



INTRODUCTION:

Microchip Technology Incorporated is pleased to respond to NIST’s request to gather information about public and private sector use of positioning, navigation and timing (PNT) services. As the world leader in network synchronization and atomic clock technology, Microchip’s Frequency and Time Systems business appreciates the opportunity to provide the following information. Microchip is a leading provider of smart, connected and secure embedded control solutions. Its easy-to-use development tools and comprehensive product portfolio enable customers to create optimal designs, which reduce risk while lowering total system cost and time to market. The company’s solutions serve more than 120,000 customers across the industrial, automotive, consumer, aerospace and defense, communications and computing markets.

MARKET LANDSCAPE:

The dependency on position, navigation, and timing (PNT) has become increasingly important to Critical Infrastructure sectors such as communications, energy, transportation, emergency services, financial services, and cloud data centers. This dependency has resulted from the ubiquitous availability of PNT through the deployment of sky-based delivery using Global Navigation Satellite System (GNSS) systems such as GPS, Galileo, GLONASS, BeiDou, and others.



Markets dependent on PNT



Critical Infrastructure has a significant and growing installed base of stationary timing receivers that serve essential applications. In many cases, operators of Critical Infrastructure are not able to maintain accurate records of all GNSS receiver locations, and the exposure of this error has caught many by surprise. Additionally, GNSS contributes to a rapidly diversifying range of applications and use cases. GNSS-delivered PNT is now a foundational function enabling Internet of Things (IoT), Big Data, Mobile Health, Augmented Reality, Smart Cities, and Multimodal Logistics. Arguably, GNSS-delivered PNT has become the most fundamentally important resource fueling the new information/data economy. "With great power comes great responsibility" is certainly true with today's GNSS use for PNT by Critical infrastructure. Because there is so much dependency on GNSS, the impact of errors or interruptions is now more significant than ever before.

GNSS errors and anomalies can be caused by a range of issues. Because real-world signals from the satellites do not travel in a vacuum, but pass through the ionosphere and the troposphere, errors are induced in the signal path even under normal operations. This causes the actual mean speed of the signal when traveling from satellite to receiver to vary and be difficult to measure because of signal path uncertainty.

Additionally, normal effects, such as reflections, can cause the satellite-to-user distance to be inaccurately determined. This can give rise to signals from the same SV arriving at the receiver having followed different paths, and therefore introducing signal disparity, a phenomenon known as multipath propagation. Errors can also be introduced due to issues with the GNSS system itself.

Problems with the clocks onboard the satellite as well as mistakes made in uploading the timing information from ground-based control stations can be contributors to GNSS failures. Additionally, GNSS signals are extremely weak and highly vulnerable to jamming. This type of incident causes partial or complete loss of the GPS signal and is commonly the result of interference from nearby RF sources. Jamming devices (or jammers) have become widely available at a low cost. A common incident is for a passing vehicle, which may be using a jamming device to prevent GNSS tracking, to also interrupt a GNSS receiver being used by Critical Infrastructure. More complex jamming incidents can be orchestrated by adversaries to make it more difficult to detect the source of the jamming, but the result is the same. In such cases, the GNSS receiver fails to acquire and track the GNSS signal. In some cases, there are more sophisticated attempts to disrupt the GNSS signal to take control of critical assets or to deny service to specific systems. This type of incident, effectively the propagation of illegitimate GPS signals, is referred to as GNSS spoofing (or complex jamming). The GPS receiver is tricked into tracking illegitimate GPS-like signals; it continues to operate, but the solution for position and time given by the receiver will be wrong. This type of incident is almost always intentional and can be difficult to detect.

GNSS-based errors, whether intentional or unintentional, can quickly impact a vast geography and widely dispersed locations. Additionally, a large variety of operational environments must be accounted



for that not only include outside deployment with a clear view of the sky, but highly obstructed locations, urban canyons, and in-building and in-cabinet scenarios. This topic has been discussed by Microchip in depth at the following link: <https://www.microsemi.com/blog/tag/gps-vulnerabilities/>

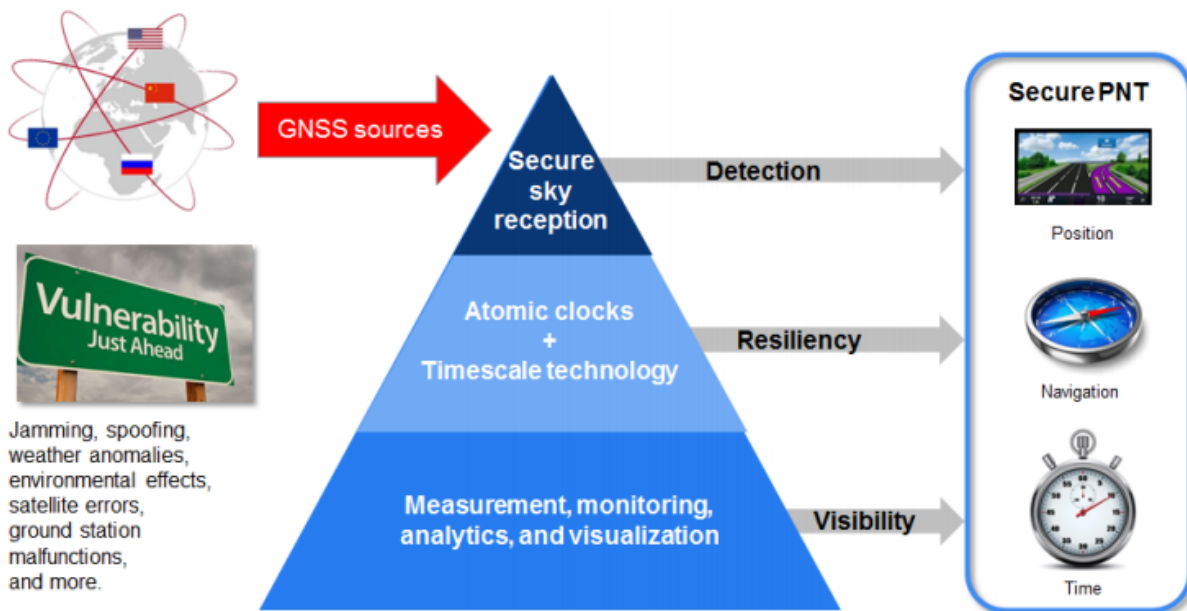
SECURING PNT AS USED BY CRITICAL INFRASTRUCTURE

