SyncServer® BlueSky™ Software Option

GPS Jamming and Spoofing Detection, Protection, Analysis

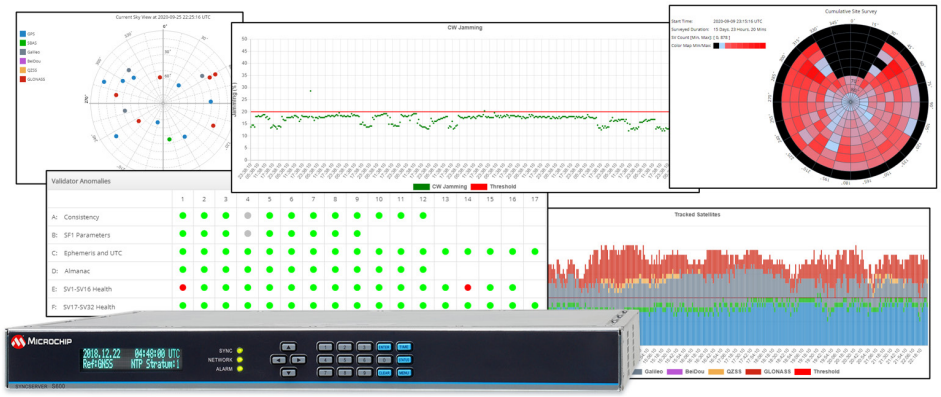
Features

- Localized GPS jamming detection
- Localized GPS spoofing detection
- Continuous wave jamming detection
- Broadband interference detection
- GPS data validation
- Automatic failover to alternative time sources or holdover on alarm
- Informational charts for quick assessment of key GNSS observables
- Configurable thresholds: carrier-to-noise, CW Jamming, satellites being tracked, position dispersion
- Customizable alarm management
- No additional hardware required
- Graphical tools for site survey and historical performance analysis

Detect and Protect

The SyncServer® BlueSky™ option detects GPS jamming and spoofing related anomalies in real-time to protect essential time and frequency outputs.

The BlueSky software option incorporates intelligent GPS jamming and spoofing detectors that continuously monitor the health of the local live sky GPS constellation. In timing applications, the GPS constellation is very predictable as the antenna is stationary. When unexpected changes are detected, and trust is compromised, alarms are sent and the BlueSky detectors respond to protect the integrity of the SyncServer time and frequency outputs.



Jamming Protection

Overt jamming can result in the loss of the GPS signal entirely, and the SyncServer will automatically fall back to alternative time sources or go into holdover. Subtle jamming detection techniques monitored by BlueSky technology require awareness of RF interference as well as establishing thresholds to detect GPS jamming anomalies in the local area. This includes the minimum number of satellites expected to be tracked, typical carrier to noise levels, and RF interference information provided by the GPS receiver circuits.

Spoofing Protection

GPS spoofing detection combines monitoring GPS receiver outputs, RAIM, and GPS data validation. Monitoring unusual position changes can be a spoofing warning and alarm thresholds are easily set. The data broadcast by the GPS satellites also contains expected data during normal operations. The BlueSky data validator continuously checks the data and presents any anomalies in a graphical display. If anomalies that could be associated with a spoofing event are detected, automatic disqualification of GPS as a time source is a user option.

