



BlueSky® GNSS Firewall Release 4.0.x

Protection and Traceability of Timing for Critical Infrastructure

Summary

The BlueSky® GNSS Firewall 2200 protects against jamming and spoofing by providing a cost-effective overlay solution installed between existing GNSS antennas and GNSS systems. Similar to a network firewall, the BlueSky GNSS Firewall 2200 protects systems inside the firewall from untrusted sky-based signals outside the firewall. With the addition of embedded SkyWire™ technology, BlueSky GNSS Firewall 2200 units can compare clocks across widely dispersed geographic locations to ensure alignment, including traceability with UTC as provided by national timing laboratories.

The combination of the BlueSky GNSS Firewall's anti-jamming and spoofing protection and the SkyWire technology for clock measurement verification and alignment is all included in the software release 4.0 to provide an industry-leading solution to protect and strengthen systems against GNSS threats.

Use Cases

- Telecommunications networks
- Power grid synchronization
- Financial trading systems
- Traceability to UTC provided by metrology labs
- Any critical infrastructure requiring precise and secure timing

Key Features

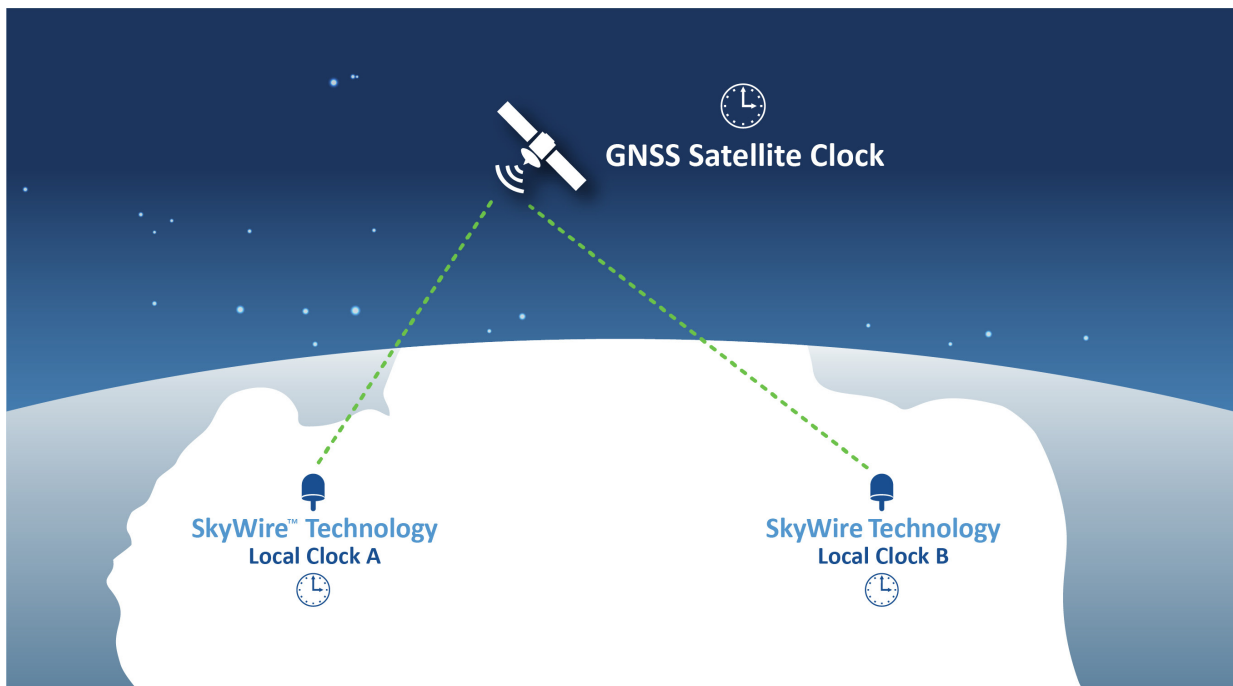
- **GNSS Firewall Functionality:** Like a traditional network firewall, the BlueSky GNSS Firewall 2200 acts as a barrier between the GNSS antenna and the GNSS receiver/system. It filters and validates incoming satellite signals, blocking those that are suspicious or potentially harmful.
- **Anti-Jamming and Anti-Spoofing:** The device detects and mitigates attempts to jam (block) or spoof (deceive) GNSS signals, ensuring that only authentic and reliable signals are passed through to the protected systems.
- **Cost-Effective Overlay:** It is designed to be easily installed as an overlay between existing GNSS antennas and systems, minimizing the need for major infrastructure changes.

