BlueSky™ GNSS Firewall - Software Release 3.0

Protection for Position, Navigation and Timing (PNT) Used by Critical Infrastructure

Summary

Position, Navigation and Timing (PNT) threats resulting from the vulnerability of GNSS signal manipulation and degradation such as spoofing and jamming is on the rise. The Department of Homeland Security (DHS) recently published the Resilient Positioning, Navigation, and Timing (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.

Key Features

- Secure Firewall provides barrier between untrusted GNSS sky signals and downstream systems
- BlueSky Information Charts for quick monitoring of key GNSS observables
- Configurable GNSS thresholds: Carrier-to-Noise, RF power, Satellites-in-View, Position Deviation, Phase Time Deviation and more
- New Trusted Time™ Anomaly Detector for comparing Network Time and GNSS Time
- New GPS Subframe Reference detection enabling the comparison of live-sky sub-frame data with sub-frame data received from a remote BlueSky GNSS Firewall
- Interoperable with TimePictra providing multi-site visibility and situational awareness

Protection against GNSS Threats needs to be part of a Cybersecurity plan

Systems which rely on GNSS for reception of Position, Navigation and Time (PNT), have been determined by national security agencies across the globe as potential cybersecurity attack vectors. Therefore, as described in the DHS Resilient PNT Conformance Framework, a cybersecurity approach has been proposed:

- **Prevent:** The first layer of defense. Idealy threats are prevented from entering a system, however, it must be assumed that it will not be possible to stop all threats.
- **Respond:** Detect atypical errors or anomalies and then take action such as mitigation, containment and reporting. The system should ensure an adequate response to externally induced, atypical errors before recovery is needed.
- **Recover:** Return to a proper working state and defined performance. It serves as the last line of defense.

Four Levels of Resilience

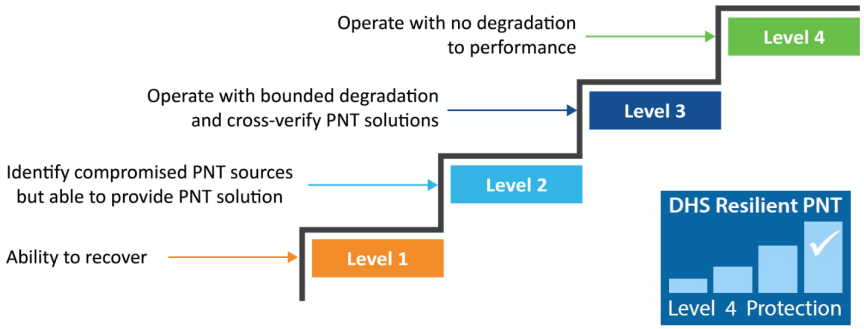
Based on the Prevent-Respond-Recover cybersecurity model, the PNT Conformance Framework document describes 4 levels of resilience. Note that the resilience levels build upon each other, that is, Level 2 includes all enumerated behaviors in Level 1, and so forth.

Using the BlueSky GNSS Firewall either as a standalone security barrier or in combination with Microchip's high-performance atomic clocks and timing distribution systems, all four levels of resilience can be achieved and exceeded.

Advanced Tools and Centralized Management

Release 3.0 further enhances the BlueSky GNSS Firewall's already field proven GNSS protection capabilities with new capabilities such as Trusted Time Anomaly Detection, GPS Subframe Reference Detection, embedded GNSS observable tools combined with new TimePictra Performance Monitoring features to

better secure, monitor, prevent, respond and recover to GNSS threats. Critical Infrastructure providers now have the most advanced set of tools for defending against all intentional or unintentional vulnerabilities and threats and achieving Level 4 Resilience as defined by the DHS PNT Conformance Framework.