Graphical Live Sky Measurements

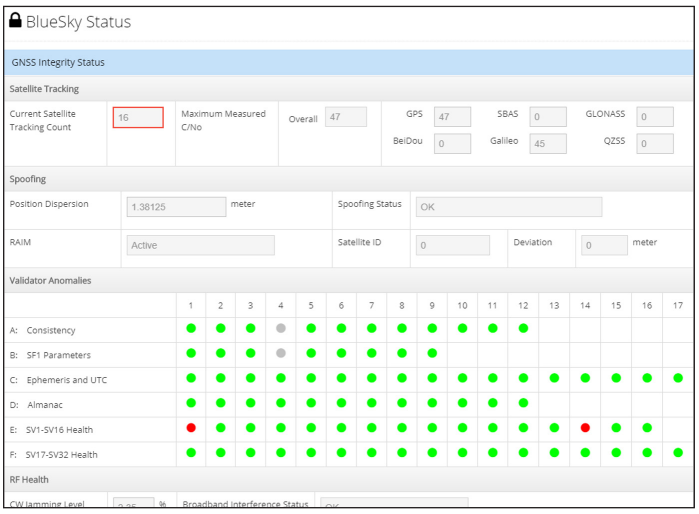
The BlueSky software option provides the graphical tools to easily characterize the local GPS environment to set meaningful alarm thresholds and subsequent SyncServer behaviors. The charts and graphs provide insights into satellite availability based on antenna location, as well as a historical look-back of data useful 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.

Emerging Threat Protection

Intentional GPS Jamming and Spoofing is an emerging security threat to critical infrastructure and ongoing business operations reliant on accurate timing. The real-time, intelligent RF signal and data analytics provided by Microchip BlueSky technology adds the necessary layer of protection to assure the integrity of ongoing time and frequency operations.

At-a-Glance GPS Data Validator Dashboard

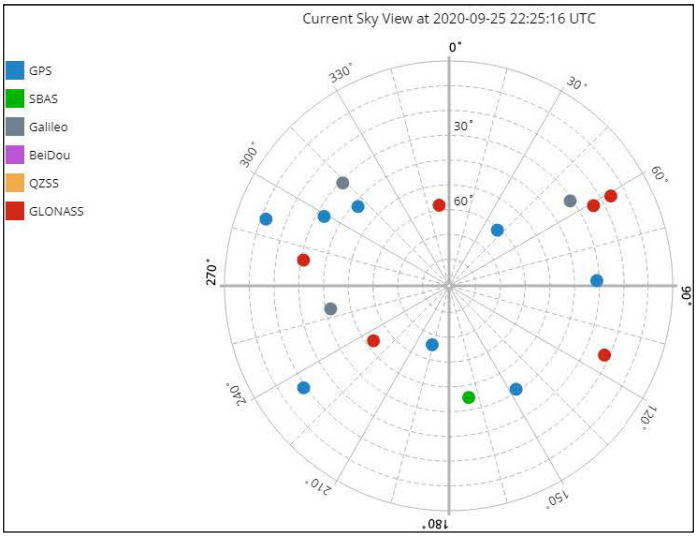
BlueSky status is localized to a single page providing insights into satellite tracking, maximum measured parameters, RAIM, data validator anomalies and signal interference.



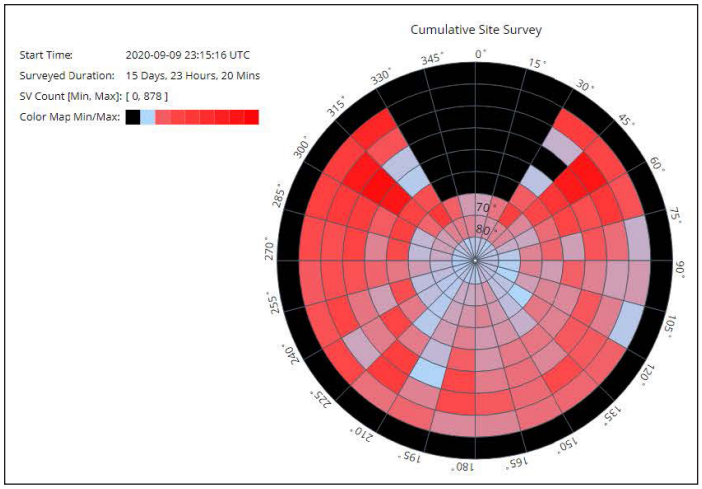
GNSS Integrity Status page including at-a-glance data validator status LEDs for GPS satellites.

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.



