BlueSky® GNSS Firewall 2200

GNSS Spoofing and Jamming Protection With SkyWire™ Technology for Clock Measurements

Key Features

BlueSky® Technology Features

- GNSS Firewall Functionality: Similar to a traditional network firewall, the BlueSky GNSS Firewall 2200 acts as a barrier between the GNSS antenna and the GNSS receiver/system by filtering and validating incoming satellite signals and blocking the suspicious or potentially harmful ones
- Anti-Jamming and Anti-spoofing: The device detects and mitigates attempts to jam (block) or spoof (deceiver) GNSS signals so that only authentic and reliable signals are passed through the protected signals

SkyWire™ Technology Features

- 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 enables all connected sites to remain synchronized and traceable to coordinated universal time (UTC), as maintained by national timing laboratories
- Enhanced Verification: The technology adds an extra layer of verification so that timing signals are not only protected from external threats, but also remain accurate and aligned across an organization's entire network

Protecting Critical Infrastructure

The vulnerability of GNSS systems to various signal incidents is well documented. The rapid proliferation of GNSS systems has embedded these vulnerabilities into critical infrastructures that rely on GNSS-delivered PNT for daily operations. This widespread deployment of GNSS makes it impractical to replace all fielded GNSS systems in a timely or cost-effective manner.

Secure Firewall Overlay

The BlueSky GNSS Firewall 2200 solves the problem of protecting already deployed systems by providing a cost-effective overlay solution installed between existing GNSS antennas and GNSS systems. The BlueSky GNSS Firewall 2200 protects systems inside the firewall from untrusted sky-based signals outside the firewall.

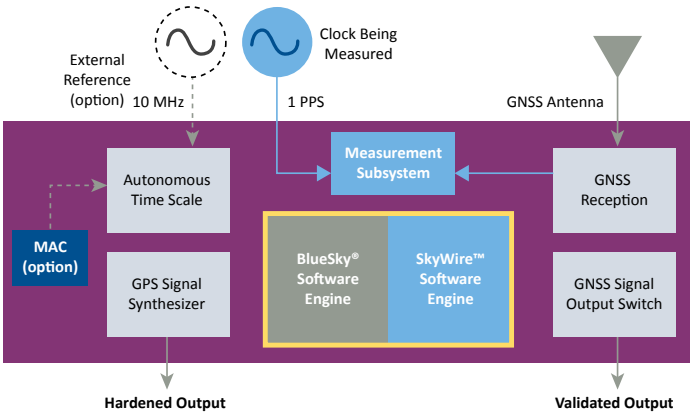
BlueSky GNSS Firewall Software

Contained within the BlueSky GNSS Firewall 2200 is a software engine that analyzes the GNSS signal. GNSS signal data is received and evaluated from each satellite to enable compliance and analyze received signal characteristics. Threshold settings of GNSS observables such as satellites-in-view, carrier-to-noise, position deviation, phase time deviation and Radio Frequency (RF) power levels are user configurable. This information provides situational awareness about the health of the GNSS reception and is used by the firewall to eliminate anomalous GNSS signals and provide a secure GNSS signal output to downstream GNSS systems.

SkyWire Technology

Our SkyWire technology utilizes advanced Positioning, Navigation and Timing (PNT) technology to compare clocks across geographically dispersed locations with high precision. SkyWire technology can perform accurate time measurements between clocks at different network locations that simultaneously observe GNSS satellite signals. This enables comprehensive, real-time analysis of time alignment throughout the network.

BlueSky GNSS Firewall 2200 Block Diagram



GNSS Input and Outputs

The BlueSky GNSS Firewall 2200 can be configured for GPS only or for a combination of Galileo and GPS reception. There are two types of outputs that are simultaneously available for protection of downstream systems.

Hardened Output

The hardened output is the most secure because it provides a synthesized GPS signal isolated from the live-sky environment. The hardened output is not a copy of the live-sky GNSS signal and is only loosely based on information received from the live-sky signal. Thus, a secure BlueSky GNSS environment is created. When GNSS incidents are detected on the input (either GPS or Galileo), the hardened output continues to be available and relies on the internal rubidium Miniature Atomic Clock (MAC) or external frequency reference to maintain accuracy.

Validated Output

The validated output provides a verified pass-through of the actual GNSS signal being analyzed. When anomalous conditions are detected (either GPS or Galileo), the validated output is turned off to protect users from potentially corrupted GNSS signals. Once conditions are deemed safe, the validated output is turned back on.

