Protecting GNSS Systems Against Spoofing and Jamming Threats

BlueSky™ GNSS Firewall

MICROCHIP

microchip.com

Protect Existing GNSS Systems Today and Secure PNT Infrastructure for the Future

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 proliferation 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, data centers and emergency services are now highly dependent on PNT information delivered by GNSS.

BlueSky™ GNSS Firewall 2200

- Protects GNSS systems from spoofing and jamming
- Integrates seamlessly between existing GNSS antenna and downstream GNSS system
- Compatible with any GNSS antenna that receives the L1/L2/L5 frequencies
- Optional Rubidium Miniature Atomic Clock (MAC) can be configured inside to provide holdover
- Optional 1 PPS and 10 MHz timing reference inputs for connection of external references (such as cesium standards) providing resiliency even in case of complete GNSS outage
- Redundant AC or DC power supplies with hitless switching and load sharing
- Command Line Interface (CLI) in addition to secure and easy-to-use web interface
- BlueSky GNSS Firewall embedded software is field upgradeable
- Integration with TimePictra™ provides end-to-end management of 10s, 100s or 1,000s of units deployed over large geographical areas
- BlueSky performance monitoring provides visibility of GNSS reception quality (software option that runs within TimePictra)

Applications

- Wireline and wireless networks
- Utility and power grids
- Data centers
- Transportation networks
- Emergency services
- Financial services
- Secure government networks

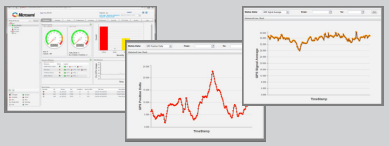
Secure Firewall Overlay

The BlueSky GNSS Firewall solves the problem of protecting already deployed systems by providing a cost-effective overlay solution installed between existing GNSS antennas and GNSS 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 GNSS signal. The BlueSky software engine analyzes received signal characteristics for both GPS and Galileo and in the case of GPS, received data is evaluated from each satellite to ensure compliance with GPS standards. This information is used by the firewall to block anomalous GNSS signals and provide a secure GNSS signal output to downstream GNSS systems.

The BlueSky GNSS Firewall also supports a range of atomic clock technologies enabling continuous operation where GNSS may be completely denied for extended periods of time, even in cases where disruptions may last for more than 30 days. The system incorporates an optional internal Rubidium MAC enabling continuous output of the GNSS signal to the downstream GNSS receiver in case of complete loss of live sky GNSS reception. Alternatively, cesium clocks, such as the 5071A or TimeCesium can be connected to the BlueSky GNSS Firewall enabling UTC traceable time for more than 30 days.

Management and performance monitoring of wide scale deployment of the BlueSky GNSS Firewall units is simplified using the TimePictra management system. TimePictra also includes BlueSky performance monitoring that enables a regional, national, or global view of your PNT infrastructure to provide early alerting to threats before your PNT network is affected.

GNSS Threat Protection Stack	
Protect Existing GNSS Systems with Secure Firewall Overlay	
Atomic Clock Resiliency for continued operations during extended outages	
Visibility, Measurement and Monitoring over regional or national geographies	

Secure Firewall Overlay

BlueSky GNSS Firewall is deployed in-line between an existing GNSS antenna and GNSS receiver system. The BlueSky GNSS Firewall analyzes incoming GNSS signals from the antenna to identify anomalous or spoofed GNSS signals.

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

The BlueSky GNSS Firewall installs in a standard 19-inch rack and can be placed near the GNSS receiver system or near the point at which the GNSS antenna cable enters the building. Power for the GNSS antenna is provided by the BlueSky GNSS Firewall using a software configurable setting for 0, 3.3, 5 or 12 VDC. Thus, nearly all currently deployed GNSS antennas are supported without modifying the existing installation.

Power for the BlueSky GNSS Firewall is provided by redundant and hitless AC or DC power supplies contained within the system. The power supplies use load share equally, which improves overall reliability, and an active power management system constantly monitors the operation. If the power to one cord is lost or if one power supply fails, the entire load is immediately picked up by the remaining energized power supply with no interruption to the GNSS signal delivery.

Critical Infrastructure

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.