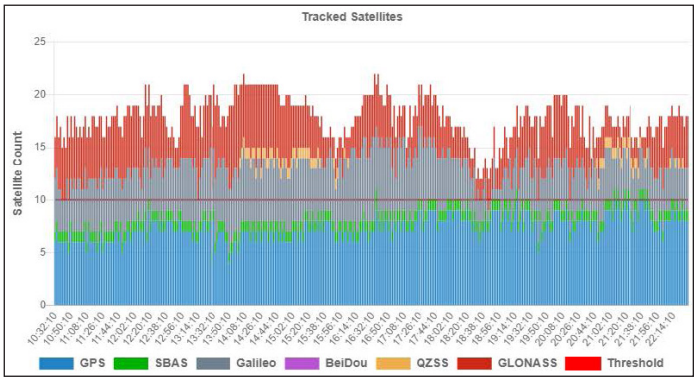
All-in-view look at currently tracked GNSS satellites to assure an acceptable view of the sky from the antenna location.



View which segments of the sky most frequently have usable satellite signals. Red = frequent satellites, blue = occasional satellites, black = no satellites ever tracked.

Historical Measurement Data

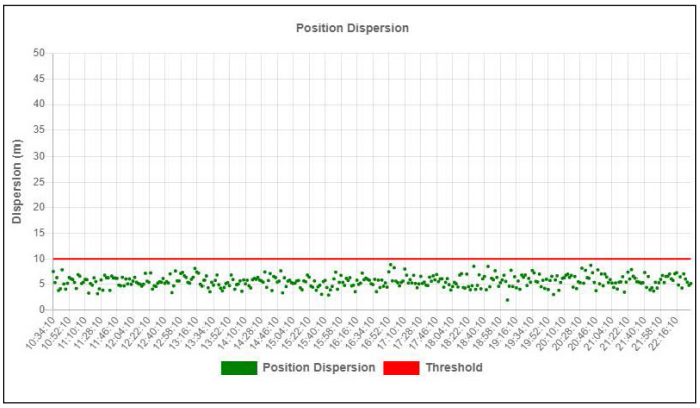
A 30-day look back of 2-minute interval measurement data helps identify the proper alarm thresholds for what is not "normal" for the local GNSS environment. This data is also useful to help correlate jamming or spoofing events to possible known changes in the local RF environment. All data can be exported for further analysis.



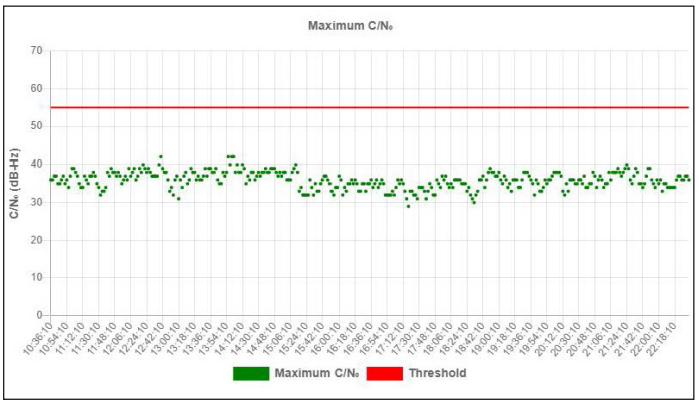
Tracked satellites over time to help identify minimum satellite coverage and verify continuous coverage.

Local Environmental RF Detector Measurements

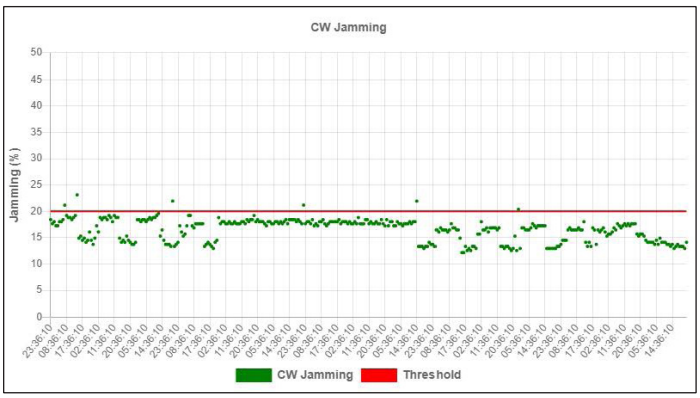
Normal RF environmental factors for the local area result in generally stable position calculations, carrier to noise levels, and background noise measured by the GPS receiver. Reviewing these levels after a period of time helps identify the level at which alarm thresholds can be set. These charts are also useful for identifying periodic noise sources that might be triggering an alarm.