SkyWire Technology (New in Software Release 4.0)

- **Clock Comparison Across Locations:** SkyWire technology enables BlueSky GNSS Firewall units to compare timing signals (clocks) across multiple, geographically dispersed sites.
- **UTC Traceability:** The system ensures that all connected sites remain synchronized and traceable to Coordinated Universal Time (UTC), as maintained by national timing laboratories.
- **Enhanced Verification:** This technology adds an extra layer of verification, ensuring that timing signals are not only protected from external threats but also remain accurate and aligned across an organization's entire network.

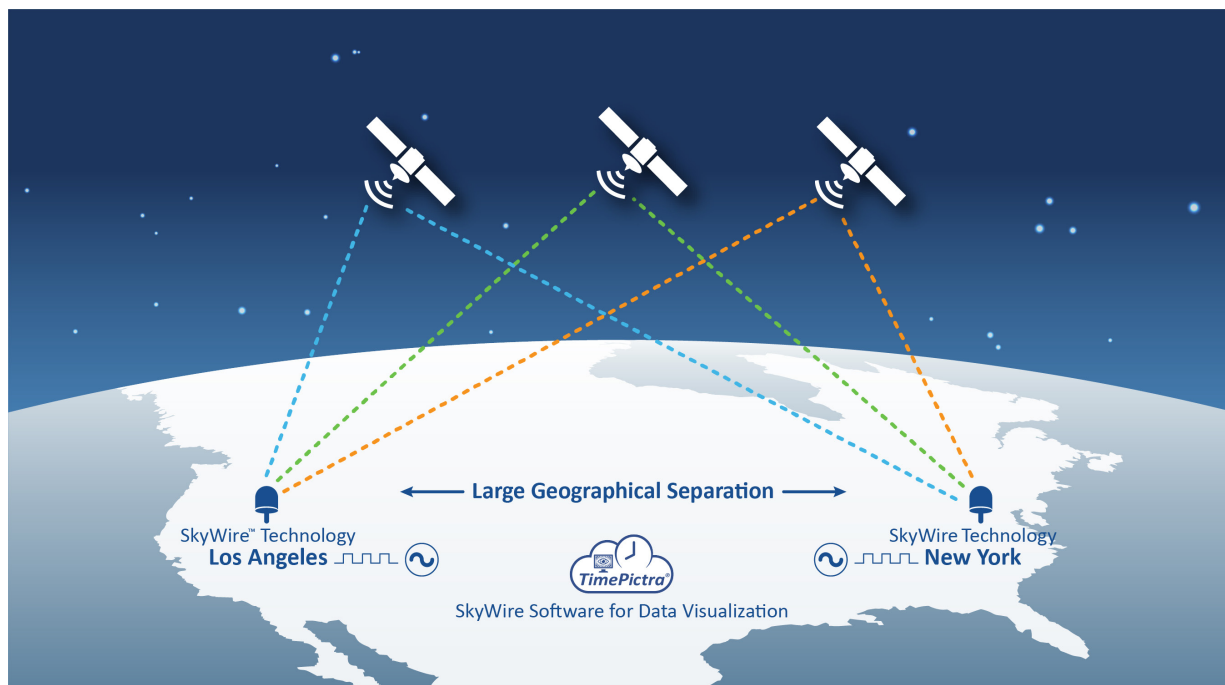


SkyWire technology leverages GNSS signals not as a direct timing source, but as a virtual wire to enable highly precise time comparisons between geographically separated locations. With SkyWire technology, two sites can achieve accurate time alignment as long as they can simultaneously track the same GNSS satellites—a concept known as common view. In this scenario, both locations observe the same set of satellites at the same time, allowing them to reference identical signals for time and frequency comparison. This shared visibility forms the foundation for precise synchronization across distributed sites, ensuring robust and reliable time transfer without relying solely on GNSS as the primary timing source.

