BlueSky™ GPS Firewall

Protecting GPS Systems Against Spoofing and Jamming Threats

Protect Existing GPS Systems

Secure Firewall Overlay

Network Management

System Deployment

Secure Operations

Features and Services

Microsemi

Power Matters.™

Protect Existing GPS Systems

The Blue*Sky* GPS Firewall Protects Existing GPS Systems Today and is Field Upgradeable to Address Future Incidents

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 proliferation 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, data centers, and emergency services now depend on PNT information delivered by GPS.

Features

- Identifies and protects GPS systems from spoofing and jamming
- Integrates seamlessly between existing GPS antenna and GPS system
- Compatible with any GPS antenna that receives the L1 frequency
- Optional 1PPS and 10 MHz timing reference inputs for extended holdover
- Power-over-Ethernet (PoE) simplifies deployment by powering the firewall from the Ethernet interface
- Remote CLI in addition to secure and easy-to-use web interface
- The Blue*Sky* GPS 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

Applications

- Wireline and wireless networks
- Utility and power grids
- Enterprise data centers
- Transportation networks
- Emergency services

Secure Firewall Overlay

The Blue*Sky* GPS 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 Blue*Sky* GPS Firewall protects systems inside the firewall from untrusted sky-based signals outside the firewall.

Contained within the Blue*Sky* GPS Firewall is a software engine that analyzes the GPS signal. GPS signal data is received and evaluated from each satellite to ensure compliance with GPS standards along with analyzing received signal characteristics. This information is used by the firewall to block anomalous GPS signals and provide a hardened GPS signal output to downstream GPS systems.

Management of wide-scale deployment of the Blue*Sky* GPS Firewall units is simplified using Microsemi's TimePictra management system. TimePictra enables a regional, national, or global view of your PNT infrastructure to provide early alerting to threats before your PNT network is affected.

Secure Firewall Overlay

Microsemi's Blue*Sky* GPS Firewall is deployed in-line between an existing GPS antenna and GPS receiver system. The Blue*Sky* GPS Firewall analyzes incoming GPS signals from the antenna to identify anomalous or spoofed GPS signals.

When anomalous signal conditions are detected, the Blue*Sky* GPS Firewall blocks the unwanted signals and prevents them from propagating to downstream GPS systems. This isolates and protects downstream GPS systems from harmful GPS signals outside the firewall.

The Blue*Sky* GPS Firewall installs in a standard 19-inch rack and can be placed near the GPS receiver system or near the point at which the GPS antenna cable enters the building. Power for the GPS antenna is provided by the Blue*Sky* GPS Firewall using a software configurable setting for 0, 5, or 12 VDC. Thus, nearly all currently deployed GPS antennas are supported without modifying the existing installation.

Power for the Blue*Sky* GPS Firewall is provided by Power-over-Ethernet (PoE) on the management port. This enables current PoE deployments to integrate seamlessly with the Blue*Sky* GPS Firewall while only requiring a small PoE midspan device for installations that need to power the Blue*Sky* GPS Firewall from AC.

Critical Infrastructure

Transportation

Communications

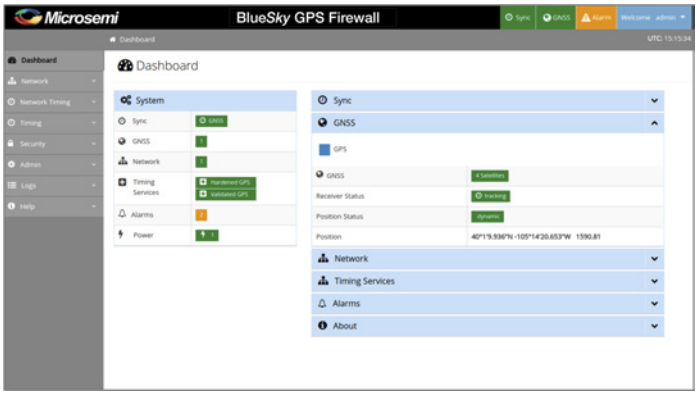
Enterprise

Power Utility

Network Management

Timing and synchronization are increasingly important to the operation of critical infrastructure sectors. A comprehensive view of an operator's time and frequency systems is paramount to identifying and localizing issues, taking corrective actions, and ensuring continued operations.

The Blue*Sky* GPS Firewall contains a client application that integrates seamlessly with Microsemi's TimePictra management system. TimePictra is a web-based management system for time, frequency, and synchronization of network elements. It features a modular architecture that scales and evolves to address new or changing operational requirements. When using TimePictra to manage a deployment of the Blue*Sky* GPS Firewall, users have centralized control and visibility of their network to ensure their enterprise is operating properly.