Position dispersion measurements with the red line indicating the current alarm threshold.



Carrier to Noise (CNo) measurements with the red line indicating the current alarm threshold.



Continuous Wave jamming detection with the red line the current alarm threshold. Present in this data is the periodic, close proximity of Wi-Fi® activity from a cell phone near the antenna.

Flexible User Notification and/or GNSS Disqualification

BlueSky GNSS detector groups can be individually enabled or disabled. You can also choose to just observe the detector activity for the local environment or alarm and take action if an anomaly is detected. Actions include notification, disqualify GNSS only while alarmed, or disqualify GNSS on alarm with a manual detector restart required to requalify and use GNSS. This level of flexibility offers tremendous control to decide how to manage the SyncServer response to possible jamming or spoofing activity in the local environment.

Automatic Failover to Alternate Time Sources

All SyncServers allow the GNSS input to be prioritized with other inputs, such as PTP or an IRIG time code, if so provisioned. Disqualification of GNSS merely means the next priority input becomes the primary source of time.

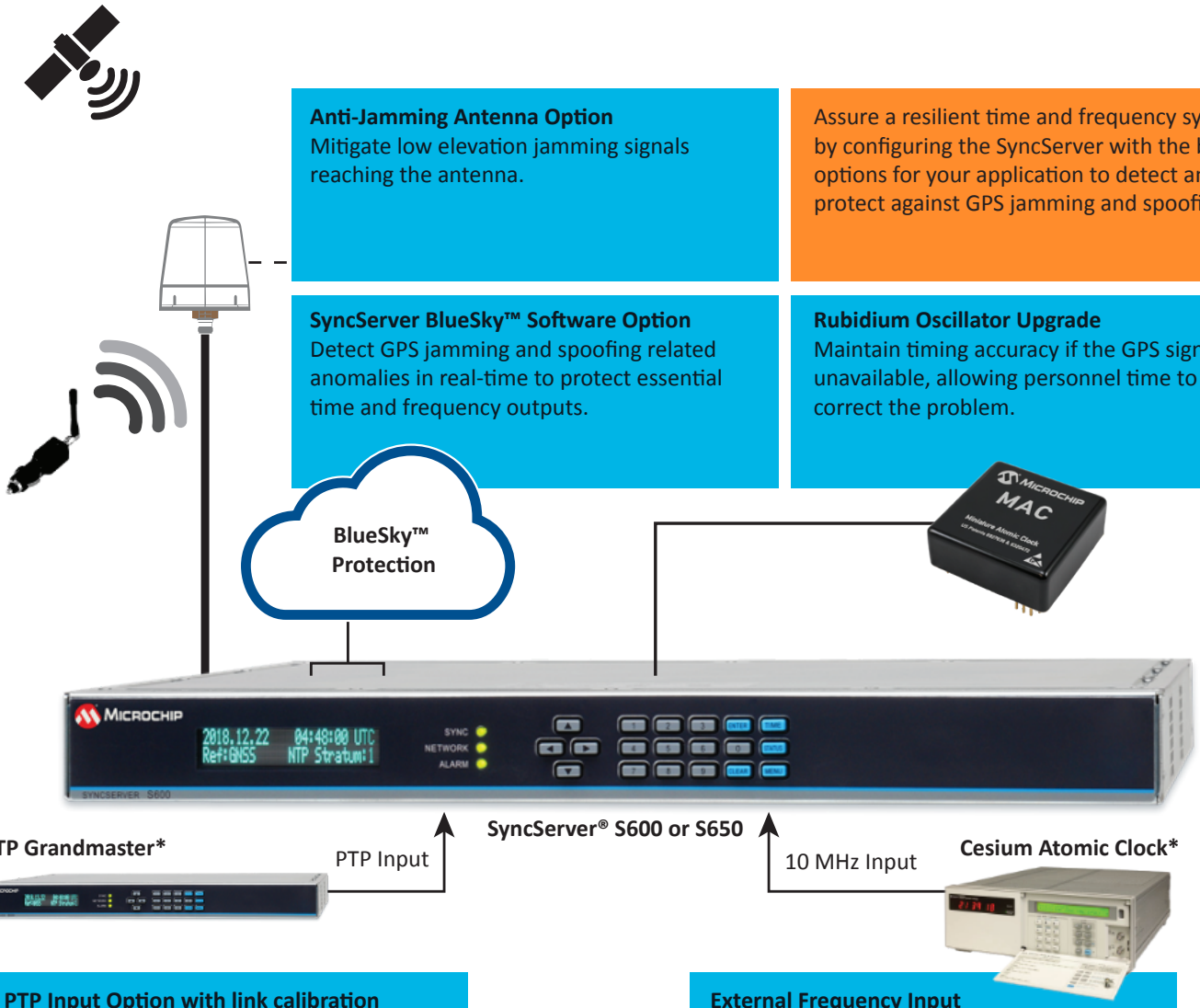
Holdover Choices To Maintain Time Accuracy