Upgrading the BlueSky GNSS Firewall 2200 with the rubidium MAC can provide excellent holdover of the hardened GPS signal output for multiple days.

The internal MAC uses a unique physics package based on the Coherent Population Trapping (CPT) atomic clock. It consumes less power and has broad temperature operation and longer life than legacy lamp-based rubidium clocks.

Measurement Subsystem Performance

Time of Arrival (TOA) measurements are taken between the GNSS satellite clock and a local clock. For example, if A and B are local clocks and C is a GNSS satellite visible to both, the TOA measurements (A-C and B-C) are recorded in their respective TMAS report files. These files are then aggregated and analyzed in the TimePictra® Software Suite, enabling visual calculation and comparison of time differences between any two clocks. By subtracting (B-C) from (A-C), the satellite reference cancels out, yielding the time difference (A-B) between the two clocks. Repeating this process across multiple satellites allows for averaging and increased accuracy of the time difference.

Atomic Clock Holdover Options

The standard BlueSky GNSS Firewall 2200 is equipped with a high-quality crystal oscillator that maintains accuracy to within nanoseconds when tracking GNSS. When using the hardened GPS output, the firewall can be equipped with a variety of atomic clock options to provide holdover in case of complete GNSS signal reception loss.

Rubidium Miniature Atomic Clock (MAC)

The first option is upgrading the BlueSky GNSS Firewall 2200 with the rubidium MAC, which can provide excellent holdovers of the hardened GPS signal output for multiple days.

The internal MAC uses a unique physics package based on the Coherent Population Trapping (CPT) atomic clock. It consumes less power and has broad temperature operation and longer life than legacy lamp-based rubidium clocks.

External References

We also have available external reference inputs that can be used for holdover in place of the internal MAC. The BlueSky GNSS Firewall 2200 comes with 10 MHz and 1 PPS reference inputs so that an external reference such as the 5071A or TimeCesium® products can be used for extended holdover in case of a complete loss of GNSS reception for long periods of time.

Specifications

GNSS Antenna Input

- Connector: TNC(F)
- Impedance: 50Ω
- Antenna bias voltage: 0 VDC, 3.3 VDC, 5 VDC and 12 VDC (software selectable)

Hardened Output

Output provided using holdover when GNSS is non-compliant:

- Connector: TNC(F)
- Impedance: 50Ω
- Antenna bias voltage: DC blocked
- Power: –126 dBm to –96 dBm (software selectable)
- Satellite channels: 8
- Accuracy: Meets or exceeds live-sky performance

Validated Output

Output interrupted when GNSS is non-compliant:

- Connector: TNC(F)
- Impedance: 50Ω

1 PPS Input

- Connector: SMA(F)
- Impedance: 50Ω
- TTL compliant

10 MHz Input

- Connector: SMA(F)
- Impedance: 50Ω
- Level: 3 dBm to 13 dBm

Time of Day (ToD) Interfaces

- 2× ToD/1 PPS input/output over RS-422 RJ45 connectors, 100Ω impedance (see operators manual for use details)

Management and Diagnostics

- Ethernet: RJ45 tri-mode Ethernet (10/100/1000BASE-T)
- Management: CLI over SSHv2, secure web-based management (HTTPS/SSL)
- x.509 Certificate support, RADIUS, LDAP, TACACS+
- IPv4, IPv6, DHCP, remote secure syslog logging
- Separate console port for local access
- LEDs: Sync, GNSS valid, alarm, Power A and Power B

Power

Parameter	AC Power	DC Power
Connection	Dual IEC 60320 C14 Connectors	Dual Phoenix Contract - 1827703, Alternate Part Number MC 1,5/ 2-DYG-3.81
Dual Power Supplies	88 VAC-264 VAC 50 Hz-60 Hz 120 VAC/25W or 240 VAC/40W	20 VDC-70 VDC 50W
Load Sharing	Yes	Yes
Hitless Switching	Yes	Yes

Compliance Marks

- NRTL: North America Safety
- CB Scheme International Safety
- CE: EU Safety and EMC
- FCC: USA EMC
- VCCI: Japan EMC
- RCM: Australia/New Zealand EMC
- KC: Korea EMC

Mechanical/Environmental

- Size: 1U 19" rack mount, 17.24" (W) × 9.32" (D) × 1.73" (H)
- Operating temperature range of −5°C to +55°C
- Operating humidity of 0–95% (noncondensing)
- Weight: 7.7 lbs standalone, 8.7 lbs with shipping package

