Galileo Interference Detection

BlueSky™ GNSS Firewall

Summary

Multi-GNSS constellation technology has become a standard capability for most GNSS receivers. In an uncertain world of GNSS jamming, spoofing, and geo-political unrest, the ability to track multiple GNSS constellations can provide one more bit of operational peace-of-mind. While there are no guarantees, multi-GNSS tracking is a way of reducing the risk of depending entirely on one GNSS constellation alone.

Today, the four primary global constellations include GPS (USA), Galileo (EU), GLONASS (Russia), and BeiDou (China). Additionally, there are regional satellite navigation systems such as Japan's Quasi-Zenith Satellite System (QZSS) which is focused on coverage in the Asia-Oceania region and the Indian Regional Navigation Satellite System (IRNSS) which primarily covers the India region.

With the advent of GPS occurring over 40 years ago, the use of GPS has become the most broadly used GNSS technology. GPS is also recognized for its long-standing reliability and performance. GLONASS was first launched in October of 1982; however, the full orbital constellation was not operational until 2010. BeiDou was first launched in October/2000 and with BeiDou-3 reached global coverage in 2018. However, GPS, GLONASS and BeiDou share one very important identity, that being each is ultimately owned and operated by the military of a single country.

Galileo, which declared initial services in 2016, is the one global GNSS constellation that is primarily for civilian use, unlike the more military-oriented systems of the United States (GPS), Russia (GLONASS) and China (BeiDou). Galileo is operated by the European GNSS Agency (GSA) made up of multi-country contributions with civilian focus. Together, Galileo and GPS are looked upon as the most ideal global GNSS constellations for use within critical infrastructure such as mobile/telecom networks, utility power grids, financial trading, data centers, aviation and emergency services.

However, although the cooperation between the USA and EU aims to ensure that GPS and Galileo will be interoperable at the user level for the benefit of civil users around the world, the Galileo GNSS signal itself is vulnerable to jamming and spoofing threats in similar ways as GPS.

This application note describes how the BlueSky™ GNSS Firewall provides protection and improved resiliency for reception of Galileo. Additionally, the paper explains an innovative approach for receiving Galileo signals and distributing Galileo derived time to legacy GPS systems.

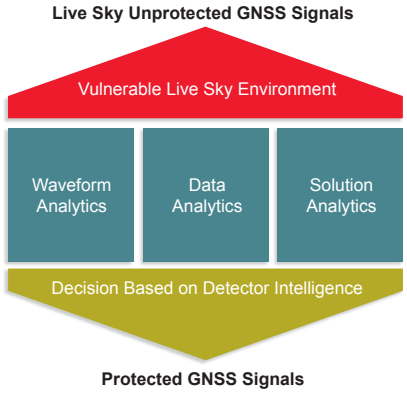
GPS and Galileo GNSS Signals-Similarities and Differences

The open civilian versions of GPS and Galileo signals operate at the frequency of 1575.42 MHz and include a constellation of satellites which can be viewed across the entire globe. Because the signals are transmitted from space, both signals operate at very-low power levels when reaching the earth's surface and therefore are subject to interference which could be intentional or unintentional.

Both GPS and Galileo use similar techniques for delivering timing to GNSS receivers. With respect to the "open message format" of the data transferred from the respective constellations, both utilize Code-Division Mulitple Access (CDMA) for the decoding; however, the formats are very different.

When considering the security of GPS and Galileo signal reception, GNSS signal analysis should be performed with an approach that treats the live-sky signals as vulnerable and unprotected. The GNSS signals should be analyzed using three types of methods:

1. **Waveform Analytics:** this involves analyzing the physical characteristics of the signal (e.g carrier frequency, power level, spectrum shape)
2. **Data Analytics:** analysis of the received data (e.g., week number, leap second info, satellite ephemeris)
3. **Solution Analytics:** analysis of the solution output characteristics (e.g. time, position, velocity)



