BlueSky™ Performance Monitoring

GNSS Visibility for Better GNSS Security

As defined by the Department of Homeland Security (DHS): Critical infrastructure describes the physical and cyber systems and assets that are so vital that their incapacity or destruction would have a debilitating impact on the physical or economic security or public health or safety. In support of this mission, DHS formed the Cybersecurity and Infrastructure Security Agency (CISA) to be the nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

In a recent publication from CISA, titled "*TIME – THE INVISIBLE UTILITY*", the following was stated:

GPS has become the de facto time standard for many commercial users because of its relatively low cost and ubiquitous availability. In 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) identified overdependence on the Global Positioning System (GPS) as a growing vulnerability within the United States Critical Infrastructure. In 2017, 5.8 billion Global Navigation Satellite Systems (GNSS) devices, such as those using GPS, were in use. By 2020, this number is forecasted to increase to almost 8 billion—an estimate of more than one device per person on the planet. Until recently, GPS devices were viewed simply as radio receivers. However, they are actually computers, with similar security risks. Threats include denial-of-service attacks (jamming) and the introduction of bad data into the system (spoofing). The advent of software-defined radios has increased the ease and lowered the cost with which these types of attacks can be launched. Efforts should be made to ensure accurate and resilient timing for your GPS devices.

The complete document can be found at:
https://www.us-cert.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

As described by CISA, there is a dramatic growth in the dependency on GPS/GNSS for the dissemination of "time" as used by critical infrastructure. While the use of GNSS based time has become more vital for critical infrastructure operations, the security of the GNSS signal itself has become increasingly vulnerable to a wide range of jamming and spoofing threats, both intentional and unintentional. Given the inherently fragile nature of the GNSS signal, an important way in which reception of the GNSS signal can be guarded is through better visibility of the GNSS signal characteristics in real-time.

This application note describes how BlueSky™ Performance Monitoring, which is a set of functionality built into Microchip's TimePictra® software delivers a solution for monitoring and characterizing live-sky GNSS signals to provide signal visibility for better protection and security of GNSS reception.

GNSS Signals are Inherently Fragile

Disruptions to the GNSS signal are typically classified into two categories referred to as "jamming" and "spoofing". Jamming is where the GNSS signal is overpowered with a locally generated signal at the same frequency, therefore making the actual live-sky GNSS signal not detectable. Spoofing can be caused by a more nefarious act which may involve the creation of a false GNSS signal that the receiver is fooled into tracking. Contained within the fake signal is inaccurate information such as false location data.

The GNSS signal is very weak and is largely only detected with a clear view of the sky. Given the significant distance the signal must travel from satellites orbiting the earth which are 12,500+ miles from the earth's surface, the GNSS signals are at a very low power level (typically –133 dBm) when reaching the Earth's surface.

To put this in context, let's compare the low power of a GNSS signal to the power level of a technology that many of us use daily, Bluetooth®. As an example, a Bluetooth device operates at a power level that is roughly 50 billion (50,000,000,000) times stronger than the GNSS signal. Many jamming devices built today are already available in small form factors that install in vehicles with the objective of jamming small areas of 10-20 meters in radius. Knowing how small a Bluetooth device can be built (example being Bluetooth headsets) the construction of a GNSS jamming device intended to wipe out a large geographical area can easily be packaged in a very small form factor. Reports of large geographical areas being jammed are now common throughout the world with the Scandinavia region being a highly impacted area due to Russia jamming NATO military exercises occuring in the Norwegian sea region which involve the use of wide area GPS jamming.

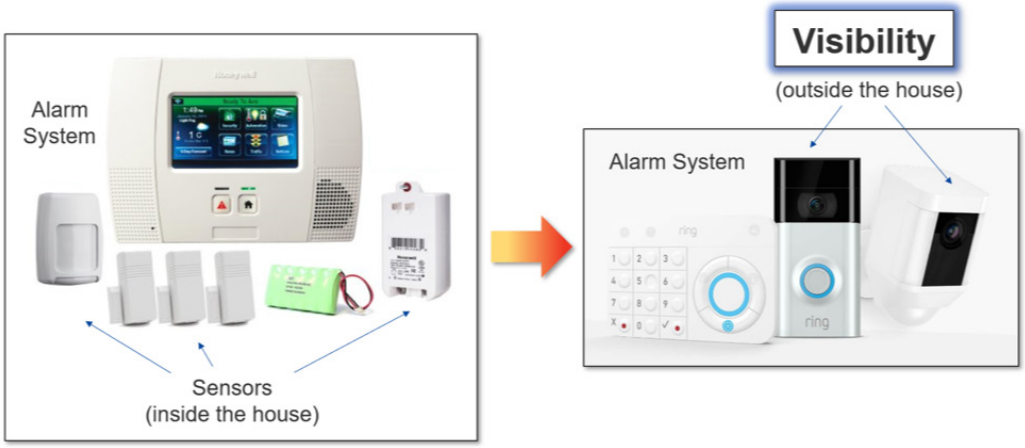
Further, intentional threats are not the only vulnerability category to be concerned with. Errors due to weather, atmosphere and even the operation of the GNSS satellite control system can impact the secure reception of GNSS. This has occurred at a global level for both GPS (https://www.gpsworld.com/world-dodges-gps-bullet/) in 2016 and more recently with Galileo unavailability (https://insidegnss.com/galileo-initial-services-have-now-been-restored/) which just occurred in 2019.