Emissions

- FCC Part 15 (Class A)
- ICES 003 (Class A)
- VCCI (Class A)
- EN300386 Telecommunications Network Equipment (EMC)
- CISPR32
- EN55032
- KN55032
- EN303413
- EN301489

Immunity

- EN55024 (Criteria A)
- KN55035 (Criteria A)
- EN/KN-61000-4-2 ESD
- EN/KN-61000-4-3 radiated immunity
- EN/KN-61000-4-4 EFT
- EN/KN-61000-4-5 surge
- EN/KN-61000-4-6 low-frequency common immunity

Safety

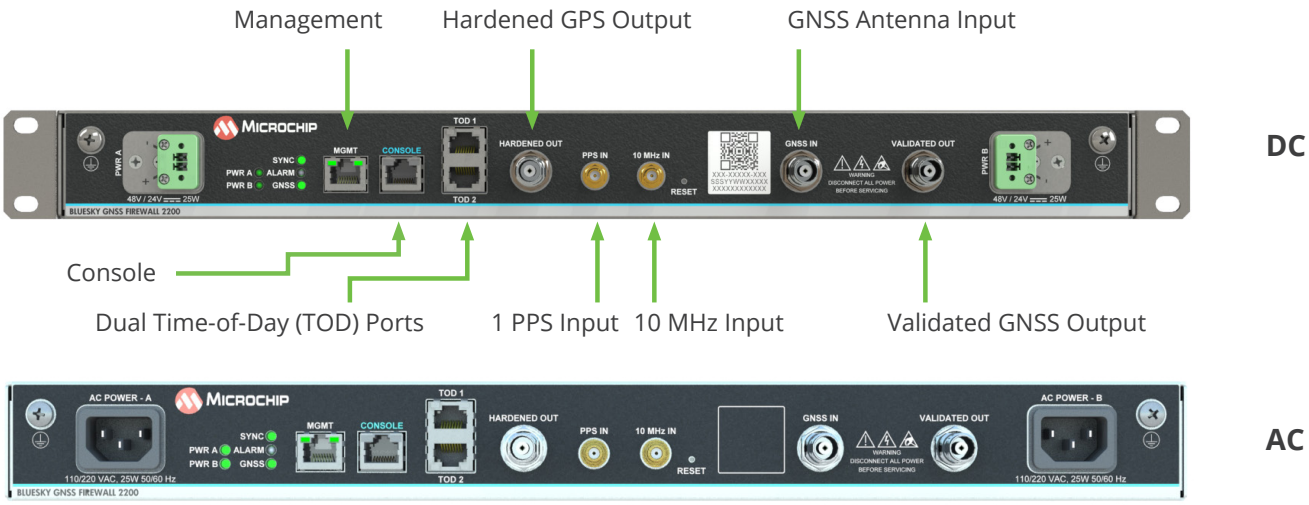
- UL 62368-1
- CAN/CSA-22.2 No. 60950-1
- IEC 62368-1
- EN 62368-1

Environmental

- ETSI EN300-019-2-3—Operating, Class T3.2
- ETSI EN 300 019-2-2 (1999)—transportation, Class T2.3
- ETSI EN 300 019-2-1 (2000)—storage, Class T1.2

Directives

- Safety Directive 2014/35/EU
- EMC Directive 2014/30/EU
- Radio Equipment Directive (RED) 2014/53/EU
- RoHS Directive 2011/65/EU and the (EU) 2015/863 amendment