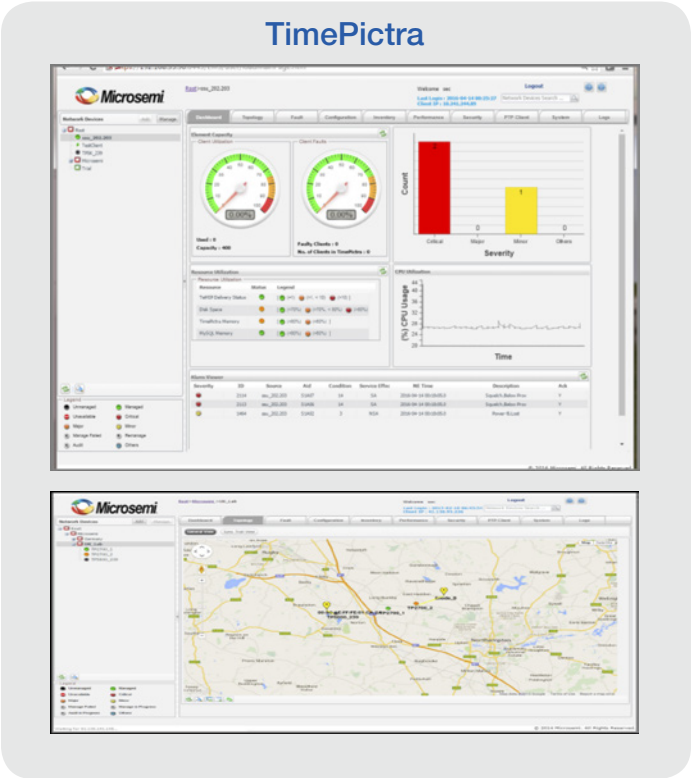
The Blue*Sky* GPS Firewall provides users control from a web-based graphical interface and the ability to update data validation rules

For small-scale deployments, the Blue*Sky* GPS Firewall provides an intuitive, web-based GUI where TimePictra may not be the right management solution. This GUI provides the same status and controls available through TimePictra and includes the ability to remotely update the Blue*Sky* client application and anomaly detection criteria.

As with any network connected device, network security is critical to ensuring continued operations. The Blue*Sky* GPS Firewall utilizes the following latest security measures and protocols to protect against network intrusion.

- Management: CLI over SSHv2, secure web-based management (HTTPS/SSL), and TimePictra support
- x.509 Certificate support, Radius, LDAP, TACACS+
- IPv4, IPv6 (future), DHCP, remote syslog logging

Within TimePictra, the Blue*Sky* GPS Firewall is managed as a network element similar to other Microsemi products. This includes auto discovery and alarm reporting, SV tracking details, latitude and longitude for mapping, remote control, and the ability to upgrade anomaly detection criteria or the entire Blue*Sky* client.



TimePictra manages the Blue*Sky* GPS Firewall and other Microsemi synchronization products

System Deployment

The Blue*Sky* GPS Firewall protects downstream users by monitoring the data contained within the GPS signals along with the GPS signal characteristics. When a GPS incident is detected, the Blue*Sky* GPS Firewall alerts users of the condition and takes appropriate action to prevent the GPS signal from propagating to downstream users, effectively creating the Blue*Sky* environment for users regardless of current live-sky GPS conditions.

Hardened GPS

Hardened GPS 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 Blue*Sky* GPS environment is created.