GNSS Vulnerabilities can be Intentional or Unintentional

Visibility Increases Security

A key part of any cyber-security solution is visibility. An interesting analogy that we are all familiar with are home alarm systems. When looking back at original alarm systems, sensors were placed throughout a home connected to a centralized alarm system that would sound off if an unexpected intruder was detected. Such an alarm system was effective; however, only after the intruder was "inside the house."

Today's alarm systems are centered on "visibility" as the key method to provide security. Specifically, cameras have become an essential part of a security system with the goal of providing visibility of a threat "before" the threat is able to gain entry.

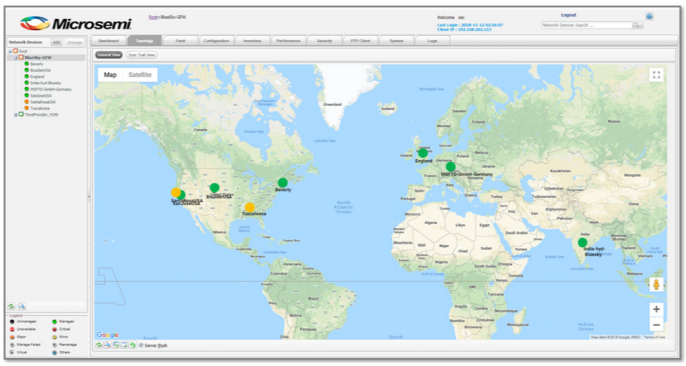


Evolution of alarm systems

Alarm systems represent a simple to understand example of the value visibility brings to securing a home. Looking beyond this example and more specifically at critical infrastructure, visibility of day-to-day operations is vital. For the data center, visibility of software and cloud applications is needed to defend against malware; for data networking, visibility is used to ensure encryption is not compromised; for the power grid, visibility is used to better manage the flow of energy, especially with distributed resources like solar and wind. To secure critical infrastructure, visibility is essential.

It Starts With Surveillance

For a critical infrastructure operator, having a bird's eye view is the starting point for visibility. In the case of GNSS surveillance, when an anomaly or outage occurs, the most immediate need is to quickly identify if the event is isolated to a specific location, affecting a regional area, or in some cases is caused by a global situation. Using BlueSky Performance Monitoring, a green, yellow, and red status indication representing different locations of interest provides a simple way for operators to know the overall health of GNSS reception. If it's a single location being impacted, then the cause can most likely be narrowed to an issue such as multi-path interference, local weather anomaly, or a potential drive-by jamming/spoofing threat (common example being a vehicle with jamming device).



Surveillance of GNSS reception

If the impact is affecting multiple locations, then a more complex problem is likely occurring and narrowing the root cause is more difficult, especially in such cases as the GPS 2016 anomaly and the recent Galileo 2019 outage.

BlueSky Performance Monitoring provides GNSS surveillance to help pinpoint the scope of the problem quickly. However, once this is understood, then the next step is to dig into more of the details.

Characterizing GNSS Signals

Multi-path interference, weather anomalies, jamming and spoofing, are terms commonly used when referring to GNSS vulnerabilities; however, these terms don't provide any insights (visibility) into the details. In order to identify root cause, more specific signal characterization is needed.