Achieving Level 4 Resilience

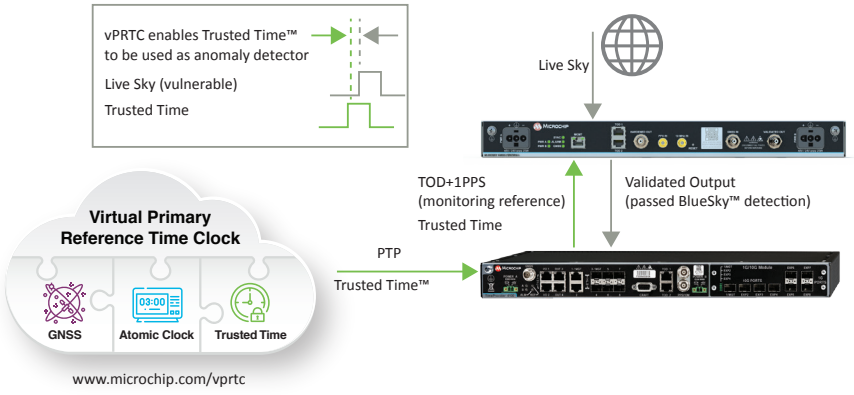
Using the BlueSky GNSS Firewall in combination with Microchip's atomic clocks and GNSS detectors enables Level 4 Resilience

Virtual Primary Reference Time Clock and the Trusted Time™ Anomaly Detector

The virtual Primary Reference Time Clock (vPRTC) is a highly secure and resilient network-based timing architecture that has been developed to meet the expanding needs of modern critical infrastructures. The vPRTC is simple in concept. It blends proven timing technologies into a centralized and protected source location and then uses commercial fiber optic network links and advanced IEEE® 1588 Precision Time Protocol (PTP) boundary clocks to distribute 100 ns PRTC timing where it is needed in end points that might be hundreds of kilometers away.

With these highly resilient clocks in place, critical infrastructure operators can use their secure fiber network to distribute protected timing to all necessary locations. Just as a GNSS-satellite-based timing system distributes timing to end points using open-air transmission, the vPRTC distributes timing using the fiber network. The difference is that the operator remains 100% in control of the network and can secure it as necessary. This network-based timing is referred to as Trusted Time. Using the vPRTC architecture, Trusted Time can be distributed as the primary source of timing or it can be deployed as a backup to GNSS timing solutions.

Release 3.0 of the BlueSky GNSS Firewall can make use of Trusted Time as an anomaly detector for GNSS Vulnerabilities. Using the TimeProvider 4100 as a high-performance boundary clock (HPBC), Trusted Time can be connected to the BlueSky GNSS Firewall using the standard Time-of-Day (TOD) interface or the 1PPS signal input. This enables the BlueSky GNSS Firewall to measure and compare the incoming live-sky signal to the Trusted Time as delivered over the network. The result is that the Trusted Time Anomaly detector within the BlueSky GNSS Firewall can alarm if the "network time" and the "GNSS time" drift too far apart.



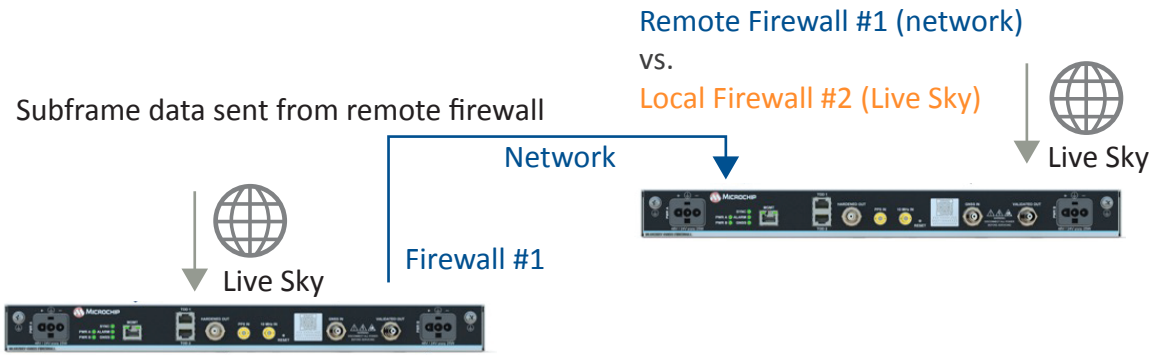
Trusted Time Anomaly Detector enables network (terrestrial) based time to cross check GNSS time

Using the Validated Output of the BlueSky GNSS Firewall, the GNSS signal is passed through to the downstream TimeProvider 4100 after being verified by the BlueSky detection algorithms, including the Trusted Time detector. If the live sky signal is determined to be compromised, the Validated Output is turned off and the TimeProvider 4100 enters holdover.