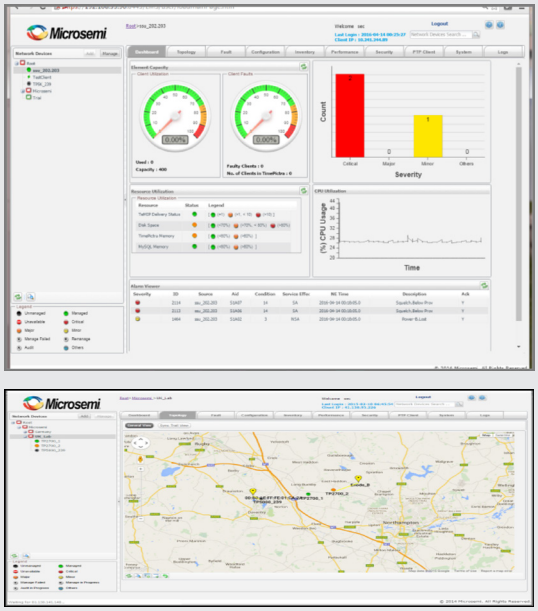
The software environment of the BlueSky GNSS Firewall integrates seamlessly with TimePictra management system. TimePictra is a web-based management system for time, frequency, and synchronization of network elements. It features a modular architecture that scales and evolves to address new or changing operational requirements. When using TimePictra to manage a deployment of BlueSky GNSS Firewall devices, users have centralized control and visibility of their network to ensure their enterprise is operating properly.

Within TimePictra, the BlueSky GNSS Firewall is managed as a network element similar to other products. This includes auto discovery and alarm reporting, latitude and longitude for mapping, remote control and the ability to upgrade anomaly detection criteria or the entire BlueSky client.

As with any network connected device, network security is critical to ensuring continued operations. The BlueSky GNSS Firewall uses the latest security measures and protocols to protect against network intrusion.

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

TimePictra

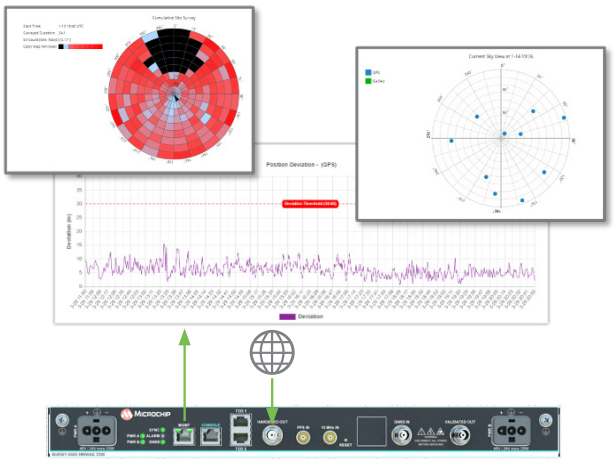


TimePictra manages the BlueSky GNSS Firewall and other synchronization products

Available as an option within TimePictra is BlueSky performance monitoring. This set of features enables performance charting of GNSS reception through data collection from individual BlueSky GNSS Firewalls. The BlueSky performance monitoring software option enables visibility of GNSS reception parameters across a wide-scale deployment of firewalls. GNSS signal analytics such as GNSS phase deviation, GNSS satellites in view status, GNSS signal strength, RF power level, GNSS satellite tracking, GNSS position data, and phase error as measured between the GNSS time and the internal time scale of the firewall can all be viewed from a centralized console. Specific time periods can be selected for plotting and identifying exactly when and where an anomaly occurred. This aids critical infrastructure operations to more quickly identify and isolate GNSS incidents.

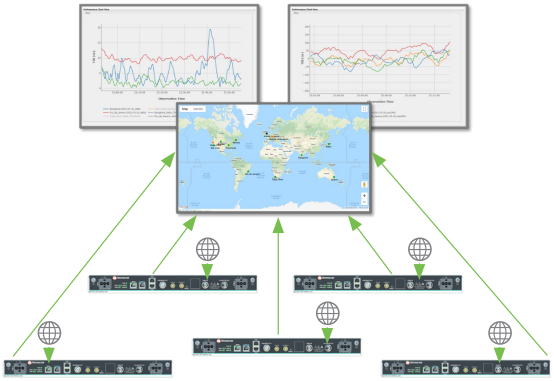
For direct user management, the BlueSky GNSS Firewall provides an intuitive, web-based GUI. This GUI provides basic status and control and includes the ability to update the BlueSky client application and anomaly detection criteria.

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.

System Deployment

The BlueSky GNSS Firewall provides protection by monitoring the data contained within the GNSS signals along with the GNSS signal characteristics coming directly from the GNSS antenna before the GNSS signal reaches the downstream receivers. When a GNSS incident is detected, the BlueSky GNSS Firewall alerts users of the condition and takes appropriate action to prevent the GNSS signal from propagating downstream, effectively creating the BlueSky environment for users regardless of current live-sky GNSS conditions.