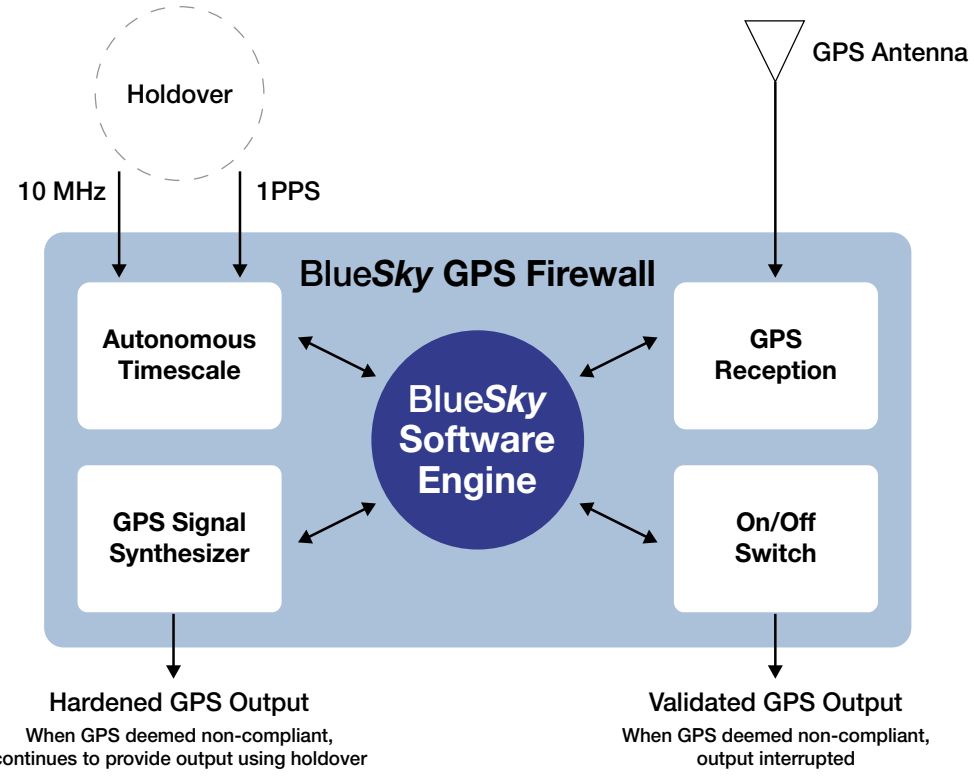
When GPS incidents are detected by the Blue*Sky* GPS Firewall, the hardened GPS output continues to be available. Downstream users can continue to use the hardened GPS signal during times of GPS jamming or GPS spoofing without impacting their system performance.

The hardened GPS output provides a synthesized version of the GPS L1 signal. Because the GPS L1 signal is supported by all current and foreseeable GPS based systems, it provides backward compatibility while also being future-proof.

Validated GPS

The Validated GPS output provides a copy of the actual GPS signal being analyzed by the firewall. When anomalous conditions are detected, the firewall turns the validated GPS output 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 Blue*Sky* GPS Firewall to provide an additional layer of protection. Also, mobile platforms can use the validated GPS signal without degrading the accuracy of their PNT solution.



Atomic Reference

External input capability from an atomic reference (10 MHz or 1PPS input) enables users to enhance the performance of the Blue*Sky* GPS Firewall. Adding an atomic reference enables the Blue*Sky* GPS Firewall to enhance its GPS event detection capabilities while also extending its ability to provide accurate time (using the hardened GPS output) during live-sky GPS incidents (or jamming). All downstream systems inherit the performance of the atomic reference being utilized by the Blue*Sky* GPS Firewall.

Secure Operations

Similar to network security threats, new GPS errors are on the rise and Microsemi is continuously tracking GPS signal manipulation including spoofing threats, jamming incidents, multipath signal interference, space weather, and many other issues that can create GPS signal anomalies, disruptions, and outages. At the core of the BlueSky GPS Firewall is a programmable anomaly detector that validates the GPS subframes for spoofing incidents based on defined data validation rules. A wide range of rules have already been built into the BlueSky GPS Firewall to detect suspicious time and position inconsistencies. As with traditional security firewalls, new validation rules are dynamically loaded into the BlueSky GPS Firewall as new threats are identified.

The Blue*Sky* GPS Firewall utilizes complementary algorithms based on fundamental observables and expected values to establish a layered defense in securing GPS signals. This provides protection against currently conceived threats and enables security updates to protect against future threats to maintain an evolving, secure system.

Data Validator

The Blue*Sky* GPS Firewall analyzes all data received from a GPS signal and validates that it complies with GPS standards and expected values. Otherwise, the signal is deemed to be non-compliant and actions are taken to prevent its dissemination to downstream systems.

A standard set of data validation rules are included on the Blue*Sky* GPS Firewall. They are based upon IS-GPS-200H. However, they are updatable by the user to provide any additional checks a user may want to implement based upon their knowledge of the live-sky GPS environment.

Time Waits for No Man

Nor does it speed up. Unique to Microsemi's Blue*Sky* GPS Firewall is the deployment of an autonomous timescale. An autonomous timescale is crucial to detecting anomalous GPS events because it provides an independent means of validating time from external sources (such as GPS). It enables a user to optimize the Blue*Sky* GPS Firewall to achieve their cost and performance requirements.

Signal Characteristics

Most GPS attacks are precipitated by a "knock-off" event that forces GPS systems to momentarily lose lock on actual GPS signals and then replace those signals with spoofed GPS signals. The Blue*Sky* GPS Firewall identifies potential knock-off events by analyzing incoming GPS signal power in conjunction with other indicators that detect the presence of potentionally corrupted GPS transmissions.