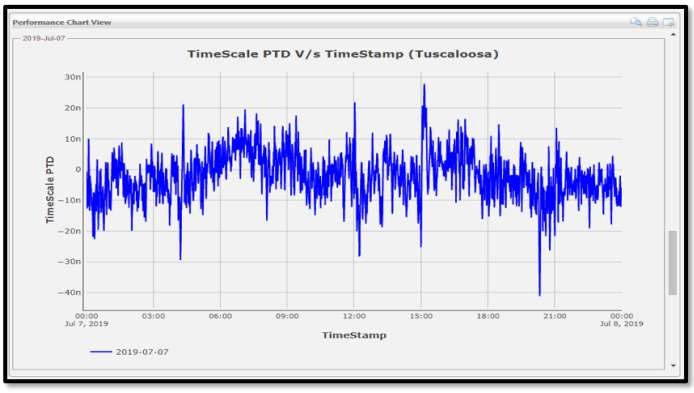
GNSS simulators typically have highly sophisticated recording capabilities which developers of GNSS receivers and related equipment have been using for years to perform test and measurement of GNSS signals. Such equipment is effective for laboratory environments or even in manufacturing; however, this instrumentation is expensive and requires instrumentation specialists with extensive training. Microchip's BlueSky Performance Monitoring simplifies these important measurement capabilities so that network operators who don't have years of GNSS expertise can quickly diagnose problems. The table below provides a sample of some of the metrics and signal characteristics that can be tracked.

Metric	Characteristic of Signal Anomaly
Tracked Satellite Count	Are the expected number of satellites in view?
GPS Position Delta	Is the position data coming from the sky moving too much relative to surveyed antenna position?
Phase Time Deviation	Is the sky received "time" moving? (suddenly, gradually, etc?)
GPS Signal Average	Is the GNSS signal strength of the visible satellites in the expected range?
Satellites in view	Are individual satellites at expected carrier-to-noise level?
RF Power	Is the RF power level within expected threshold?

Typical Characteristics of a GNSS Signal

Visibility of Timing Anomalies

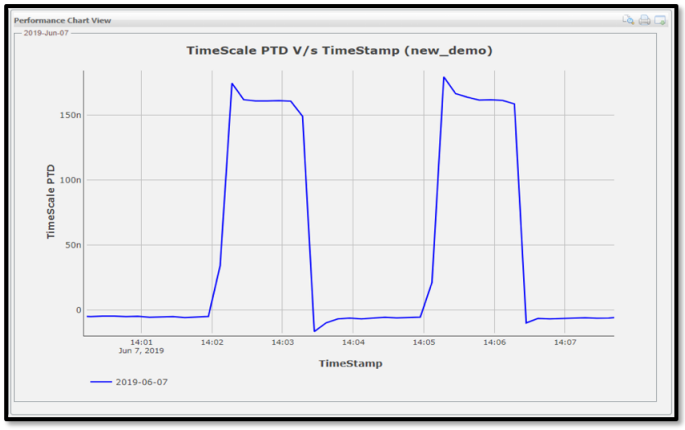
Although GNSS systems are mostly known for "navigation", the fundamental operation of GNSS is completely dependent on timing accuracy. When determining if the GNSS reception is performing well, measurement of the phase difference between what is expected versus what is being received is a good signal characteristic to visualize.



Phase measurements of GNSS reception

Under normal conditions, the phase offset should typically be in the ±50 ns range as seen in the previous plot. Given this small range of acceptable performance, detection of a timing anomaly can be quite difficult and is one of the most important techniques for protecting against GNSS vulnerabilities. Timing anomalies can be gradual, sudden, or complex such as repeated phase jumps. Timing errors can cause serious havoc and confusion as such errors can cascade down to the underlying timing distribution systems operating a large data center or mobile switching office.

Below is an example of a timing anomaly where there is a repeated timing offset of roughly 150 ns being generated. With this type of repeated event, a typical GNSS receiver/timing system could be jumping in and out of holdover causing major confusion for a critical infrastructure operation.

