White Paper

GNSS Security for PNT Applications

Abstract

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. To guide operators of Critical Infrastructure, published best practice documents by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) have described a number of steps that can be taken to mitigate outages and disruptions with GPS reception, thus improving its PNT resiliency.

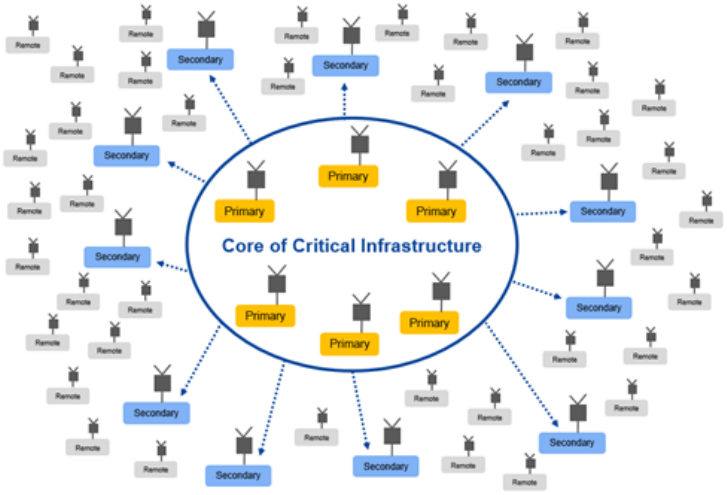
In alignment with the DHS recommendations, Microsemi provides a portfolio of technologies, products, and services that enables operators of Critical Infrastructure to construct a secure and robust PNT network that is resilient to GPS errors as well as any sky-based delivery channels such as Galileo, GLONASS, BeiDou, or another. This paper will describe a solution for securing GNSS to support PNT applications as used by Critical Infrastructure.

Critical Infrastructure Expansion

Critical Infrastructure is typically constructed in a tiered manner beginning with a set of core sites that are connected to secondary sites that are ultimately connected to remote sites. For example, in the case of a telecom and/or mobile network, the core sites are large central offices that feed smaller offices that then feed remote cabinets and/or base station sites. With the rollout of future 5G networks, densification and massive deployment of wireless access points will improve coverage and enable higher bandwidths to support the promise of IoT and related services. As a second example, within power utility infrastructure, the core power grid network is augmented and expanded with alternative energy sources, such as solar and wind. This transformation creates higher volumes and more dispersed nodes as energy management transitions to the smart grid.

At the foundation of critical infrastructure buildout is the use of PNT delivered using GNSS. According to the GNSS Market Report, Issue 5, copyright© European GNSS Agency, 2017, professional market segments such as Maritime, Rail, Telecom/Utility/Enterprise, Surveying, Aviation, Agriculture, and Drones, which use GNSS devices to operate their infrastructures, benefit billions of people globally on a day-to-day basis—from providing enjoyable produce of sustainable and cost-effective agriculture, to efficiently coordinating transport networks, or even leveraging on GNSS-synchronized telecommunications networks. The total installed base of GNSS devices in these professional segments was estimated at 14.4 million units in 2015 and is expected to grow to 97.8 million units by 2025.

Figure 1 • Massive Expansion of Critical Infrastructure and GNSS Dependency



This expansion of Critical Infrastructure is driving a massive deployment of GNSS, thus creating an exponential increase in dependency on GNSS. 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 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 Impacting Position, Navigation, and Timing (PNT)

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.

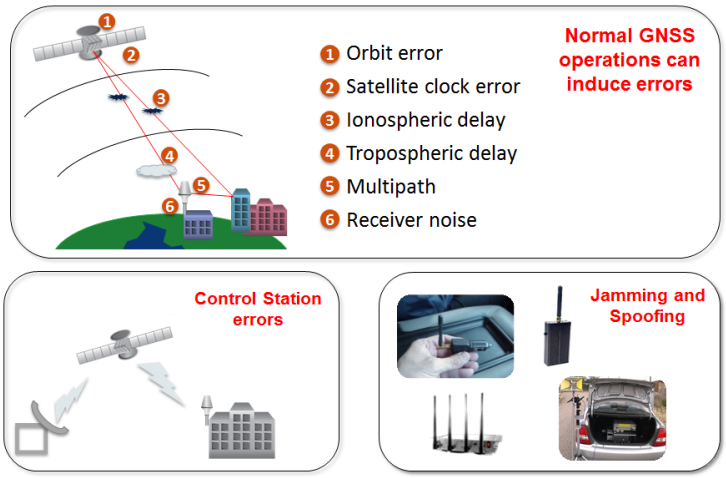
Errors can also be introduced due to issues with the GNSS system itself. Problems with the clocks onboard the satellite as well as mistakes made in uploading the timing information from ground based control stations can be contributors to GNSS failures.

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.

The following figure summarizes the types of GNSS errors previously described.

Figure 2 • Sources of Error from GNSS Delivery



To summarize, there are many types of error, both intentional and unintentional, that can impact GNSS reception. Ultimately, the goal is to ensure the integrity of PNT coming from GNSS given this wide range of susceptible environments.