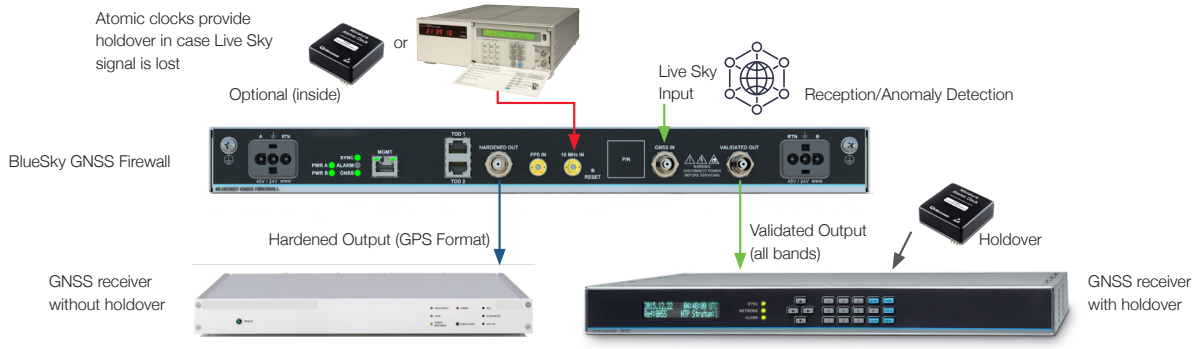
Protection should make use of the aggregated information from multiple detectors

The above data is processed by a decision engine to determine the signal validity. A good decision engine is not based on the "number of rules" that the signal can be checked against but instead comes from having detectors of each type and being able to make 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.

BlueSky GNSS Firewall

A long-time and proven architecture for defending against security threats is the use of a firewall. In the world of cyber security for network protection, a firewall refers to a network device which blocks certain kinds of network traffic, forming a barrier between a trusted and an untrusted network. It is analogous to a physical firewall in the sense that firewall security attempts to block the spread of computer attacks.

The BlueSky GNSS Firewall solves the problem of protecting already deployed systems by providing a cost-effective overlay (firewall) solution installed between existing GNSS antennas and GNSS systems. Like 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 decision engine that analyzes the GNSS signal (Galileo and/or GPS). GNSS signal data is received and evaluated with GNSS standards along with analyzing received signal characteristics. This information is used by the firewall to block anomalous GNSS signals and provide protected signal outputs to downstream GNSS receivers.



The BlueSky GNSS Firewall provides two types of outputs: (1) Hardened GPS and (2) Validated GPS.

Hardened Output

The Hardened output is the most secure output because it provides a synthesized GPS signal isolated from the live-sky environment. The hardened output is in the GPS format but is not a copy of the live-sky GPS signal and is only loosely based on information received from the live-sky signal. The hardened output provides a synthesized version of the GPS L1 signal. Thus, a secure BlueSky GPS environment is created. When incidents are detected on the input 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 jamming or spoofing without impacting their system performance. Because the GPS L1 signal output is supported by all current and foreseeable GPS based systems, it provides backward compatibility while also being future proof.

Validated Output

The Validated output provides a copy of the actual input signal being analyzed by the firewall. When anomalous conditions are detected, the firewall turns the validated output off to protect users from potentially corrupted GNSS signals. Once conditions are deemed safe, the validated output is turned back on. The validated output 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 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, (with the exception of Beidou) as well these satellite signals are simply passed through, but not analyzed for anomolies as with the GPS or Galileo signals.

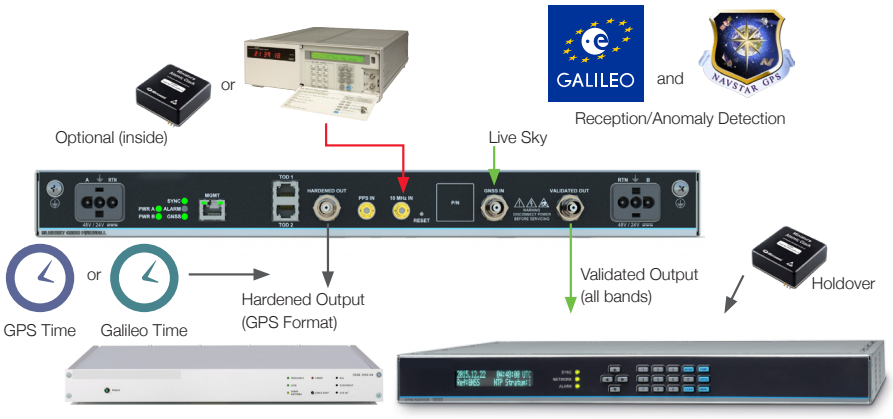
Galileo Protection

The BlueSky GNSS Firewall can receive live sky GPS or live sky Galileo as an input. Both modes are user selectable. This can be accomplished using the built-in WebGUI, Command Line Interface (CLI), or using Microchip's TimePictra Synchronization Management software.