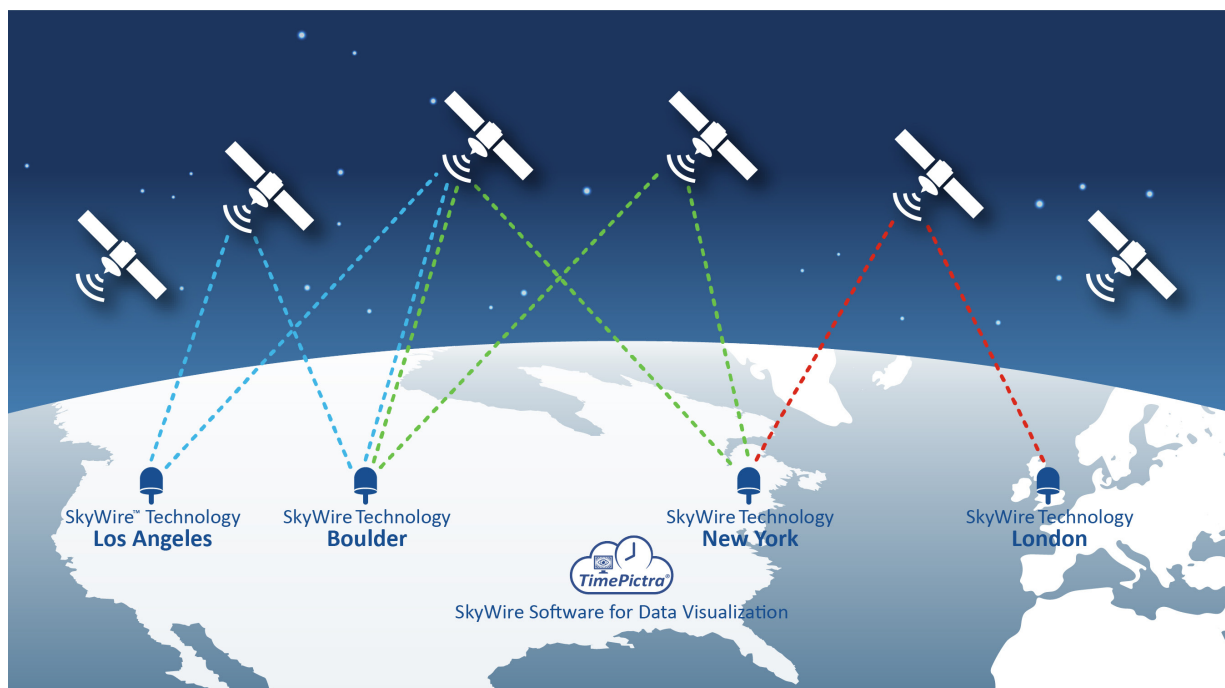


When a satellite is in common view between two locations, both sites can independently record the time of arrival of the satellite's signal. In this scenario, the GNSS satellite effectively serves as a shared reference clock for both locations. At each site, a BlueSky GNSS Firewall 2200 uses SkyWire technology to measure the local clock against the satellite's clock—Clock A versus the GNSS clock, and Clock B versus the GNSS clock. By subtracting these two measurements, you obtain the time offset between

Clock A and Clock B. The BlueSky GNSS Firewall with SkyWire technology maintains accurate knowledge of both the satellite's position and the antenna locations to ensure that signal path delays are accounted for. This enables a highly precise comparison of the two clocks.