Securing PNT as Used by Critical Infrastructure

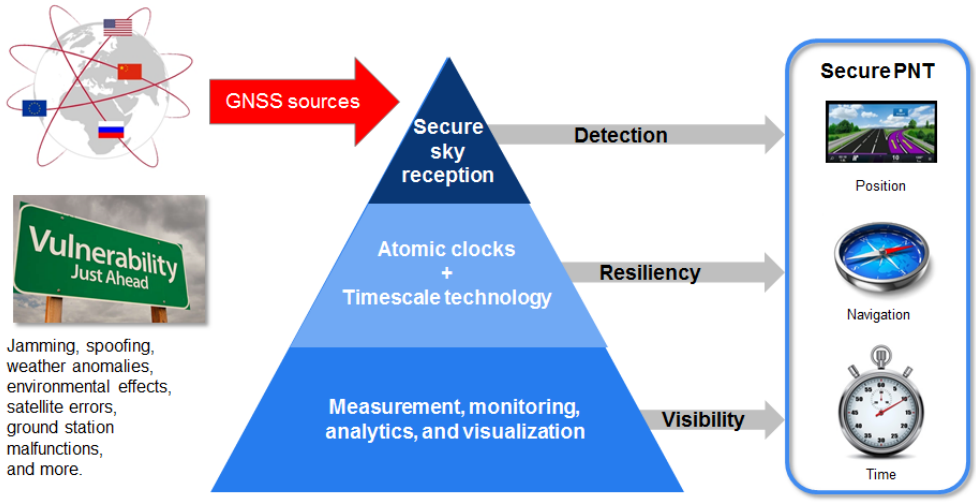
GNSS-based errors, whether intentional or unintentional, can quickly impact a vast geography and widely dispersed locations. Additionally, a large variety of operational environments must be accounted for that not only includes outside deployment with a clear view of the sky, but highly obstructed locations, urban canyons, and in-building and in-cabinet scenarios.

The following are three main objectives to consider when constructing a secure PNT infrastructure:

- Detection— early sensing of threats, both intentional or unintentional
- Resiliency—continuous operation until threats are mitigated and resolved
- 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.

Figure 3 • Secure PNT Requires Detection, Resiliency, and Visibility



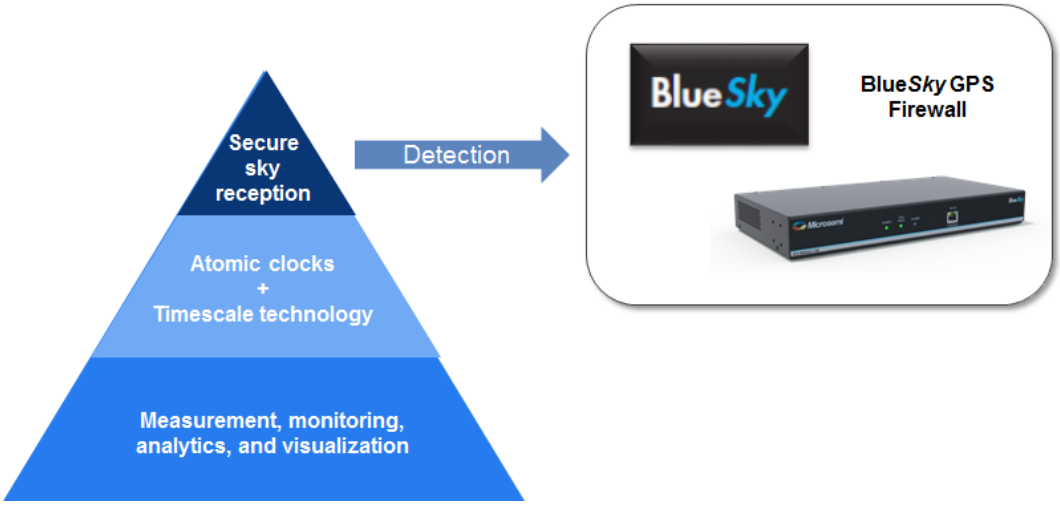
The following sections describe the solution with focus primarily on the use of time in Critical Infrastructure. Additionally, although the detection, resiliency, and visibility provided by this solution are applicable to both mobile and stationary applications, the primary target markets for this solution are stationary Critical Infrastructure, such as telecom networks, power grids, enterprise, and transportation networks and datacenters.

Secure Sky Reception

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 their 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.

Microsemi has recently launched the Blue*Sky*™ GPS Firewall that solves the problem of protecting already deployed systems by providing a cost-effective overlay solution installed between existing GPS antennas and GPS systems. Similar to a network firewall, the Blue*Sky* GPS Firewall protects systems inside the firewall from untrusted, sky-based signals outside the firewall.

Figure 4 • BlueSky GPS Firewall



A software engine that analyzes the GPS signal is contained within the Blue*Sky* GPS Firewall. The GPS signal data is received and evaluated from each satellite to ensure compliance, along with analyzing received signal characteristics. This information is used by the firewall to eliminate anomalous GPS signals and provide a hardened GPS signal output to downstream GPS systems.