The Trusted Time Anomaly Detector can use either the TOD or the 1PPS input for monitoring. The threshold (phase difference between Live Sky and Trusted Time) for triggering an alarm is configurable by the user.

GPS Subframe Reference Detection

Release 3.0 of the BlueSky GNSS Firewall enables a revolutionary new approach to verify GNSS reception using a technique called GPS Subframe Reference Detection. Redundant BlueSky GNSS Firewall systems can be deployed throughout a building, across an airport, rail station, maritime port, datacenter or across large geographical areas and can be interconnected together to compare subframe data. The remote BlueSky GNSS Firewall can be identified as the "truth source" such that the local BlueSky GNSS Firewall compares it's locally received live sky subframe data to the remote (trusted) subframe data coming from the remotely deployed Firewall. If a difference is detected, then an alarm can be generated to indicate a miss-match (i.e., an anomaly).



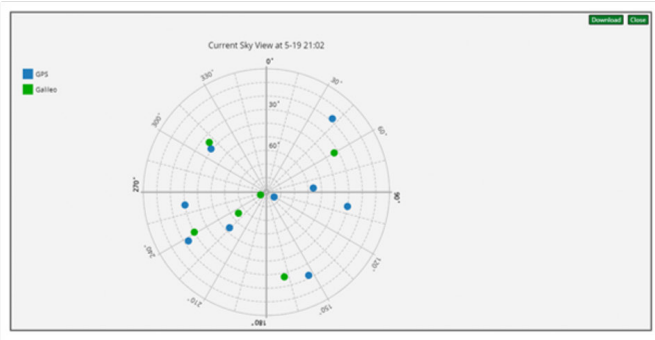
GPS Subframe Reference Detection enables subframes from remote Firewall to be compared to subframes being received from the live-sky signal within local Firewall

Embedded Tools for set-up and viewing GNSS Observables

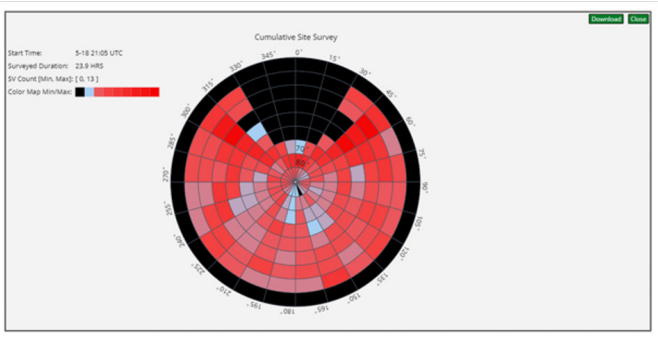
Securing GNSS delivered PNT services requires tools that can deliver efficient tactics for managing, monitoring and responding to threats. Small deployments can many times be managed directly using the Web GUI that is provided directly from the BlueSky GNSS Firewall. The built-in WebGUI of the BlueSky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

GNSS Antenna Site Survey Tools

Assure proper antenna placement with live-sky satellite maps and cumulative site survey measurements. Useful to determine if an adequate view of the sky is available for normal GNSS operations, or if parts of the sky might be obscured by local surroundings.



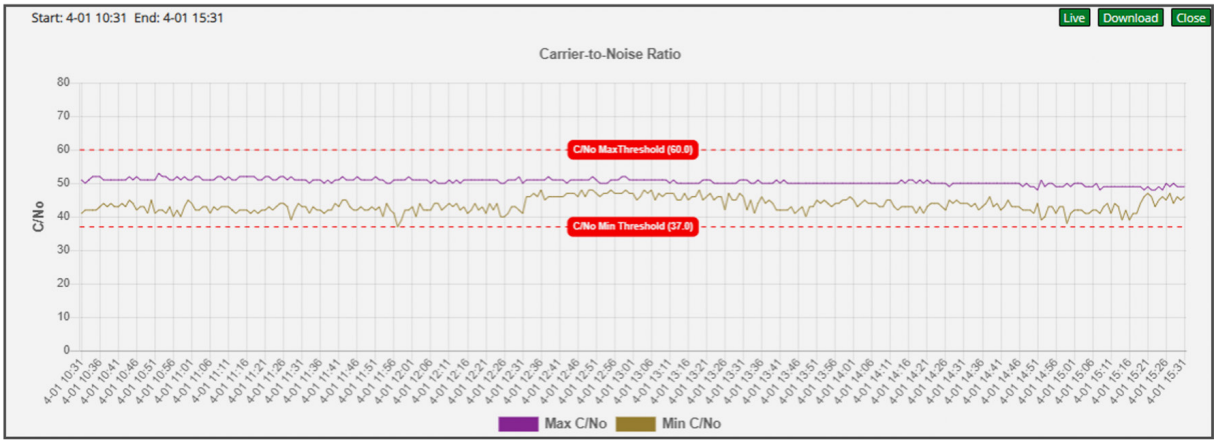
All-in-view look at currently tracked GNSS satellites to assure an acceptable view of the sky.



