchronization failures would make it hard to align event data with event data observed to a different time reference

Step by Step – Normal Operations, SCADA MMS

Table 2-9
Normal Operations Step by Step - SCADA MMS

Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged
1	Control center breaker operation	Operator initiates distribution breaker operation via SCADA	SCADA Terminal	CC Switches	TCP/IP wrapped MMS, channel control traffic
2	Control center breaker operation	Control center switches receives MMS control operation and forwards it to CC MPLS router	CC Switches	CC MPLS router	TCP/IP wrapped MMS, channel control traffic

Table 2-9 (continued)
Normal Operations Step by Step - SCADA MMS

Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged
3	Control center breaker operation	Control center MPLS router receives MMS control operation and forwards it to station MPLS router	CC MPLS router	Station MPLS router	TCP/IP wrapped MMS, channel control traffic
4	Control center breaker operation	Station MPLS router receives MMS control operation and forwards it to station bus switches	Station MPLS router	Station bus switches	TCP/IP wrapped MMS, channel control traffic
5	Control center breaker operation	Station bus switches forwards MMS control operation to destination IED	Station bus switches	Control IED	TCP/IP wrapped MMS, channel control traffic
6	Control center breaker operation	Control IED publishes GOOSE control point change to breaker IED(s)	Control IED	Process bus switches	GOOSE packets
7	Control center breaker operation	GOOSE msg forwarded to breaker IED(s)	Process bus switches	Breaker IED(s)	GOOSE packets
8	Control center breaker operation	Breaker(s) observes goose msg control point change, operates and generates GOOSE event	Breaker IED(s)	Process bus switches	GOOSE packets

Step by Step – compromised operations for SCADA MMS

Most of the potential issues in this scenario can be tied to time sensitivities in TCP/IP operations or issues within the network transport due to time synchronization misalignment impacting transport availability. Depending upon the type and configuration of transport technology and the method of obtaining time synchronization, there may be a potential for channel latency or information loss due to time synchronization misalignment. Depending on the scale of the time synchronization difference, the potential also may exist that the MMS traffic is dropped between the MPLS station router and the local station bus switches. No potential time synchronization issues were identified once the traffic was being forwarded locally within the station house.

Table 2-10
Compromised Operations Step by Step - SCADA MMS

Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged	Impact to resiliency
1	Control center breaker operation	Operator initiates distribution breaker operation via SCADA	SCADA Terminal	CC Switches	TCP/IP wrapped MMS, channel control traffic	Undetermined – variable recovery based on deployed components and systems
2	Control center breaker operation	Control center switches receives MMS control operation and forwards it to CC MPLS router	CC Switches	CC MPLS router	TCP/IP wrapped MMS, channel control traffic	Undetermined – variable recovery based on deployed components and systems
3	Control center breaker operation	Control center MPLS router receives MMS control operation and forwards it to station MPLS router	CC MPLS router	Station MPLS router	TCP/IP wrapped MMS, channel control traffic	Potential channel latency or information loss due to time synchronization error between MPLS routers – but needs additional research
4	Control center breaker operation	Station MPLS router receives MMS control operation and forwards it to station bus switches	Station MPLS router	Station bus switches	TCP/IP wrapped MMS, channel control traffic	Possible drop of MMS due to time sync error/timeout – but recovery needs to be researched

Table 2-10 (continued)
Compromised Operations Step by Step - SCADA MMS

Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged	Impact to resiliency
5	Control center breaker operation	Station bus switches forwards MMS control operation to destination IED	Station bus switches	Control IED	TCP/IP wrapped MMS, channel control traffic	Undetermined – variable recovery based on deployed components and systems
6	Control center breaker operation	Control IED publishes GOOSE control point change to breaker IED(s)	Control IED	Process bus switches	GOOSE packets	Undetermined – variable recovery based on deployed components and systems
7	Control center breaker operation	GOOSE message(s) forwarded to breaker IED(s)	Process bus switches	Breaker IED(s)	GOOSE packets	Undetermined – variable recovery based on deployed components and systems
8	Control center breaker operation	Breaker(s) operates and generates GOOSE event	breaker IED(s)	Process bus switches	GOOSE packets	Undetermined – variable recovery based on deployed components and systems

Step by Step – Normal Operations, Local Disparity

The local disparity scenario considered the impact a local time source disparity could have upon communications within the substation.

