BlueSky™ GNSS Firewall 2200

Protects GNSS Systems Against Spoofing and Jamming Threats

Features

- Identifies and protects GNSS systems from spoofing and jamming
- Integrates seamlessly between existing GNSS antenna and GNSS system(s)
- Independent RF power monitoring of L1, L2 and L5 bands
- Optional internal Rubidium Miniature Atomic Clock (MAC) for holdover
- 1 PPS and 10 MHz timing reference inputs for extended holdover (for example, connection of external cesium reference)
- Redundant AC or DC power options with power monitoring, load sharing and hitless switching
- Remote CLI in addition to secure and easy-to-use web interface
- BlueSky™ GNSS Firewall embedded software is field upgradeable
- Seamless integration with TimePictra™ provides end-to-end management of 10s, 100s or 1,000s of units from a single server
- BlueSky performance monitoring integrated into TimePictra provides visibility of GNSS observables
- New Trusted Time™ Anomaly Detector for comparing Network Time and GNSS Time
- New GPS Subframe Reference detection enabling the BlueSky GNSS Firewall to compare live-sky subframe data with subframe data received from a remote BlueSky GNSS Firewall

The PNT Revolution

GNSS revolutionized the world with its ability to provide an accurate, reliable, and cost-effective Positioning, Navigation and Timing (PNT) service with global coverage. Its rapid adoption and widespread deployment enhances our way of life, but has also led to a dependency on GNSS to maintain that way of life. Critical infrastructure sectors

such as wireline and wireless networks, power grids, airports, railway, maritime ports, data centers and emergency services are all highly dependent on PNT information delivered by GNSS.

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 national infrastructures as well as corporate 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. Similar to a network firewall, the BlueSky GNSS Firewall 2200 protects systems inside the firewall from untrusted sky-based signals outside the firewall.

BlueSky GNSS Firewall Software

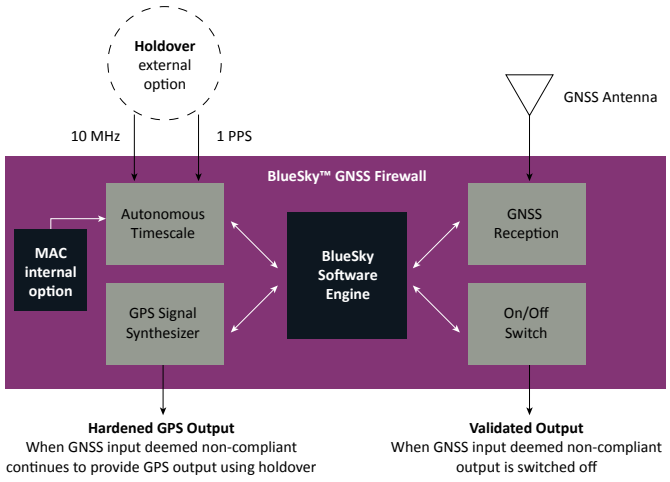
Contained within the BlueSky GNSS Firewall 2200 is a software engine that analyzes the GNSS signal. GNSS signal data is received and evaluated from each satellite to ensure compliance along with analyzing received signal characteristics. Threshold settings of GNSS observables such as satellites-in-view, 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.

Resilient PNT Conformance

The Department of Homeland Security (DHS) recently published the Resilient PNT Conformance Framework document providing a common reference point to help critical infrastructure become more resilient to PNT disruptions. The BlueSky GNSS Firewall Software, Release 3.0 provides new features and security hardening for the BlueSky GNSS Firewall to meet the highest levels of resilience as defined by the new PNT Conformance Framework. Please refer to the BlueSky GNSS Software, Release 3.0 data sheet for more details.

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. The Validated output allows pass-through of all bands including the L1, L2, and L5 signals on a single output. This enables downstream systems that use multiple GNSS constellations or GPS frequencies (such as SAASM or M-code) to use the BlueSky GNSS Firewall 2200 to provide an additional layer of protection. Additionally, other constellations such as GLONASS and Beidou are available on the Validated output. These signals are simply passed through but not analyzed for anomalies as with GPS and Galileo.

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 the 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 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.

External References

Also available are 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.

Multi-Site GNSS Anomaly Detection

GNSS anomaly detection across multiple sites is vital for critical infrastructure operators.

Trusted Time Anomaly Detector

Using the Time-of-day (TOD) interface, live-sky GNSS time can be compared to network time for GNSS anomaly detection. This approach leverages the Virtual Primary Reference Time Clock (vPRTC) architecture.

GPS Subframe Reference Detection

Live-sky subframe data can be compared to subframe data received from a remote (trusted) firewall. If a difference is detected, then an alarm is generated to indicate a miss-match.

More details about these features are available in the BlueSky GNSS Firewall Release 3.0 data sheet.