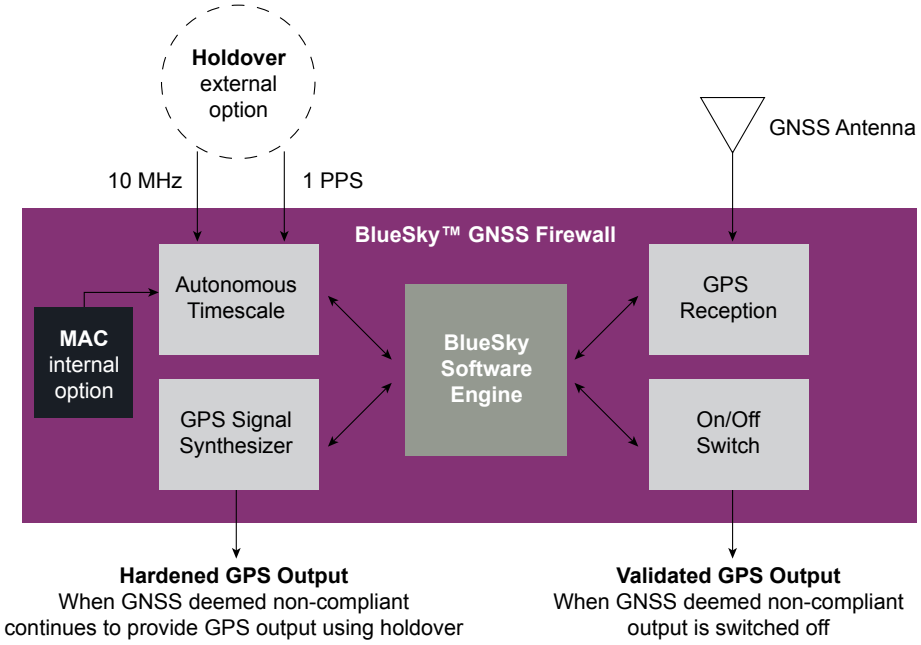
Hardened GPS Output

Hardened GPS Output is the most secure 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 by the BlueSky GNSS 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.

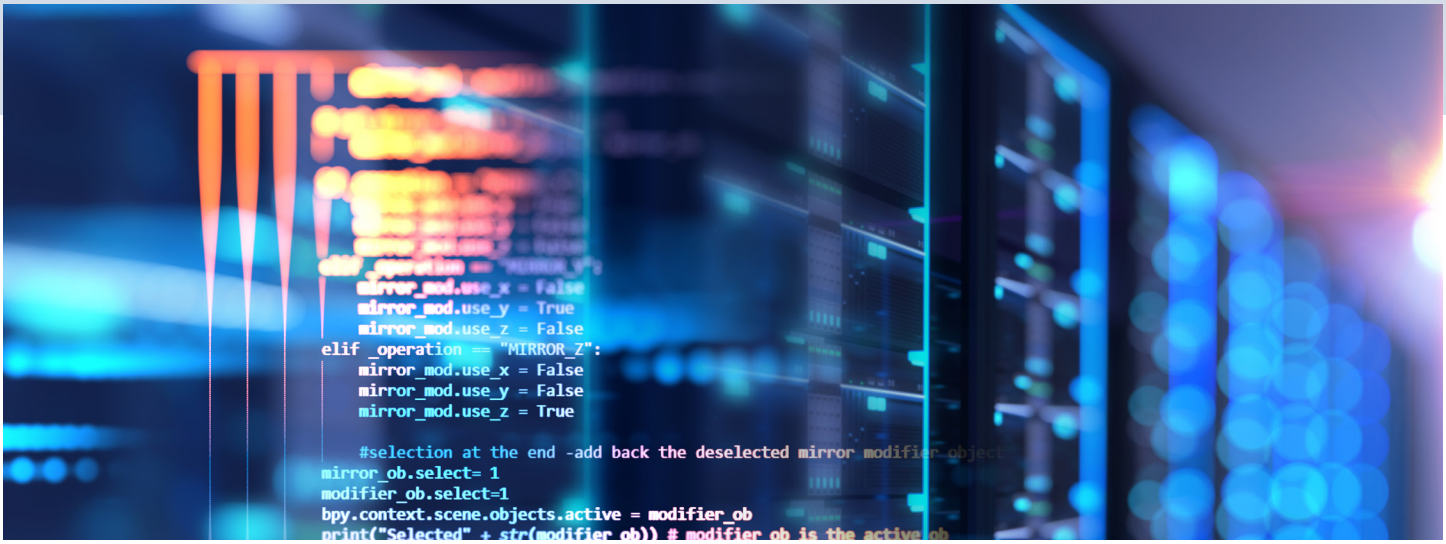
The hardened GPS output provides a synthesized version of the GPS L1 signal. Because the GPS L1 signal is supported by all current and foreseeable GPS based systems, it provides backward compatibility while also being future-proof.