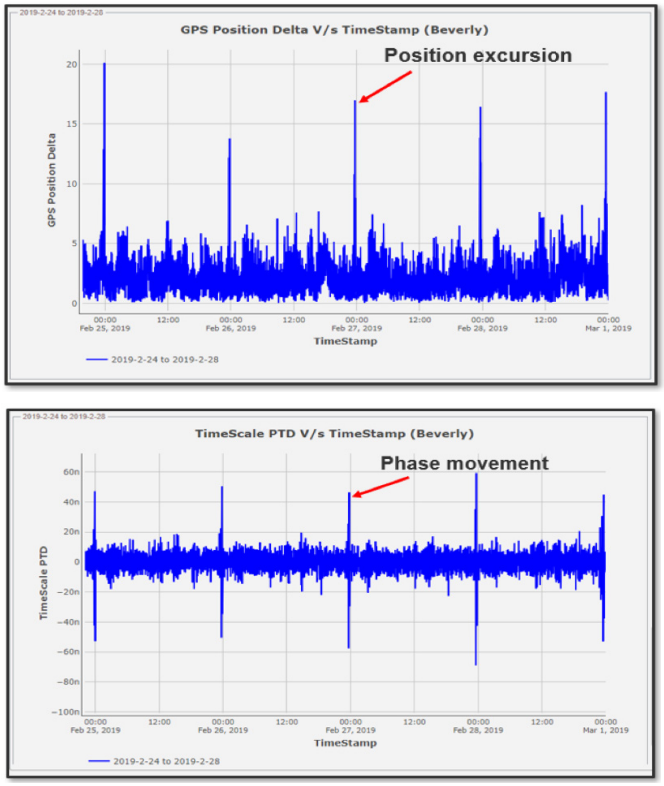


Timing Anomaly - repeating offset of 150 ns

Visibility of Position Anomalies

For critical infrastructure, the GNSS antenna is typically installed in a fixed location with a clear view of the sky and the exact position of the antenna is surveyed with the coordinates programmed into the receiver. When the GNSS receiver is being used for “timing”, precise survey of the antenna is necessary to ensure the most accurate timing performance. Any kind of offset and/or spoofed position data can cause the GNSS receiver to have degraded timing performance and ultimately cause the GNSS receiver to lose the ability to track satellites completely.

In the example below, under normal conditions the position as received by the GNSS receiver is roughly 1–5 meters as compared to the surveyed position of the GNSS antenna. The first plot shows normal position fluctuation; however, occurring once per day, there is also a position excursion of about 15 to 20 meters. The second plot, is of phase movement which shows a phase shift of roughly 100 ns (peak-to-peak) simultaneous with the position movement of the first plot. The position movement, which is likely the result of multi-path interference, is impacting timing performance. BlueSky Performance Monitoring enables multiple GNSS signal characteristics to be viewed together to better understand cause and effect.



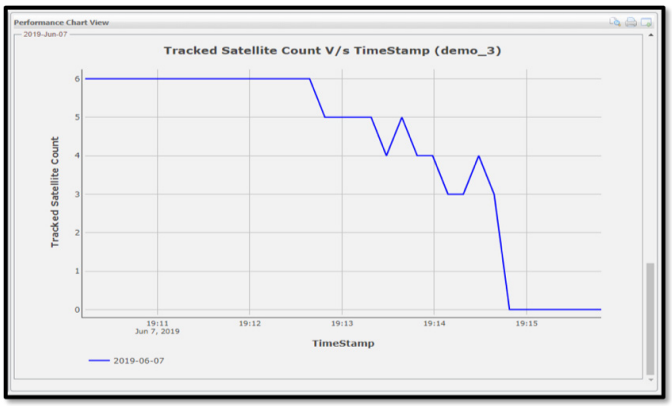
Position excursion creating phase jumps

Visibility of Spoofing

GNSS Spoofing has taken on a new level of concern with the advent of software defined radios and the ability of these systems to be programmed to generate spoofing threats. This trend has almost become a common hobbyist ambition, especially as spoofing attacks can cause chaos with consumer level navigation systems and even mobile gaming such as Pokémon.

Spoofing attacks can be difficult to detect as it is the GNSS data itself which is being manipulated. Like data network threats, GNSS spoofing is an on-going and evolving threat vector which requires a defense system that can be upgraded to guard against emerging threats.

In the following example, a GNSS receiver is tracking six satellites under normal conditions and then satellites begin to be prematurely knocked out, and over the course of approximately three minutes, all satellites are no longer being tracked. Satellites falling out of view this quickly is abnormal and is just a simple example of how spoofing can create a confusing situation for a GNSS receiver trying to track satellites.



Spoofing of GNSS satellite tracking

Conclusion

Security has become the most important requirement for critical infrastructure operations. Any device connected to critical infrastructure can become a target for exploitation and needs to be as secure as possible.

Security hardening of a GNSS system is a continual process due to the constant emergence of new threats. Like network security vulnerabilities, new GNSS vulnerabilities are on the rise and “GNSS signal visibility” is a vital capability for helping to determine the root cause of a GNSS vulnerability, especially before a minor disruption becomes a more serious outage.

When a GNSS vulnerability is detected, BlueSky Performance Monitoring provides surveillance of GNSS reception quality and enables critical infrastructure operators to identify if the problem is specific to a location or affecting a larger geographical area. Further, having visibility of key performance metrics enables the operator to take quick and cost-effective action. Dispatching network operations personnel to a roof-top on a high rise building to unnecessarily check on a GNSS antenna is expensive. “GNSS visibility” using BlueSky Performance Monitoring prevents these costly mistakes.

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

DS00003200A