

TimeSafe

GNSS Vulnerability Assessment Service

WHY TIMING MATTERS TO THE POWER GRID

PRECISE TIME IS FOUNDATIONAL — AND FRAGILE

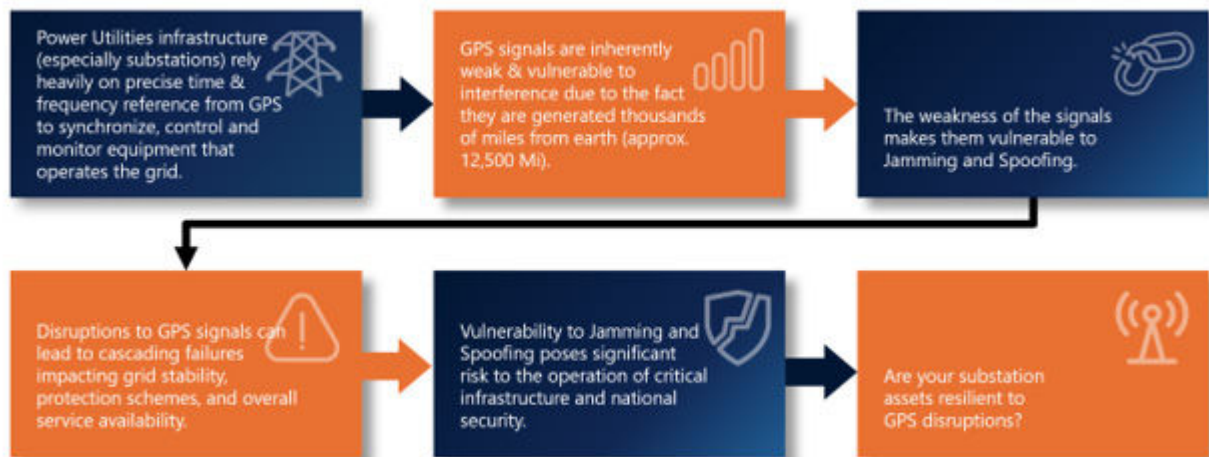
Power utilities rely on GPS timing to synchronize protection, control, and monitoring systems across substations and control centers. From protection relays to PMUs and SCADA systems, **loss or corruption of timing can directly impact grid stability and safety.**

GPS signals are inherently weak, transmitted from satellites over 12,000 miles away, making them vulnerable to interference — whether accidental or malicious.

When timing fails, systems don't simply go offline — they behave incorrectly.

THE THREATS: JAMMING AND SPOOFING. TWO TYPES OF ATTACK. ONE SHARED RISK.

- **Jamming:** Overpowers legitimate GPS signals, causing receivers to lose lock and timing reference.
- **Spoofing:** Introduces false GPS signals, deceiving equipment into accepting incorrect time or position — often without alarms.



Both can be unintentional or deliberate, and both can impact **multiple substations simultaneously.**

Direct impact of jamming or spoofing

- Protection mis operations or failure to trip
- Loss of synchrophasor integrity
- Incorrect event timestamps and alarms
- Extended outage investigation and restoration time
- Increased regulatory and operational risk

KNOW HOW YOUR SYSTEMS BEHAVE BEFORE AN EVENT OCCURS

Safran's GNSS Vulnerability Assessment Service (TimeSafe) evaluates how real utility equipment responds to GPS jamming and spoofing under **controlled, repeatable, and non disruptive conditions.**

The result: **clear visibility into vulnerabilities, quantified risk, and a practical mitigation roadmap.**



EXPERT-LED. CONTROLLED. SAFE.



Asset inventory and GPS dependency analysis



Lab based testing using controlled scenarios



Threat modeling based on real world interference techniques



No impact to live substations or operations

All scenarios are **repeatable**, allowing direct comparison before and after mitigation.

ACTIONABLE RESULTS

Deliverables include:	Representative test scenarios	Sample findings
• Comprehensive vulnerability assessment report • Quantified timing and synchronization performance metrics • Identification of affected assets (device, model, configuration) • Mitigation roadmap tailored to your environment • Expert review session with Safran SMEs	• Loss of GPS signal (jamming) • Gradual timing drift (low power spoofing) • Sudden time step events • Combined interference scenarios	• Maximum timing error before protection mis operation • Holdover performance and recovery behavior • Devices that fail silently vs. alarm correctly

SUPPORTING RESILIENT PNT & COMPLIANCE

Safran TimeSafe supports alignment with evolving expectations and best practices, including:

- Executive Order 13905
- IEEE P1952 (Resilient PNT for Power Systems)
- DHS Resilient PNT Best Practices for Critical Infrastructure

Testing provides **documented evidence of proactive risk management.**

ABOUT SAFRAN NAVIGATION & TIMING

Safran provides trusted positioning, navigation, and timing solutions for mission critical applications worldwide. When the integrity of time cannot be compromised, utilities rely on Safran to help protect system uptime, safety, and resilience.

Learn how your assets behave under real GPS threats.

Email us: timingsupport@nav-timing.safrangroup.com

Visit us online: safran-navigation-timing.com



Scan to learn more

**POWERED
BY TRUST**

safran-navigation-timing.com