Specifications

GNSS Antenna Input

- Connector: TNC(F)
- Impedance: 50Ω
- Antenna bias voltage: 0 VDC, 3.3 VDC, 5 VDC, 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 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 03P UMNL V0 Molex power connector (P/N 0003121036)
Dual Power Supplies	88 VAC–264 VAC 50 Hz–60 Hz 120 VAC/25W or 240 VAC/40W	24V–48V/60 VDC 25W
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: −5°C to +55°C
- Operating humidity: 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

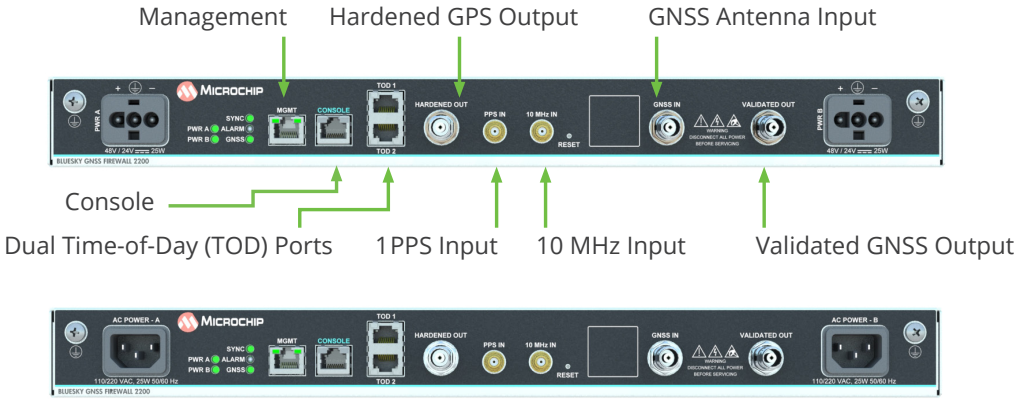
Environmental

- 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

BlueSky GNSS Firewall 2200



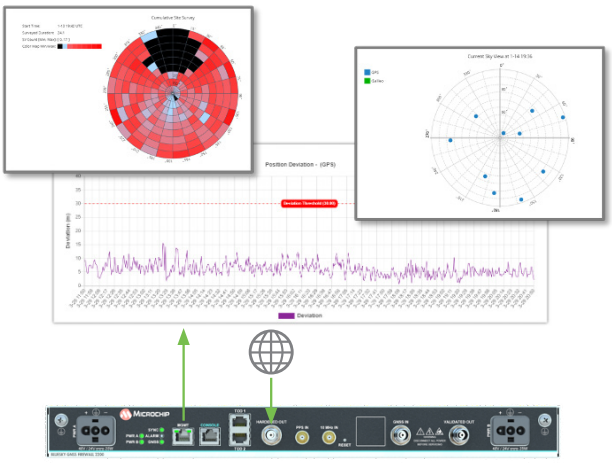
Ordering Information

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 Subscription (multi-year subscriptions also available)	999-82001-01

BlueSky GNSS Firewall Software Release 3.0

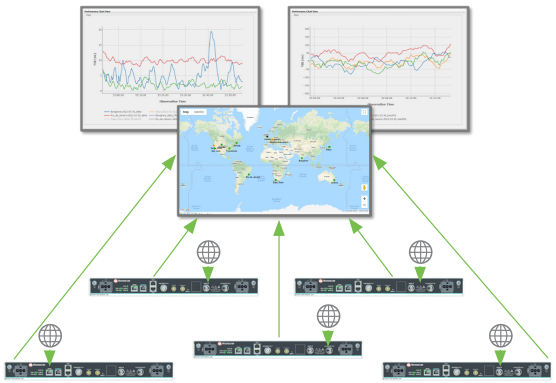
Release 3.0 adds new capabilities such as Trusted Time Anomaly Detection, GPS Subframe Detection, embedded GNSS observable tools combined with new TimePictra Performance Monitoring features to better secure, monitor, prevent, respond and recover to GNSS threats. Refer to the BlueSky GNSS Firewall Software Release 3.0 data sheet for details.

WebGUI for Set-up and Viewing From a Single Firewall



Securing GNSS delivered PNT services requires tools that can deliver efficient tactics for managing, monitoring and responding to threats. Small deployments can many times be managed directly using the Web GUI that is provided directly from the BlueSky GNSS Firewall 2200. The built-in WebGUI provides simple to use tools for antenna surveying, cable compensation as well as quick access to dashboards containing GNSS observables.

Centralized Management of Multiple Firewalls for Critical Infrastructure



For most critical infrastructure deployments, a large geographical view of GNSS reception is required and for this scenario TimePictra with BlueSky Performance Monitoring is an efficient way to manage these environments. Knowing quickly which sites were affected by a GNSS anomaly and being able to compare GNSS observables between sites are examples of how centralized management provides situational awareness for larger deployments.