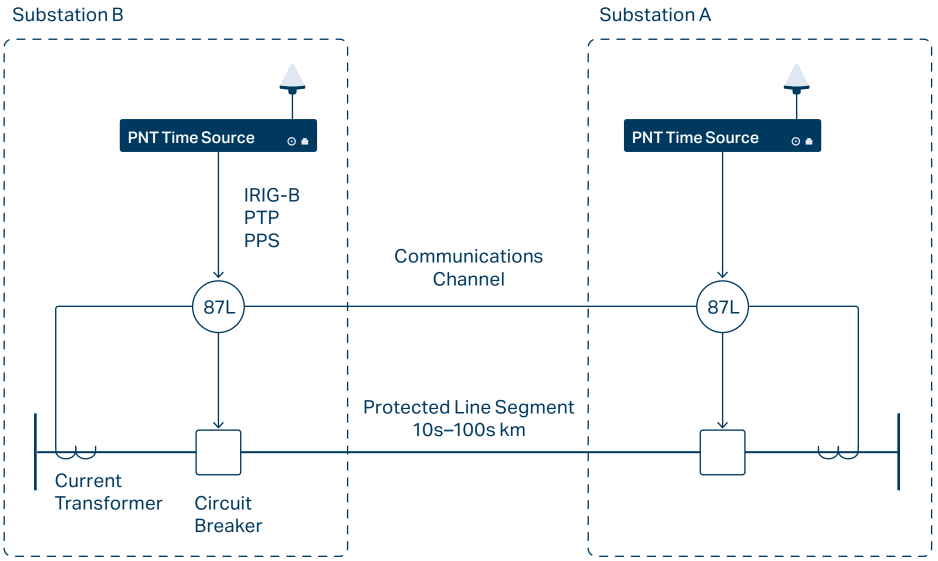
PRECISE TIME

Time as a Threat Vector: Security Risks in Line Current Differential (87L) Protection Systems

Marcel Geor
Schweitzer Engineering Laboratories, Inc.

In modern power grids, line current differential (87L) protection plays a critical role in safeguarding transmission lines. Its effectiveness hinges on the accurate comparison of current measurements made at both ends of a transmission line. This comparison is only meaningful when the measurements are precisely time-aligned. As such, time synchronization is not just a technical requirement, it is a cybersecurity imperative. Any compromise in time synchronization can lead to undesirable consequences, including false tripping and fault detection failure, both of which threaten grid stability and reliability.



The Role of Time Synchronization in 87L Protection

The 87L protection scheme compares local and remote current measurements at each end of the protected zone of a transmission line. The scheme must synchronize these measurements to the same time reference to ensure the comparison reflects the same moment in time. There are two primary synchronization methods:

1. Channel-Based Synchronization (Ping-Pong Protocol)
   - Time-deterministic symmetrical channels, such as dedicated fiber-optic links and telecommunication equipment, provide support for synchronous serial data circuits (e.g., IEEE C37.94 or G.703).
   - 87L relays exchange timing messages to estimate and compensate for communications channel delays.
   - Channel asymmetry must be minimal for this method to be effective.
2. External Time-Based Synchronization
   - Although external time-based synchronization can also be used when the communications channel is based on a synchronous serial interface (e.g., IEEE C37.94 or G.703), it is more commonly employed when the teleprotection channel is using Ethernet. And because Ethernet is non-deterministic, it can result in variable channel latencies that, therefore, cannot be characterized using the ping-pong method. Time-based synchronization is also required for packet-switched networks, such as Multiprotocol Label Switching (MPLS).
   - 87L relays rely on either Global Navigation Satellite Systems (GNSS) or IEEE 1588 Precision Time Protocol (PTP) to synchronize clocks.
   - Current samples are accurately time-stamped for alignment.

While both methods aim to ensure accurate time alignment, the external synchronization method introduces cybersecurity vulnerabilities that must be addressed.

Security Risks of External Time-Based Synchronization

In 87L applications, a 5.6 ms time offset can cause a 120° phase error, enough to shift the current ratio in the alpha plane from the restrain to the operate region. This shift can result in false tripping under normal load conditions or missed detection of internal faults [1]. An offset of this magnitude could be caused by any of the following failure mechanisms:

1. GNSS Adversities—Spoofing and Jamming

   GNSS signals, such as those from GPS, are weak and unencrypted, making them vulnerable to spoofing and jamming by bad actors:

   - Spoofing involves transmitting fake GNSS signals to mislead receivers into accepting false time data.
   - Jamming is deliberate interference that causes constant or intermittent loss of GNSS reception, leading to difficulties in locking on to signals, maintaining synchronization, and estimating time errors.