When receiving Galileo, the BlueSky GNSS Firewall performs both "power" and "timing" anomaly detection on the live sky Galileo signal input. This same detection is also occurring on the GPS signal in parallel along with GPS data validation for compliance with GPS standards. A future release of the BlueSky GNSS Firewall software will include data validation of the Galileo signal as well.

As previously described, the Validated Output passes through "all bands"; however, in the case of the hardened output, only the "live sky timing" is incorporated into the synthesized hardened output. The BlueSky GNSS Firewall provides the unique capability of allowing the user to select between "GPS time" or "Galileo time" for the Hardened output. For example, although the signal format of the hardened output is in the GPS (L1) format, the "time" that is on this signal can be selected to be Galileo.

Selectable time on the hardened output is ideal for environments where legacy equipment is designed to receive GPS; however, the critical infrastructure provider desires to use Galileo as their time reference. The BlueSky GNSS Firewall essentially acts as a translator by recovering "time" from the live-sky Galileo input and mapping it onto the Hardened Output. The diagram below outlines this unique capability.



Galileo time mapped onto the Hardened Output (GPS format)

Galileo + GPS Protection

Redundancy is critically important in today's cloud driven data centers. The use of multi-constellation reception enables not only timing source redundancy but also increased diversity which further reduces the likelihood of failure. The diagram below shows how BlueSky GNSS Firewall systems can be deployed in a redundant pair. If using the Hardened output, both units deliver a common L1 formatted signal for the downstream receivers to use (redundancy); however, the "source of time" is "diversified" with one receiving Galileo and the other receiving GPS. In both cases, the GNSS vulnerability protection built into the BlueSky GNSS Firewall provides secure GNSS reception (firewall protection for both Galileo and GPS).

- Use Validated or Hardened output (depending on use case)
- Select from redundant and diverse live sky sources: Galileo or GPS
- BlueSky™ GNSS Firewalls provide detection, resiliency and visibility for both Galileo and GPS

Redundant and Diversified GNSS timing (Galileo and GPS) for data centers

Conclusion

GPS, GLONASS and BeiDou are GNSS constellations which are all globally available, but which are ultimately owned and operated by the military of a single country. Galileo is the only global GNSS constellation focused on civilian infrastructure.

When evaluating global usage of GNSS by critical Infrastructure providers, too many have become overly dependent on GPS because of its ubiquitous availability and long-standing reliability. Now that Galileo has become equally ubiquitous, the combination of GPS and Galileo provides for redundancy and diversification such that GPS is not a single point of failure.

However, like GPS, the signal reception of Galileo is vulnerable to the same threats of jamming and spoofing, whether intentional or unintentional. Protection of live-sky GNSS reception using a well proven "firewall" architecture provides for a secure and resilient use of both GPS and Galileo. Further, with the BlueSky GNSS Firewall, "Galileo time" can be mapped onto the GPS L1 signal format using the hardened output so that downstream GPS receivers can immediately adopt Galileo as their time source.

The BlueSky GNSS Firewall with its extensible platform and upgrade capability, delivers future proof security to defend against new threats for continued security of GPS and Galileo reception.

For more information about Microchip's portfolio of GNSS Vulnerability Protection and Security, please visit:
https://www.microsemi.com/company/technology/gps-threat-protection-and-security.

To find out more details about Microchip's BlueSky GNSS Firewall visit:
https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall

To find out more about Microchip's TimePictra software with BlueSky Performance Monitoring visit:
https://www.microsemi.com/product-directory/management-monitoring/4159-timepictra

DS00003207A