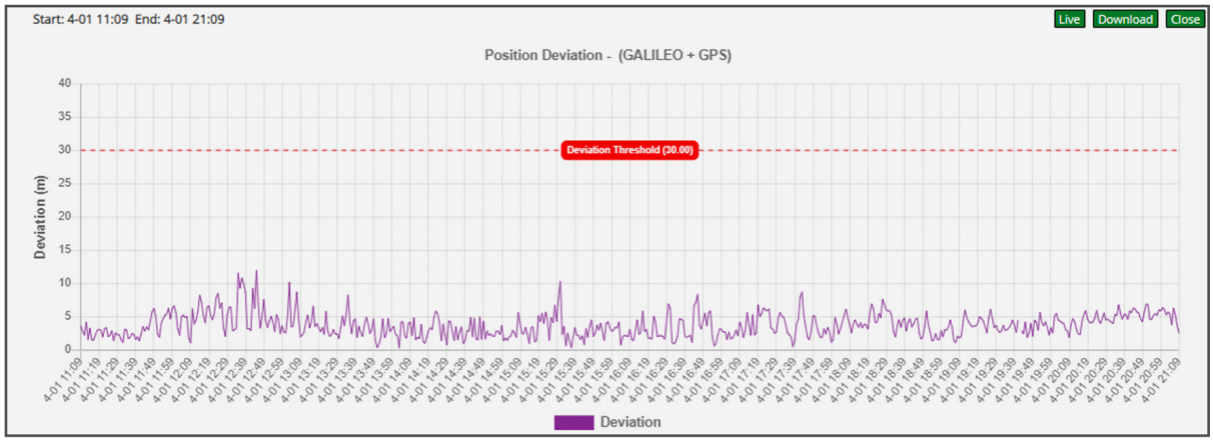
View which segments of the sky most frequently have Satellite signals. Red = frequent satellites, blue = occasional satellite signals, black = satellites not tracked.

At-a-Glance Dashboard and Signal Detector Measurements

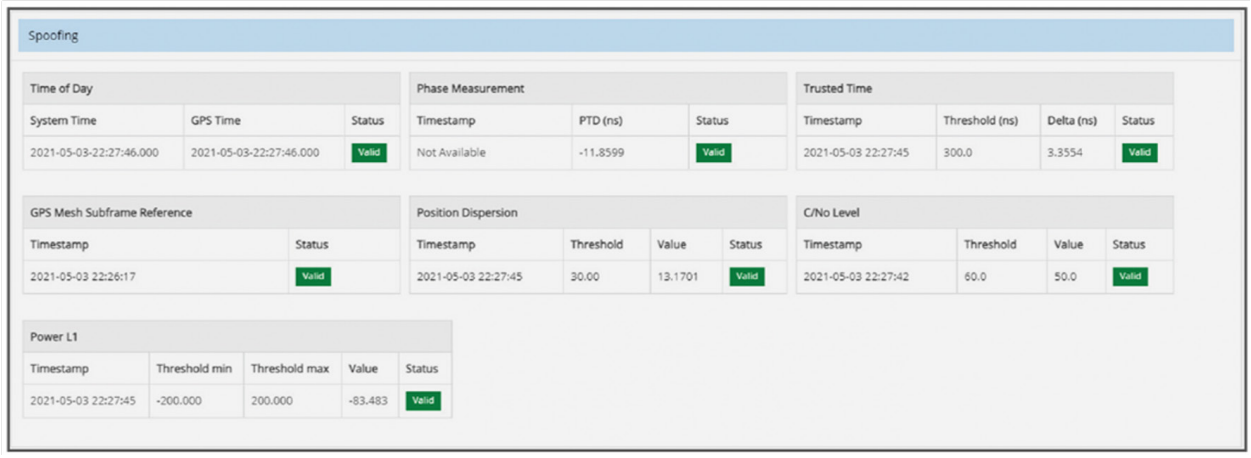
Using the embedded Web GUI, the BlueSky GNSS Firewall provides insights into measured GNSS signal qualities and data validator anomalies. The direct web access makes set-up and diagnostics simple and provides an immediate view to the status of key GNSS observables. Examples include Position Deviation, Carrier-to-Noise issues and verification that RF power levels are within range.