   When 87L relays at one end of a transmission line are synchronized to a source affected by either spoofing or jamming, a loss of measurement coherency will result.

2. PTP Attacks on Ethernet Networks

   While substations increasingly use IEEE 1588 PTP for time synchronization over Ethernet networks, it is susceptible to several attack vectors:

   - Delay attacks are when hostile parties introduce artificial delays in PTP messages, causing time drift.
   - Packet manipulation is when a hostile party intercepts and modifies PTP messages.
   - Rogue master attacks involve devices that claim to be grandmaster clocks but distribute incorrect time.
   - Replay attacks occur when hostile parties record PTP messages and replay them later without changes.
   - PTP spoofing is when a hostile party uses tools to impersonate a legitimate clock and introduces false timing information.

3. Clock Errors

   Clocks providing synchronization for 87L relays may synchronize to one or more reference source, such as PTP or GNSS, through its embedded receiver, which could be third-party modules. If the PTP source is compromised or the embedded receiver gives unexpected or erroneous data, clock errors may result.

4. Clock Drift and Holdover Vulnerabilities

   When a clock loses its time reference (e.g., due to GNSS signal loss), it enters a holdover state, relying on its internal oscillator to maintain time. Drifts that go undetected and clocks that do not correctly estimate worst-case time errors while in holdover compromise the dependability and security of the protection scheme.

   In any of the aforementioned cases, these failure mechanisms can silently degrade synchronization accuracy, leading to 87L relay misoperation. Without immediate detection, this misoperation can result in:

   - False current differential, leading to unnecessary tripping.
   - Masked real faults, resulting in protection failure.

Mitigation Strategies and Best Practices

To secure time synchronization in 87L protection, utilities must adopt a multi-layered defense strategy, such as:

1. Redundant Time Sources

   - Use multiple GNSS constellations, including GPS and Galileo, to enhance validation of timing solutions.
   - Deploy local backup clocks and holdover-capable oscillators to maintain accuracy during GNSS outages.
   - Leverage several time synchronization sources including GNSS and PTP to mitigate common mode failure.

2. Time Signal Monitoring
    - Continuously monitor time-quality indicators (e.g., IRIG-B quality bits and PTP jitter).
    - Implement alarms and fallback modes when time quality degrades or synchronization fails.
3. Secure PTP Implementation
    - Monitor network integrity, connected nodes, and PTP variables.
    - Isolate PTP traffic on dedicated VLANs or out-of-band networks to prevent tampering.
    - Deploy boundary and transparent clocks designed to reduce delay variation, thereby minimizing time errors during distribution.
4. GNSS Signal Protection
    - Install GNSS antennas in secure, shielded locations to reduce spoofing risk.
    - Monitor GNSS signal and data to detect anomalies.
5. Validation

    Install clocks purpose-built for critical infrastructure that validate the synchronization sources against their own internal time to filter out or disqualify erroneous sources.
6. Cybersecurity Hardening
    - Apply network segmentation to isolate protection systems from external threats.
    - Use firewalls, intrusion detection systems, and access controls to protect time-synchronization infrastructure.
    - Regularly patch and update firmware on clocks, relays, and network devices.

The Importance of Time Integrity for Grid Stability

The consequences of time misalignment in 87L protection are not theoretical—they are real and can be costly. A single false trip on a high-voltage transmission line can result in a loss of load, widespread outages, equipment damage, and economic losses. Conversely, a failure to trip during a genuine fault can lead to prolonged fault currents, damage, and system instability.

As the power grid becomes more digitized and interconnected, the attack surface for time-based vulnerabilities expands. Cyber adversaries may target time synchronization as a low-effort, high-impact vector toward disrupting grid operations. Therefore, power utilities must treat time as a critical asset, on par with voltage, current, and frequency.

Conclusion

87L protection is a cornerstone of modern transmission line protection, but its reliability depends on the accuracy, integrity, and security of its time synchronization. As utilities transition to packet-based communications networks and external time sources, they must recognize and mitigate the cybersecurity risks associated with time misalignment.

By implementing redundant, secure, and monitored time-synchronization systems, utilities can ensure that 87L protection remains dependable—even in the face of cyber threats, GNSS adversities, and network disruptions. Within the evolving landscape of smart grids and digital substations, time is not optional, it is mission critical. Protect it accordingly.

References

[1] A. Shrestha, P. Nadkar, and J. Fultz, "Understanding the Impact of Time Inaccuracy on Synchrophasors, Traveling-Wave Fault Locating, and Line Current Differential Protection," Protection, Automation & Control World Americas Conference, Raleigh, NC, August 2023.

SEL SCHWEITZER ENGINEERING LABORATORIES

info@selinc.com | selinc.com | 20260128