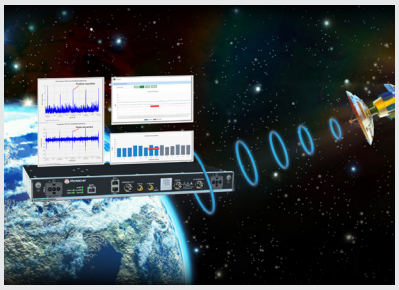
BlueSky™ GNSS Firewall Software

Release 2.0

Summary

New GNSS threats are on the rise including GNSS signal manipulation and degradation such as spoofing threats, jamming incidents, multipath signal interference, space weather conditions and many other issues that can create GNSS signal anomalies, disruptions and outages. At the core of the BlueSky™ GNSS Firewall is a software platform which detects suspicious inconsistencies coming from the live-sky GNSS environment. The BlueSky GNSS Firewall Software Release 2.0 provides new features and security hardening to maintain an evolving, secure system.



The BlueSky GNSS Firewall uses advanced anomaly detectors based on GNSS observables and theshold values to establish a layered defense in securing GNSS signals. The anomaly detectors are organized into three general categories:

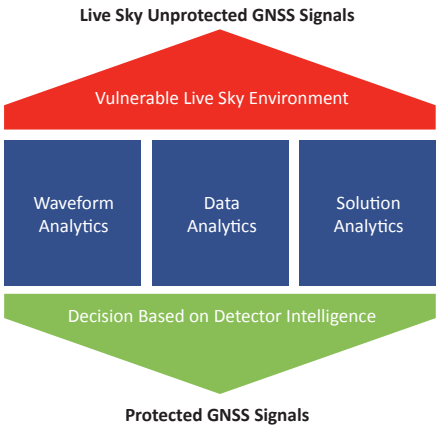
Waveform Analytics – Most GNSS attacks are precipitated by a "knock-off" event that forces GNSS systems to momentarily lose lock on actual GNSS signals which can be replaced with spoofed GNSS signals. The BlueSky GNSS Firewall identifies potential knock-off events by analyzing incoming GNSS signal power in conjunction with other indicators that detect the presence of potentially false GNSS signal transmitters.

Data Analytics – Analysis is performed on data received from a GNSS signal and validates that it complies with expected values. If data inconsistencies are detected (such as incorrect week number, false leap second information, erroneous satellite ephemeris, etc.), the signal is deemed to be non-compliant and actions are taken to prevent its dissemination to downstream systems.

Solution Analytics – Measuring observables such as time, position and velocity are another key part of detecting GNSS vulnerabilities. Unique to the BlueSky GNSS Firewall is the internal autonomous timescale. The autonomous timescale is crucial to detecting anomalous GNSS events because it provides an independent means of validating time from external sources (such as the live-sky GNSS signal itself).

Features

- Improved resiliency for smart recovery from deliberate threats or natural incidents
- BlueSky information charts for quick monitoring of key GNSS observables
- Configurable thresholds: Carrier-to-Noise, RF power, Satellites-in-View
- Simplified configuration of GPS or Galileo constellation reference settings
- SNMP configuration from the webGUI and MIB download
- Improved alarm management
- System logs downloadable for remote troubleshooting
- Interoperable with TimePictra® 10.9 SP1, TimePictra 10.10 and TimePictra Enterprise Edition



Protection aggregats information from multiple detectors

Data from the anomoly detectors is processed by a decision engine to determine the signal validity. A good decision engine is not simply based on the “number of rules” that the signal can be checked against but instead comes from making decisions based on the aggregated information. Single-mode anomaly detectors and protection technologies (for example, an anti-jam antenna) can create false alarms since they don't have the intelligence to fully analyze the potential threat in its entirety.