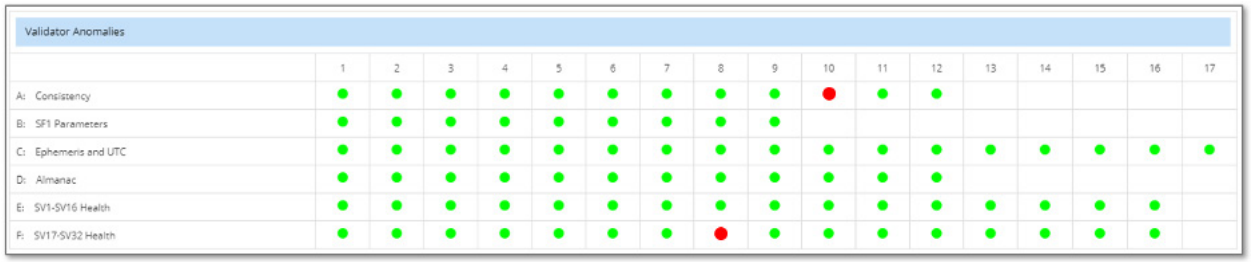
Carrier-to-Noise (C/No) measurements with the red lines indicating the alarm thresholds



Position deviation measurements with the red line indicating the current alarm threshold



GNSS Integrity Status provides at-a-glance view of GNSS health reception

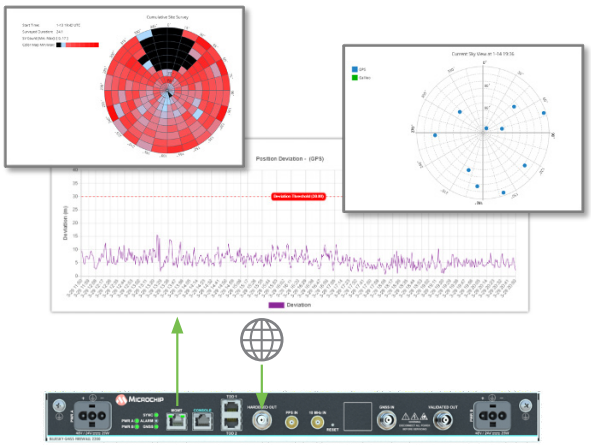


Validator Anomalies dashboard provides status LEDs for GPS satellites

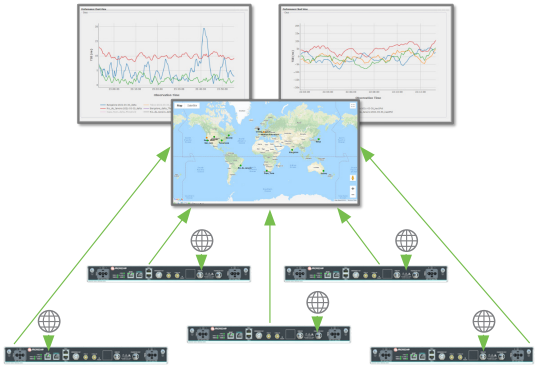
The charts and graphs provide both “real-time” charting and historical look-back of data to fine tune alarm thresholds. The historical data is also valuable to identify when a jamming or spoofing event occurred and possibly correlate it to known changes in the local RF environment. All data can be exported for further analysis.

Centralized Management 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, whether the GNSS problem appeared the same at different sites, whether the problem is occurring periodically at different locations are all example questions that surface immediately upon a GNSS threat being detected. The BlueSky GNSS Firewall Software Release 3.0 software integrates seamlessly with the TimePictra management system.