DC

AC

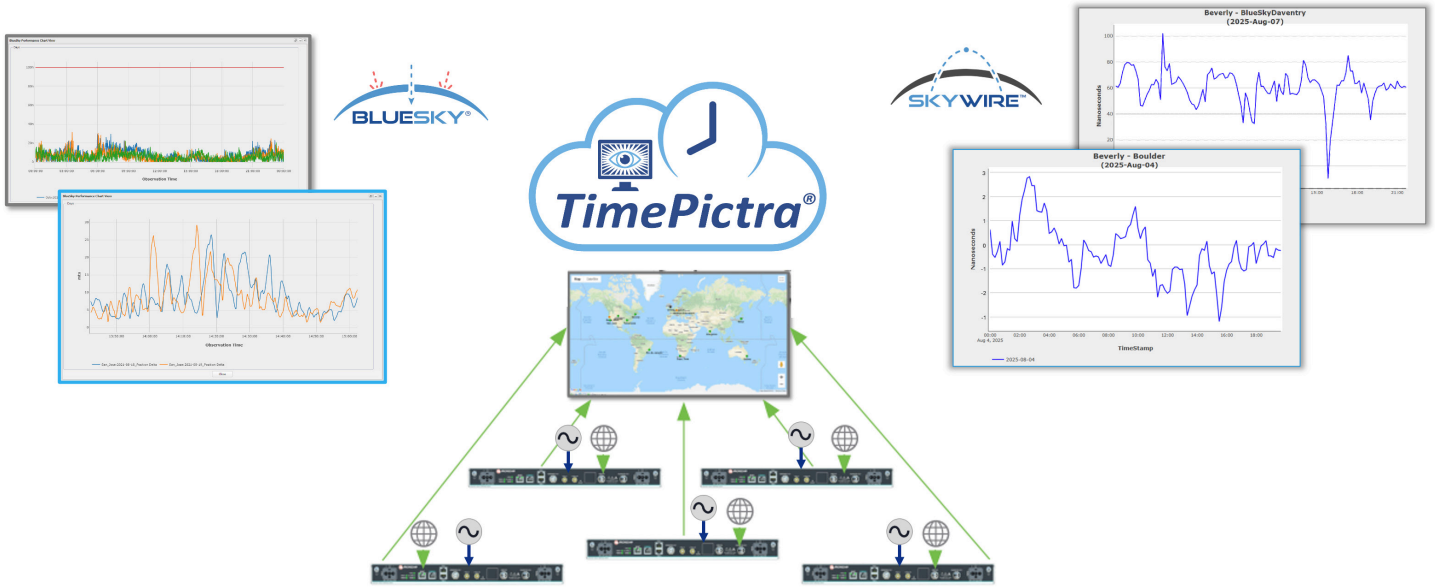
Ordering Information

Description	Part Number
BlueSky® GNSS Firewall 2200 Dual AC Power Without MAC	090-03391-101
BlueSky GNSS Firewall 2200 Dual AC Power With MAC	090-03391-201
BlueSky GNSS Firewall 2200 Dual DC Power Without MAC	090-03391-102
BlueSky GNSS Firewall 2200 Dual DC Power With MAC	090-03391-202

BlueSky GNSS Firewall Software Release 4.0

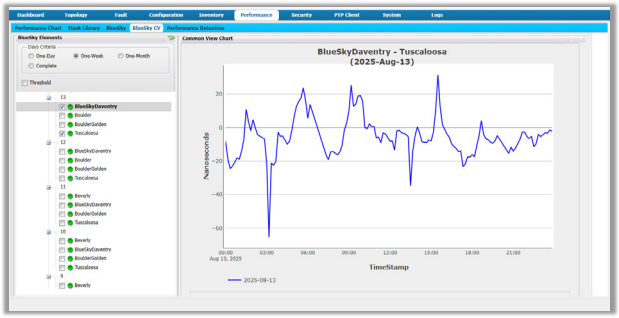
Release 4.0 adds new capabilities such as a RINEX precise site survey, enhanced security features and advanced TimePictra interoperability with SkyWire Technology to better secure, monitor, prevent, respond and recover to GNSS threats. Refer to the BlueSky GNSS Firewall Software Release 4.0 data sheet for details.

Centralized Management of Multiple Firewalls for Critical Infrastructure



For critical infrastructure deployments, maintaining a broad geographical perspective is essential. The TimePictra software suite provides an efficient and comprehensive solution for managing these complex environments. The BlueSky GNSS Firewall with integrated SkyWire technology works seamlessly with the TimePictra platform to deliver robust protection and advanced monitoring capabilities.

The TimePictra software suite serves as a centralized platform for overseeing networks equipped with BlueSky GNSS Firewall and SkyWire technology. BlueSky technology enables rapid identification of sites affected by GNSS anomalies, whether these issues arise simultaneously at multiple locations or recur periodically at different sites.



The TimePictra software suite with integrated SkyWire technology enables clock comparison data to be efficiently collected and stored within a centralized database. Users can easily select a specific date and view the clock offset between any two locations. In the example above, Daventry, UK, and Tuscaloosa, US, have been chosen for comparison. Over the 24-hour period, the peak-to-peak clock offset between these locations is measured and plotted within the TimePictra interface.

The Microchip name and logo, the Microchip logo, BlueSky and TimePictra are registered trademarks and SkyWire is a trademark of Microchip Technology Incorporated in the U.S.A. and other countries. All other trademarks mentioned herein are property of their respective companies.
© 2025, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved. 11/25