Validated GNSS Output

The Validated GNSS output provides a copy of the actual GNSS signal being analyzed by the firewall. When anomalous conditions are detected, the firewall turns the validated GNSS output off to protect users from potentially corrupted GNSS signals. Once conditions are deemed safe, the validated GNSS output is turned back on.

The validated GNSS output also includes copies of the L1, L2, and L5 signals on a single output. This enables downstream systems that use multiple GNSS frequencies (such as SAASM or M-code) to use the BlueSky GNSS Firewall to provide an additional layer of protection. Because the validated output is a pure copy of the input, if other constellation bands are being received, such as Galileo, GLONASS and Beidou, these signals are available on the validated output as well. The GLONASS and Beidou satellite signals are simply passed through, but not analyzed as with the GPS and Galileo signals.



Secure Operations

Atomic References

The BlueSky GNSS Firewall provides two options for atomic references to be connected: (1) inside the BlueSky GNSS Firewall, a Rubidium MAC can be installed, or (2) atomic references (such as TimeCesium or 5071A cesium clocks) can be connected using the 10 MHz or 1 PPS inputs. Adding an atomic reference enables the BlueSky GNSS Firewall to enhance its GNSS event detection capabilities while also extending its ability to provide accurate time (using the hardened GPS output) during live-sky GNSS incidents. All downstream systems inherit the performance of the atomic reference being utilized by the BlueSky GNSS Firewall and GPS time continues to be delivered even in the case of a complete outage of the GNSS signal input.

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

The BlueSky GNSS Firewall uses advanced algorithms based on fundamental observables and expected values to establish a layered defense in securing GNSS 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 BlueSky 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 BlueSky GNSS Firewall. Additionally, the BlueSky subscription service provides users with access to new validation rules which can be securely installed on the BlueSky GNSS Firewall to protect against new threats.

Autonomous Time Scale

Unique to the BlueSky GNSS Firewall is the deployment of an autonomous time scale. An autonomous time scale is crucial to detecting anomalous GNSS events because it provides an independent means of validating time from external sources (such as GNSS). A user can optimize the BlueSky GNSS Firewall to achieve their cost and performance requirements using an optional internal MAC or by using external references such as cesium clocks.

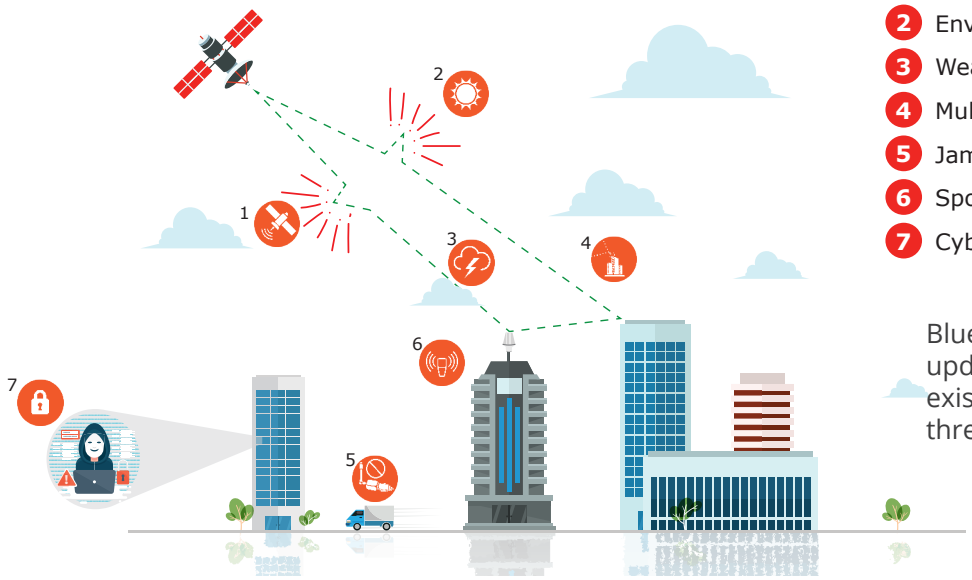
Signal Characteristics

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

Updates to GNSS Data Validation Rules

Microchip is continuously tracking GNSS signal activity. Microchip's worldwide deployment of atomic clocks and GNSS systems are used as a reference frame to continuously analyze GNSS data for changes including spoofing threats, jamming attacks, multipath signal interference, atmospheric activity and any other effect that degrades GNSS performance.