WebGUI for Set-up and Viewing From a Single Firewall



Centralized Management of Multiple Firewalls using TimePictra for Critical Infrastructure

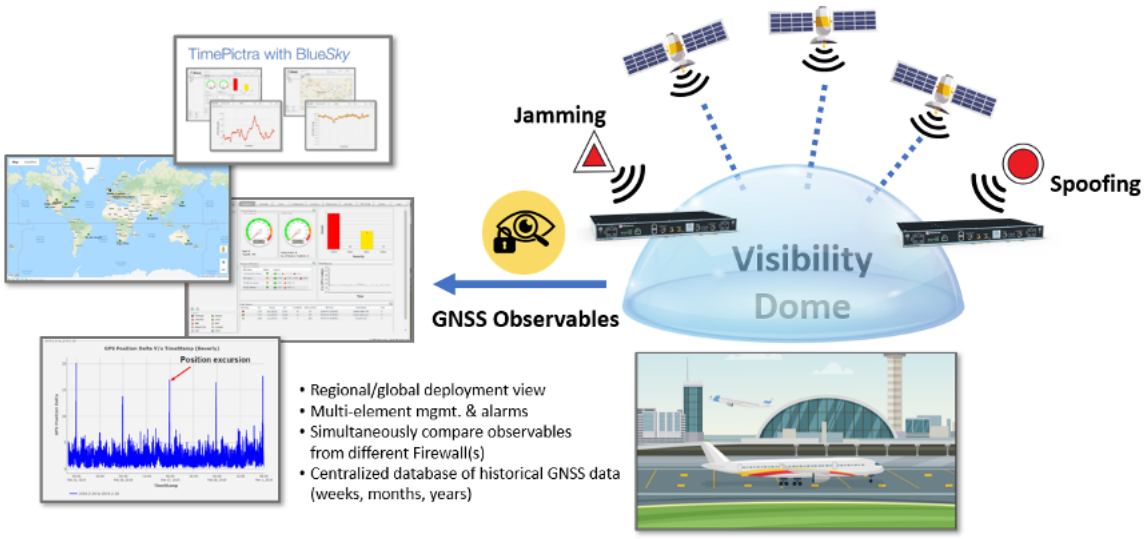
When using TimePictra to manage a deployment of BlueSky GNSS Firewalls, users have centralized control and visibility of GNSS reception. This is especially valuable for use cases in critical infrastructure that support transportation industries such as aviation, rail stations and maritime ports.

PNT services that are used across transportation infrastructure can be separated into two parts. One part being the use of Position and Navigation services. The applications for Position and Navigation are far reaching from asset tracking to fuel truck dispatching to avoiding train-to-train collisions to assisting vessels with their position in congested harbors. And then common across all these sectors is the need for very accurate, precise and now very resilient timing for network communications. The networks that these transport infrastructures rely on must be extremely secure and therefore the timing for these networks must also be well protected and robust.

Better securing the use of GPS within the aviation industry has recently taken on an even higher level of importance as the FAA issued an order (FAA Order Number 1770.68) which establishes the policy by which the FAA will use time and frequency sources for systems, services, and applications supporting National Airspace System (NAS) operations in order to ensure safety, security, required performance, and resilience.

As stated in section 5c of the FAA order:
GNSS satellite signals are extremely low power and are susceptible to interference caused by a variety of events, including jamming, spoofing, space weather, spectrum encroachment, and infrastructure disruptions. If the NAS (National Airspace System) experiences these disruptions or manipulations, then operations using GNSS time and frequency can receive degraded, misleading signals or cease to receive time/frequency inputs. FAA may even need to replace malfunctioning equipment to restore services, resulting in potentially significant impacts to NAS capacity and efficiency.

Preventing GNSS threats from causing disruptions begins with visibility into the quality of the live-sky GNSS signal. This visibility is best achieved by monitoring key GNSS observables which are used to calculate position, navigation and time. Examples of GNSS observables include tracked satellite count, RF power level, carrier-to-noise ratio and phase-time-deviation measurements. Just as a network firewall detects and protects against network attacks, the BlueSky GNSS Firewall using TimePictra delivers visibility of jamming and spoofing threats to alert transportation operations of untrusted sky-based signals.