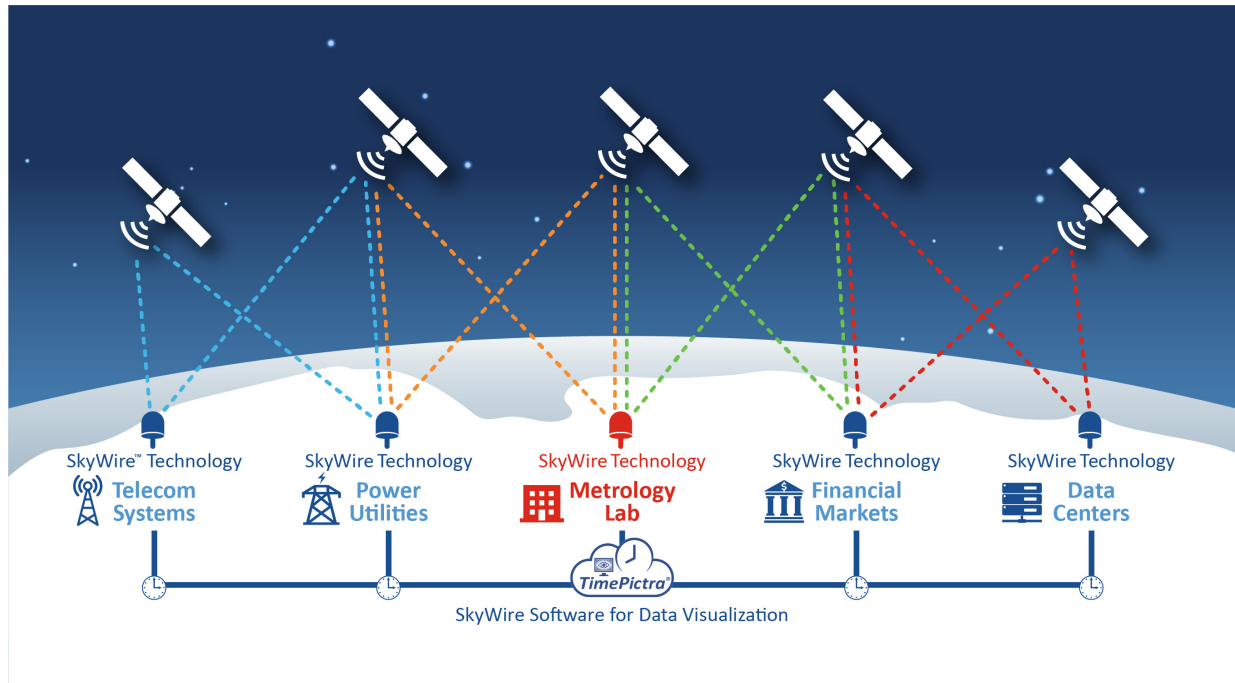


Historically, performing common view time transfer required specialized, high-end GNSS receivers. Today, however, advances in technology have made it possible to achieve very high accuracy in common view time transfer. By developing advanced techniques to mitigate Radio Frequency (RF) interference in challenging GNSS environments and leveraging real-time processing, the BlueSky GNSS Firewall with SkyWire technology provides a common view solution that can now be deployed reliably and efficiently at scale.



The BlueSky GNSS Firewall with SkyWire technology can compare clocks located at vast distances from each other. Multiple locations can simultaneously measure the same satellite(s) that are visible at the same time. The resulting measurement data is

aggregated and analyzed by the TimePictra® software suite, allowing the time differences between any and all clocks to be computed and displayed visually. This capability is optimal for operators of data centers, hyperscales and other critical infrastructure with dispersed locations that require precise time alignment for applications such as distributed database access.



SkyWire technology enables national metrology laboratories to serve as the definitive authority for time and to provide reliable traceability services to all critical infrastructure sectors, including financial markets, data centers and power or utility companies. As countries implement alternative or multi-source Positioning, Navigation, and Timing (PNT) solutions, the ability to measure and verify traceability to the national time standard becomes increasingly crucial. Deploying the BlueSky GNSS Firewall with SkyWire technology at both metrology laboratories and at critical infrastructure sites establishes the foundation for a resilient national timing grid.

Coming Soon: TimePictra® Software Suite Provides an Intuitive Graphical Interface for Managing Large Deployments of BlueSky GNSS Firewalls with SkyWire Technology

BlueSky GNSS Firewall Trusted Time Security Check List for Zero Trust Network

Users	RADIUS authentication and two-factor authentication
	TACACS+ support
	Administrative Security - Web session timeouts (5–1440 minutes long) - Custom login banners
	LDAP authentication (LDAP v2 and LDAP v3)
	User Settings - Password expiration - User management (creation/deletion, username, password, email) - Multiple user privilege levels - Administrator: Can create new roles and users - User: Default basic role
	SSH (allowed and denied users)
Devices	Software Upgrades - Available exclusively through FTS Resource Portal - Requires authenticated user access to the FTS Resource Portal - Requires authorization to download the system software file and serialized authorization file
	Alarms (extensive user-configurable alarms, notification via trap, logs)
	Hardened output provides a synthesized GPS signal isolated from the live-sky environment
	Validated output delivers a verified pass-through of the actual GNSS signal being analyzed
	HTTPS Secure management - Protocols: TLS 1.3 or higher - Session timeout: 5 to 1440 minutes - Self-signed certificate: 2048 or 4096 RSA key bit; expiration days 1–1825; customizable locality codes
	X.509 Cert/CSR: Create and download Certificate Signing Requests (CSRs) with 2048 or 4096 RSA key bits
	X.509 installation: Install multiple CA-signed X.509 certificates
	Timing Security - Anti-jam antenna - Atomic clock upgrades for timing holdover
Network	Dedicated and distinct network management port along with a local console port
	Service/system control (enable/disable HTTPS, SNMP, SSH, ToD)
	GPS Subframe Anomaly Detector compares subframes from a remote firewall to those received from the live-sky signal within the local firewall (For more information, see the BlueSky® GNSS Firewall Software-Release 3.1.1 data sheet)
	Trusted Time Anomaly Detector allows terrestrial network-based time to cross check GNSS time (For more information, see the BlueSky GNSS Firewall Software-Release 3.1.1 data sheet)
Analytics	SNMP V3 - Secure authentication - Secure encryption
	TimePictra® platform monitoring - Tracks last configuration changes - Supports autonomous messaging - Monitors firmware versions
	Secure Syslog - X.509 authentication - TLS encryption