In the event there are no alternate time sources configured, if GNSS is disqualified the SyncServer will go into holdover on the installed oscillator, or from an externally supplied frequency reference, until GNSS tracking is resumed. In the case of the installed oscillator, the drift of the standard oscillator is about 400 microseconds in the first day without GNSS and progressively gets worse. Upgrading to the superior Rubidium atomic clock oscillator keeps the SyncServer accurate to better than 3 microseconds for the first 3 days if no GNSS, and continues to keep the drift rate well contained. The value of the upgraded Rubidium oscillator is that if the GNSS signal is disqualified, the SyncServer can continue to provide accurate time and frequency for much a longer period of time compared to the standard oscillator. This provides personnel time to rectify the GNSS issue with minimal degradation in the SyncServer time synchronization accuracy.

BlueSky Software Option Specifications/ Requirements

- GPS receiver-equipped SyncServer S600 or S650 models only
- Serial numbers starting with SCA19 or later (i.e. built in 2019 or later); contact Microchip for SCA16-SCA18 models).
- Software Version 4.1 or later installed in the SyncServer
- Not available for SyncServer S650 SAASM or SyncServer S650 M-Code models
- Enabling the GPS Data Validator Detector will reduce standard NTP operations to a maximum rate of 6000 NTP requests per second. The NTP Reflector timestamping capacity remains unchanged at 360,000 NTP requests per second.

Reference Configuration for Resilient Time and Frequency



Anti-Jamming Antenna Option
Mitigate low elevation jamming signals reaching the antenna.

Assure a resilient time and frequency system by configuring the SyncServer with the best options for your application to detect and protect against GPS jamming and spoofing.

SyncServer BlueSky™ Software Option
Detect GPS jamming and spoofing related anomalies in real-time to protect essential time and frequency outputs.

Rubidium Oscillator Upgrade
Maintain timing accuracy if the GPS signal is unavailable, allowing personnel time to correct the problem.

PTP Input Option with link calibration
Use PTP input from a PTP grandmaster as a calibrated backup source of time if GPS is unavailable.

External Frequency Input
Maintain very long term, ultra precise timing accuracy with a Cesium atomic clock if the GPS signal is unavailable for extended periods of time.

*Alternative reference source if GPS is impaired

	Protection Against		Resiliency Combinations		
	Jamming	Spoofing	Good	Better	Best
BlueSky™ Software	■	■	■	■	■
+ Rubidium Oscillator	■			■	■
+ Anti-Jam Antenna	■				■