The following are three main objectives to consider when constructing a secure PNT infrastructure which is aligned with the NIST Cybersecurity Framework:

- (1) Detection — early sensing of threats, both intentional or unintentional
- (2) Resiliency — continuous operation until threats are mitigated and resolved
- (3) Visibility — measurements and analytics for ongoing PNT health monitoring.

This solution for securing PNT focuses on a network approach based on layers of resiliency that can be deployed cost effectively across infrastructure with 10s, 100s, 1000s, or even 10,000s of nodes. These layers are built using a broad array of technologies, including GNSS anti-jamming and anti-spoofing technology, time transport protocols, atomic clocks, and software management and monitoring.


Secure PNT Requires Detection, Resiliency, and Visibility






The solution stack starts with the ability to support sky GNSS signal reception in a highly secure manner. The vulnerability of these GNSS systems to various signal incidents is well documented, and the proliferation of GNSS systems has embedded these vulnerabilities into critical national and corporate infrastructures that rely upon GNSS-delivered PNT for daily operations. Such widespread deployment of GNSS makes it impractical to replace all the fielded systems in a timely or cost-effective manner.

A “GNSS Firewall” solves the problem of protecting already deployed systems by providing a cost-effective overlay solution installed between existing GPS antennas and GPS systems. Like a network firewall, the GNSS Firewall protects systems inside the firewall from untrusted sky-based signals outside the firewall. Contained in the GNSS Firewall is a software engine that analyzes the GPS signal. GPS signal data is received and evaluated from each satellite to ensure compliance with GPS standards along with



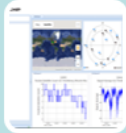
Trusted Source

- Validated Timing Source
- Trusted Supply Chain




Validation

- Live Sky Monitoring
- Anomaly Detection



Visibility

- Analytics
- Situational Awareness
- Heat Maps



Resiliency

- Integrated & External Holdover Clocks
- Autonomous Time-Scales
- Alternate Sources (e.g. eLORAN)

analyzing received signal characteristics. This information is used by the firewall to block anomalous GPS signals and provide a hardened GPS signal output that is validated and trusted for use by downstream GPS systems.

The GNSS Firewall can be connected to a range of atomic clock technologies enabling continuous operation where GPS may be completely denied for extended periods of time, even in cases where disruptions may last for more than 30 days. The system can make use of rubidium atomic clock technology to enable continuous output of the GPS signal to the downstream GPS receiver in case of complete loss of live sky GPS reception.

Alternatively, cesium clocks can be connected to the GNSS Firewall enabling UTC traceable time for more than 30 days. The use of atomic clocks

enables the highest level of resiliency and autonomous operation.

Management and performance monitoring of wide-scale deployment of GNSS Firewalls provide visibility at a regional, national, or global level of your PNT infrastructure to provide early alerting to threats before your PNT network is affected. The GNSS Firewall combined with atomic clocks, management and monitoring provide for a secure and resilient PNT infrastructure.



Additional information and recommendations related to the responsible use of PNT services.

The U.S. Department of Transportation (DOT) recently conducted a series of Positioning, Navigation, and Timing (PNT) technology field demonstrations to assess their efficacy as a complement/back-up to the Global Positioning System (GPS), and more generally Global Navigation Satellite System (GNSS). Enhanced Loran (eLoran), a high-powered, long-range, low-frequency, terrestrial-based PNT technology was included in those demonstrations, one of which was conducted by a team of companies led by Hellen Systems (www.hellensystems.com), including L3Harris Technologies (www.l3harris.com), Microchip Technology (www.microchip.com), Continental Electronics Corporation (www.contelec.com), and others. This team has been working closely together to develop the supporting equipment needed to implement the eLoran system in the U.S. should the DOT select eLoran to be part of a more resilient national PNT solution.

As a member of the Hellen Systems Team, Microchip will provide the time and frequency equipment (TFE) needed at the eLoran transmitter sites and for transferring time from authoritative sources like USNO and NIST to the eLoran system, as well as the eLoran receiver equipment for critical infrastructure operators and other domestic eLoran users. Additionally, Microchip will provide the TFE and eLoran receiver equipment used at the eLoran Reference Stations which determine regional differential timing corrections for users who require high accuracy. By pairing an eLoran receiver with Microchip's BlueSky GNSS Firewall protection solutions and atomic clocks, critical infrastructure operators can significantly increase the resiliency of their timing networks in support of Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services, issued on 12 February 2020.

We applaud NIST for initiating contact with industry regarding more responsible use of PNT by critical infrastructure. We look forward to the opportunity for continued discussions and contributing technology and solutions to address this challenge.

Related Links

Microchip Frequency and Timing: <https://www.microchip.com/design-centers/synchronization-and-timing-systems>

DOT PNT Technology Field Demonstrations: <https://www.transportation.gov/pnt/gps-backup-demonstration-national-defense-authorization-act-2018-section-1606>

Microchip Technology GNSS BlueSky Firewall: <https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall>

GPS Threat Protection: <https://www.microsemi.com/company/technology/gps-threat-protection-and-security>