BlueSky™ GNSS Firewall

Protects GPS Systems Against Spoofing and Jamming Threats

Features

• Identifies and protects GPS systems from spoofing and jamming
• Integrates seamlessly between existing GPS antenna and GPS system
• Compatible with any GNSS antenna that receives the L1 frequency
• Optional internal Rubidium Miniature Atomic Clock (MAC) for holdover
• 1PPS 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 with new GPS validation rules
• 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 GPS reception measurement and visibility

The PNT Revolution

GPS 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 GPS to maintain that way of life. Critical infrastructure sectors such as wireline and wireless networks, power grids, financial services, data centers, and emergency services now depend on PNT information delivered by GPS.

Secure Firewall Overlay

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

Contained within the BlueSky GNSS Firewall is a software engine that analyzes the GPS signal. GPS signal data is received and evaluated from each satellite to ensure compliance along with analyzing received signal characteristics. This information is used by the firewall to eliminate anomalous GPS signals and provide a secure GPS signal output to downstream GPS systems.

Microsemi provides the BlueSky Subscription, which delivers continuous security updates and improvements to the software engine. Details of the service are provided in the BlueSky Subscription datasheet.

Applications

• Wireline and wireless networks
• Utility and power grids
• Financial services
• Data centers
• Transportation networks
• Emergency services
BlueSky™ GNSS Firewall
Protects GPS Systems Against Spoofing and Jamming Threats

BlueSky Firewall Block Diagram

Multiple Levels of Resiliency
The BlueSky GNSS Firewall provides the following two types of GPS outputs.

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

Validated GPS Output
Validated GPS output provides a copy of the actual GPS signal being analyzed. When anomalous conditions are detected, the validated GPS output is turned off to protect users from potentially corrupted GPS signals. Once conditions are deemed safe, the validated GPS output is turned back on. Validated GPS includes copies of the L1, L2, and L5 signals on a single output. This enables downstream systems that use multiple GPS frequencies (such as SAASM or M-code) to use the BlueSky GNSS Firewall to provide an additional layer of protection. Additionally, other constellation bands such as Galileo, GLONASS, and Beidou are available on the validated output. These signals are simply passed through but not analyzed for spoofing along with the GPS signal.

Atomic Clock Holdover Options
The standard BlueSky GNSS Firewall is equipped with a high-quality crystal oscillator that maintains accuracy to within nanoseconds when tracking GPS. 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 GPS signal reception loss.

Rubidum Miniature Atomic Clock (MAC)
The first option is upgrading the BlueSky GNSS Firewall with the Rubidium Miniature Atomic Clock (MAC), which can provide excellent holdover of the hardened GPS signal output for multiple days.

Microsemi’s 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 comes with 10 MHz and 1PPS reference inputs so that an external reference such as Microsemi’s 5071A or TimeCesium products can be used for extended holdover in the case of a complete loss of GPS reception for long periods of time.

TimePictra with BlueSky Performance Monitoring Software
Management of wide scale deployment of BlueSky GNSS Firewall units is simplified using Microsemi’s TimePictra management system. Included with the TimePictra platform is the BlueSky Performance Monitoring that enables a regional, national, or global view of your timing infrastructure to provide early alerting of threats before your timing network is adversely impacted. Data metrics such as RF power, GPS position data, GPS phase error, and satellite count can be collected from each individual firewall and then plotted from the centralized TimePictra platform. The BlueSky Performance Monitoring functionality is included as part of the BlueSky Subscription service.

BlueSky™ GNSS Firewall
Protects GPS Systems Against Spoofing and Jamming Threats

Rubidum Miniature Atomic Clock (MAC)
BlueSky™ GNSS Firewall
Protects GPS Systems Against Spoofing and Jamming Threats

Specifications

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

Hardened GPS Output
Output provided using holdover when GPS is non-compliant
- Connector: TNC(F)
- Impedance: 50 Ω
- Antenna bias voltage: DC blocked
- Power: –126 dBm to –96 dBm (software selectable)
- Satellite channels: 8
- Accuracy: Meets or exceeds live-sky performance

Validated GPS Output
Output interrupted when GPS is non-compliant
- Connector: TNC(F)
- Impedance: 50 Ω

1PPS Input
- Connector: SMA(F)
- Impedance: 50 Ω
- TTL compliant

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

Time of Day (ToD) Interfaces
- 2 x ToD/1PPS input/output over RS-422 RJ45 connectors, 100 Ω 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
- LEDs: Sync, GNSS (GPS) valid, Alarm, Power A, and Power B

Power

<table>
<thead>
<tr>
<th>Parameter</th>
<th>AC Power</th>
<th>DC Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>Dual IEC 60320 C14 connectors</td>
<td>Dual 03P UMNL V0 Molex power connector (P/N 0003121036)</td>
</tr>
<tr>
<td>Dual power supplies</td>
<td>88 VAC-264 VAC 50 Hz–60 Hz 65 W each</td>
<td>15 A/125 VDC</td>
</tr>
<tr>
<td>Load sharing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hitless switching</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Mechanical/Environmental
- Size: 1U 19” rack mount, 17.24” (W) × 9.32” (D) × 1.73” (H)
- Operating temperature: 0 °C to 50 °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)
- EN300386 Telecommunications Network Equipment (EMC)
- CISPR32
- EN55032
- KN55032
- EN303413

Immunity
- EN301489
- EN55024 (Class A)
- KN55035 (Class 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. 62368-1
- IEC 62368-1
- EN 62368-1
- Safety directive 2014/35/EU
- CE mark

Environmental
- EN300-019-2-3, 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
- RoHS (6 of 6)
BlueSky™ GNSS Firewall
Protects GPS Systems Against Spoofing and Jamming Threats

For direct user management, the BlueSky GNSS Firewall provides an intuitive, web-based GUI.

BlueSky GNSS Firewall Dashboard

BlueSky GPS Firewall Software Upgrade Interface

The GUI also provides the ability to securely update the BlueSky client application and anomaly detection criteria.