Hosted Applications

In addition to updating its data validation rules as threats evolve, the Blue*Sky* GPS Firewall can host third-party applications to enable entities (government or private) to develop applications hosted on the Blue*Sky* GPS Firewall that address their unique needs and protects their proprietary information.

Updates to GPS Data Validation Rules

Microsemi's experts are recognized leaders in the field of time and frequency synchronization. Similar to network security threats, new GPS errors are on the rise and Microsemi is continuosly tracking GPS signal activity. Microsemi's worldwide deployment of atomic clocks and GPS systems are used as a reference frame to continuously analyze GPS data for changes including spoofing threats, jamming attacks, multipath signal interference, atmospheric activity, and any other effect that degrades GPS performance.

New GPS data validation rules can be deployed using either Microsemi's TimePictra management software or the Blue*Sky* GPS Firewall's secure web-based interface.

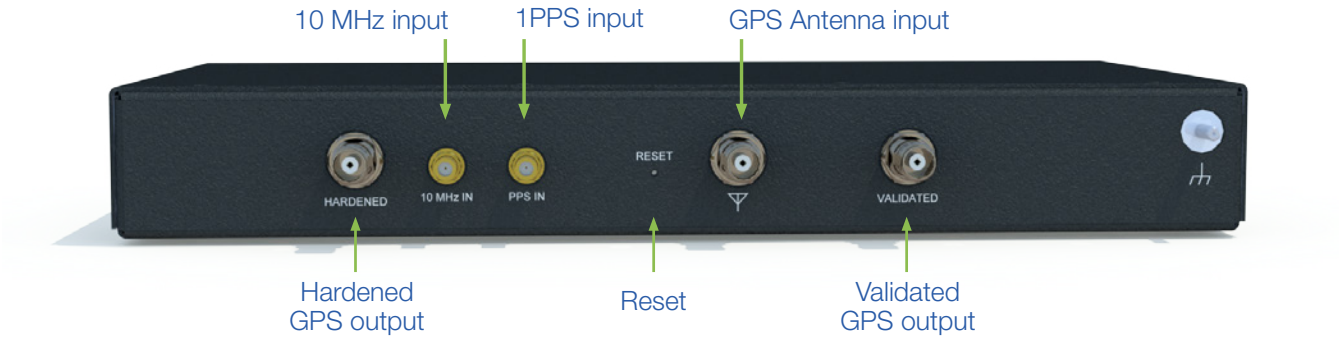
Features and Services

BlueSky GPS Firewall System Specifications

GPS Antenna Input	
Connector	TNC(F)
Impedance	50 Ω
Antenna bias voltage	0 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)
Satellites channels	12
Time transfer 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

Management, Power Interfaces, and Diagnostics	
Ethernet and POE	RJ45 tri-mode Ethernet (10/100/1000BASE-T) with Power-over-Ethernet (PoE) per 802.3a
Management	CLI over SSHv2, secure web-based management (HTTPS/SSL), and TimePictra support
User Authentication	x.509 Certificate support, Radius, LDAP, TACACS+
Network Interfaces	IPv4, IPv6 (future), DHCP, remote syslog logging
LEDs	Power, GPS valid, alarm
Mechanical/Environmental	
Size	1 U rack mount, 13” (W) × 6.7” (D) × 1.72” (H)
Operating temperature	0 °C to 50 °C
Operating humidity	0–95% (noncondensing)
Weight	2 lbs standalone, 3 lbs with shipping package
Regulatory Compliance	
EMC compliance	FCC part 15 (Class A)
Environmental compliance	RoHS (6 of 6)
Hardware Accessories Included	
Microsemi PD-3501 (single-port Power-over-Ethernet adapter)	
Mounting hardware for 19-inch rack	

BlueSky GPS Firewall Rear Panel



Services

Microsemi provides a wide range of services. With over 40 years of designing timing systems for mission-critical applications, Microsemi has comprehensive support resources available to ensure that customers are able to use all of the features of the BlueSky GPS Firewall.

Available services for the BlueSky GPS Firewall include:

- Site survey and verification
- Training
- 24/7 technical support
- Extended hardware warranty
- On-site installation
- Rapid Replacement Service

Microsemi's BlueSky™ GPS Firewall Evaluation Kit

Microsemi is continually adding new products to its industry-leading portfolio.

For the most recent updates to our product line and for detailed information and specifications, please call, email, or visit our website.

Toll-free: 800-713-4113

sales.support@microsemi.com

www.microsemi.com

Microsemi
Power Matters.™

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California and has approximately 4,800 employees globally. Learn more at www.microsemi.com.

MSCC-0104-BR-0106-1.00-0917