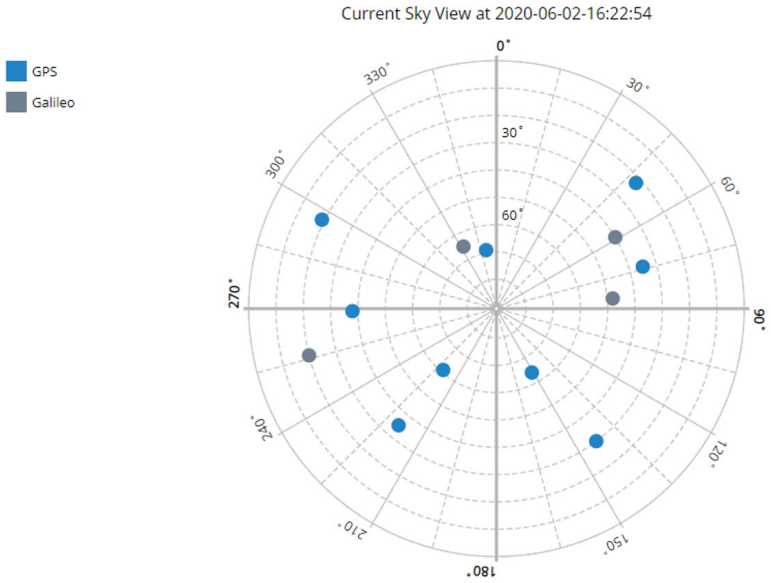
Programmable Observable Thresholds

In the BlueSky GNSS Firewall Software 2.0 Release, programmable thresholds are available so that the end-user can customize GNSS observables to achieve their desired level of security. The table below shows the observables for which thresholds can be set:

Observable	Description of Measurement
Satellites in View	Are the satellites in their expected locations?
Tracked Satellite Count	Are the number of satellites in view as expected (note: minimum is 4)?
Carrier-to-Noise Level	Is the strength of the satellite signal being received above a minimum level?
Phase Time Deviation	Is the live sky “time” moving? (as measured against a rubidium or cesium reference)
Position Dispersion	Is the position data from the sky moving too much?
RF Power	Is the RF power level within the expected threshold?

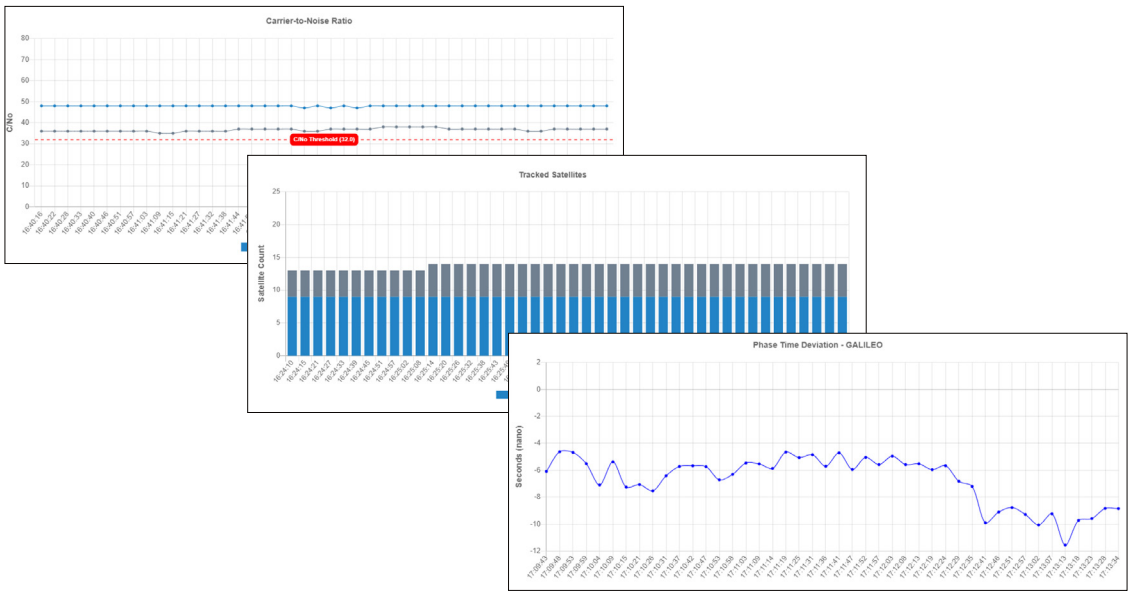
BlueSky GNSS Information Charts

For quick viewing of GNSS observables, the BlueSky GNSS Firewall Software Release 2.0 includes built-in charting features for immediate visibility of the quality of GNSS reception. A polar plot provides a comprehensive view of satellite-in-view status with a mouse rollover feature providing more details about the individual satellite status.



Current Sky View Polar Plot

From a drop-down task bar, a selection of observables can be plotted over time for verifying performance against user configurable thresholds.



BlueSky Information Charts for Carrier-to-Noise, Tracked Satellites and Phase Time Deviation

TimePictra with BlueSky Performance Monitoring

Many critical infrastructure deployments require a large geographical view of GNSS reception and for this scenario TimePictra with BlueSky Performance Monitoring is an efficient way to manage these environments. The BlueSky GNSS Firewall Software Release 2.0 integrates seamlessly with the TimePictra management system. When using TimePictra to manage a deployment of BlueSky GNSS Firewall devices, users have centralized control and visibility of their network to ensure their critical infrastructure timing network is operating properly.

- Regional/global deployment view
- Multi-element management and alarm monitoring
- Simultaneously compare observables from different Firewall(s)
- Centralized database of historical GNSS data (weeks, months, years)