New GNSS data validation rules, available as part of the BlueSky Subscription service, can be deployed using either TimePictra management software or using the BlueSky GNSS Firewall's secure web-based interface.



1. Satellite Error
2. Environmental Effects
3. Weather Anomolies
4. Multipath Interference
5. Jamming
6. Spoofing
7. Cyber Attack

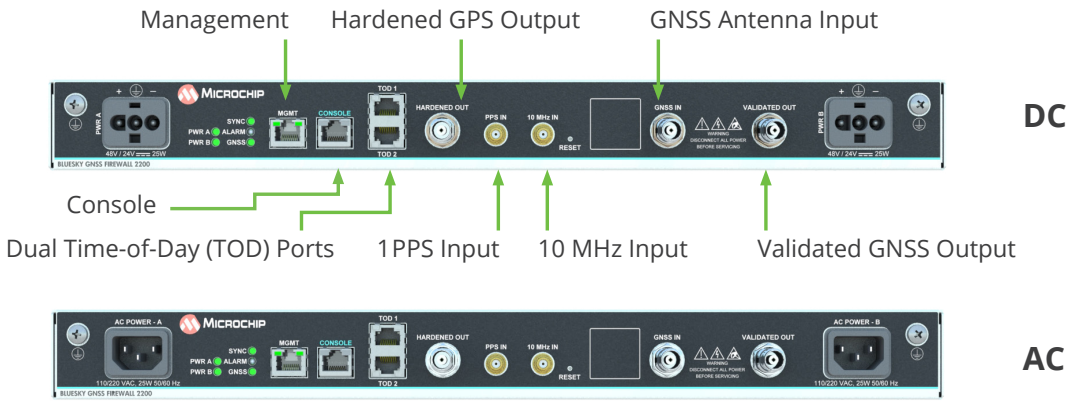
BlueSky GNSS Firewall can be updated to protect against existing and emerging GNSS threats

Features and Services

GNSS Antenna Input	
Connector	TNC(F)
Impedance	50Ω
Antenna Bias Voltage	0 VDC, 3.3 VDC, 5 VDC, 12 VDC (software selectable)
Hardened GNSS 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)
Satellites	8
Time Transfer Accuracy	Meets or exceeds live-sky performance
Validated GNSS Output	
Output interrupted when GNSS is non-compliant	
Connector	TNC(F)
Impedance	50Ω
1PPS Input	
Connector	SMA(F)
Impedance	50Ω
Signal Format	TTL compliant

10 MHz Input	
Connector	SMA(F)
Impedance	50Ω
Level	3 dBm to 13 dBm
Management, Power Interfaces and Diagnostics	
Time of Day (TOD) ports	Bidirectional 1PPS+TOD for connection to Microchip TimeProvider products
AC or DC power	Redundant AC or DC power supply options with load sharing and hitless switching
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, DHCP, remote syslog logging
LEDs	Power A & B, Sync, Alarm, GNSS

BlueSky GNSS Firewall 2200



Services

Microchip provides a wide range of services. With over 40 years of designing timing systems for mission-critical applications, we have comprehensive support resources available to ensure that customers are able to use all of the features of the BlueSky GNSS Firewall. The BlueSky subscription service provides on-going improvements to the GNSS anomaly detectors contained within the BlueSky GNSS Firewall. Details of this service are available on a separate BlueSky subscription datasheet. Additional services for the BlueSky GNSS Firewall include:

- Site survey and Verification
- On-site installation
- Consulting Services
- Training
- Extended Hardware Warranty
- Rapid Replacement Service

Please register through the online support portal at my.microsemi.com. A broad collection of information is available through the portal and Microchip will keep you informed of important updates once you have registered.

Microchip Technology Inc. | 2355 W. Chandler Blvd. | Chandler AZ, 85224-6199 | microchip.com

DS00003096B