Table 2-11
Normal Operations Step by Step - Local Disparity

Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged
1	Generation of event data	Breaker IEDs performs	Breaker IED	Process bus switches	GOOSE msg
2	Forwarding of GOOSE msg	Process bus Ethernet switch forwards GOOSE msg to bay IEDs	Process bus switches	Bay IEDs	GOOSE msg
3	Generation of MMS event from GOOSE event msg	Bay IED generates event notification message from GOOSE event msg	Bay IED	Station bus Ethernet switches	MMS msg
4	Local historian	Local historian records event data as observed from process and/or station bus.	IEDs	Local Historian	GOOSE/MMS msgs
5	Event data retrieval/Sync	Local historian data is uploaded to higher level historian or operator reviewing event data	Local historian	Central historian/Operator	Event data

Step by Step – Compromised Operations, Local Disparity

Outside of the excluded applications group with Use Case 1, digital fault recorders and historians may be the most sensitive to time misalignment. While the implications of the synchronization failure may not have substantial impact, the potential does exist that incorrect time could cause difficulty in diagnosing or aligning during post event analysis. A worst case scenario might be that incorrectly timestamped data leads to the utility investing resources where they are not needed or results in potentially dangerous decisions due to improper information.

Table 2-12
Compromised Operations Step by Step - Local Disparity

Step	Name of activity or process	Description	Producing stakeholder	Receiving stakeholder	Data exchanged	Impact to resiliency
1	Generation of event data	Breaker IEDs performs	Breaker IED	Process bus switches	GOOSE msg	Event data timestamp is misaligned – recovery may be differentiated by vendor
2	Forwarding of GOOSE msg	Process bus Ethernet switch forwards GOOSE msg to bay IEDs	Process bus switches	Bay IEDs	GOOSE msg	Undetermined – variable recovery based on vendor
3	Generation of MMS event from GOOSE event msg	Bay IED generates event notification message from GOOSE event msg	Bay IED	Station bus Ethernet switches	MMS msg	Undetermined – variable recovery based on vendor
4	Local historian	Local historian records event data as observed from process and/or station bus.	IEDs	Local Historian	GOOSE/MMS msgs	Event data recorded is misaligned in time, recovery may vary by vendor
5	Event data retrieval/Sync	Local historian data is uploaded to higher level historian or operator reviewing event data	Local historian	Central historian/Operator	Event data	Misaligned event data makes analysis more difficult, recovery may vary by vendor

Regulatory Requirements

The use case examined general requirements.

Table 2-13
Regulatory Requirements

Entity	Mandatory compliance?	Description	Notes
North American Electric Reliability Corporation (NERC)	YES	NERC CIP has a number of regulations that apply on a broader scope	There are a number of components in the IEC 61850 standard that can help address a number of the regulatory requirements.
NERC CIP-010 (Change management), CIP-009 (Recovery plans for BES), CIP-011 (Information protection), CIP-007 (Cyber security), CIP-005 R1 (Electronic security perimeter)	YES	Using IEC 61850-6 Substation Configuration Language to satisfy some of the regulatory requirements	A number of the CIP requirements can be partially fulfilled with information that is contained within or can be generated using SCL files. Others may need to be considered for data privacy and protection.
NERC CIP V5	YES		May also be applicable to IEC 61850-9 process bus. Due to location of MU in the yard, this may present additional ESPs and the need for electronic access control or monitoring systems for the cabinets containing them.
PRC-002 -> PRC-018	YES	CIP protection and control	Contains some time synchronization requirements for protection and control.

Next Steps

These two use case results can now be tested in laboratory settings to confirm or disprove the expected impacts to normal operations. The use cases also serve to inform vendor product plans, utility procurement plans, industry association actions, standards development organizations, and governmental agencies actions regarding precision timing resiliency for critical infrastructure.

The research identified additional scenarios for transmission and distribution grid operations that could be described in this same use case methodology. The same benefits of knowledge contributions to the electricity subsector stakeholders could be achieved with continuation of this research activity. While timing dependencies in transmission operations have been studied for some time, the growing adoption of time-dependent applications in distribution operations increases the need for research to identify any precision timing vulnerabilities and develop risk mitigations. As 61850 is adopted in digital substation deployments, more use cases should be developed and tested and information should be shared with the electricity sector. As one possibility, routable GOOSE (R-GOOSE) could be studied for precision timing considerations.

3
CONCLUSION

This use case research activity demonstrated the value of collaborative research within a team of industry stakeholders and use of forums to encourage information and experiences. There is a continued need for additional awareness of the issues regarding timing vulnerabilities and their impacts to utility grid operations, and use cases serve a good starting point to describe “what-if” scenarios for stakeholders to consider. Electricity subsector stakeholders may leverage these use cases as tools to enable transitions in precision timing risk perceptions from low to higher risk so the most effective risk mitigation actions are adopted.

About EPRI

Founded in 1972, EPRI is the world's preeminent independent, non-profit energy research and development organization, with offices around the world. EPRI's trusted experts collaborate with more than 450 companies in 45 countries, driving innovation to ensure the public has clean, safe, reliable, affordable, and equitable access to electricity across the globe. Together, we are shaping the future of energy.

Program:

Cyber Security for Power Delivery and Utilization

3002025563

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 • USA

800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com