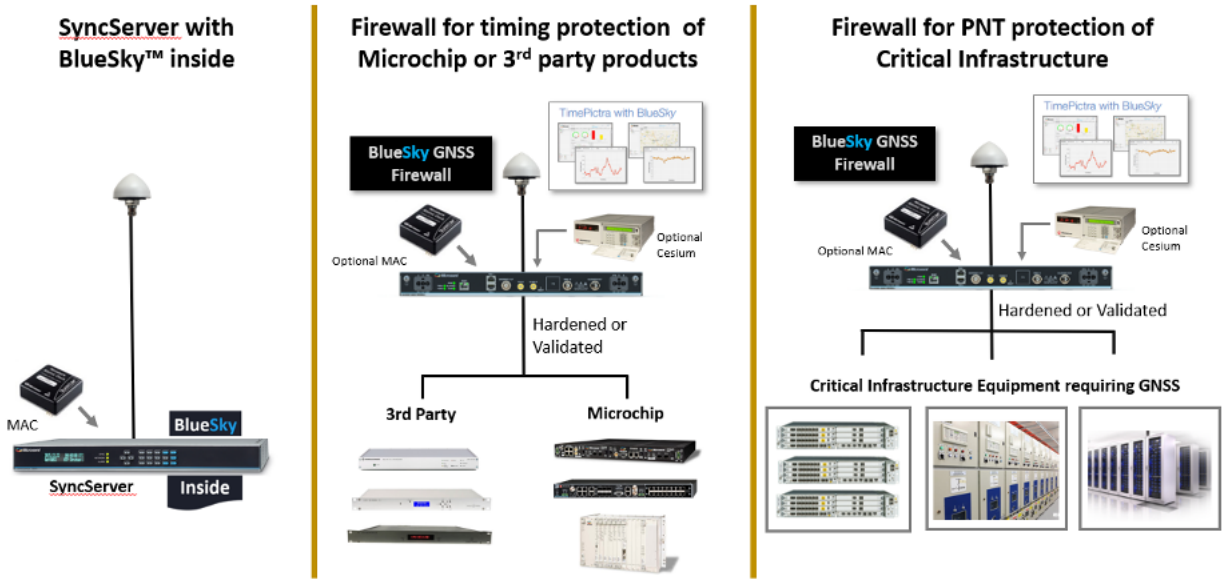
BlueSky GNSS Firewalls & TimePictra BlueSky Performance Monitoring deployed for situational awareness

While the firewall provides situational awareness of live-sky GNSS reception for position and navigation, in parallel the firewall secures private network communications as part of the Virtual Primary Reference Time Clock (vPRTC). The vPRTC is a highly secure and resilient network-based timing architecture that blends secure GNSS firewall technology, high-precision atomic system clocks and a portfolio of trusted time solutions to meet the expanding needs of modern critical infrastructures such as those required by Critical Infrastructure (CI) transportation (for more information go to www.microchip.com/vprtc).

The combination of GNSS visibility using TimePictra and the vPRTC architecture provides CI transportation operators with a dual-purpose solution for securing the use of PNT services as delivered by GNSS. It provides situational awareness about the health of GNSS reception by monitoring and evaluating key GNSS observables in real time to determine if there is risk in the use of PNT services delivered by GNSS. It also offers a layer of protection that enables a more responsible use of PNT services, including greater resiliency if live-sky delivery of PNT by GNSS is disrupted, degraded, or worse, becomes unavailable. Like a network firewall, this solution creates a dome of protection that strengthens the overall use of PNT services delivered by GNSS for CI transportation.

Resilient Positioning, Navigation and Timing (PNT) Deployment Models

Microchip's BlueSky offerings solve a range of different use cases and applications. Beginning with the SyncServer and BlueSky inside, this simple embedded solution protects a single SyncServer from GNSS threats. Moving to the right in the diagram below, the BlueSky GNSS Firewall is a simple overlay solution that can protect 3rd party timing servers as well as any of the Microchip timing products such as the SSU 2000 and TimeProvider 5000. It's important to note that a single Firewall can protect multiple products which is many times the situation in locations where there are legacy timing and new packet timing products co-located. On the far right of the diagram, the BlueSky GNSS Firewall is providing GNSS protection directly to critical infrastructure that requires access to GNSS. Examples are cellular base station equipment, utility substations and data centers.



BlueSky Deployment Models