The Blue*Sky* GPS Firewall can be deployed in-line between any standard GPS antenna and stationary GPS receiver to provide detection of GPS signal incidents before they enter into a GPS receiver system. The system can be deployed in-building and/or in a cabinet without requiring changes to the GPS antenna and/or cabling.

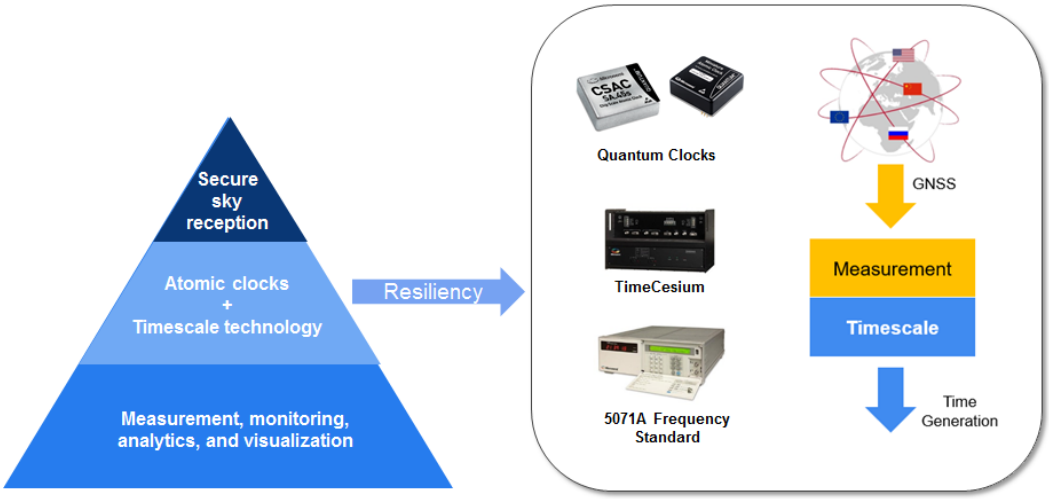
Figure 5 • Deployment of GPS Firewall

Similar to network security threats, new GPS errors are on the rise and Microsemi is continuously tracking GPS signal manipulation including spoofing threats, jamming incidents, multipath signal interference, space weather, and many other issues that can create GPS signal anomalies, disruptions, and outages.

At the core of the Blue*Sky* GPS Firewall is a programmable anomaly detector that validates the GPS subframes for spoofing incidents based on defined data validation rules. A wide range of rules have already been built into the Blue*Sky* GPS Firewall to detect suspicious time and position inconsistencies. As with traditional security firewalls, new validation rules are dynamically loaded into the Blue*Sky* GPS Firewall as new threats are identified.

Atomic Clocks and Timescale Technology

When a GNSS failure occurs, dispatching personnel to a location to resolve an issue could take hours or even days. Critical Infrastructure operators rely on holdover clocks to provide valuable operational benefits and for service continuity during such conditions.



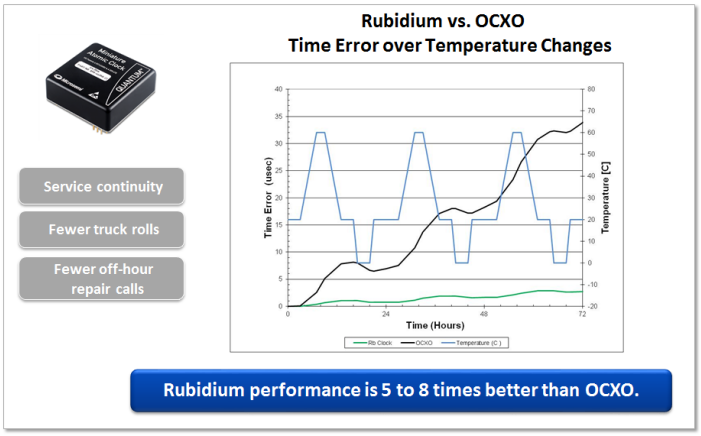
There are a wide variety of oscillator types in use today that have been deployed for the purpose of holdover, each providing a different performance/cost profile. It's important to have a clear understanding of the accuracy and period of time that the holdover is needed for and the ability of the holdover clock to maintain the needed performance given changing environmental conditions, particularly temperature variations.

Atomic Holdover Clocks

Microsemi has leveraged significant advances in miniaturization and integration to design the world's first commercially available miniature atomic clocks. These Quantum™ atomic clocks include the newly enhanced Miniature Atomic Clock (MAC) that provides a new generation of rubidium clock technology and the Chip Scale Atomic Clock (CSAC), the world's smallest atomic reference that achieves historic breakthroughs in size, weight, and power consumption.

Previously, ovenized crystal oscillators (OCXO) were a popular choice for holdover prior to Quantum atomic clock technology, even though rubidium oscillators in particular have proven to provide far better holdover performance. However, now with the new Quantum MAC (rubidium based), time error performance, over temperature, is now possible at an economical price for time holdover applications. In fact, the performance advantage of the Quantum MAC as compared to an OCXO has proven to be 5 to 8 times better.

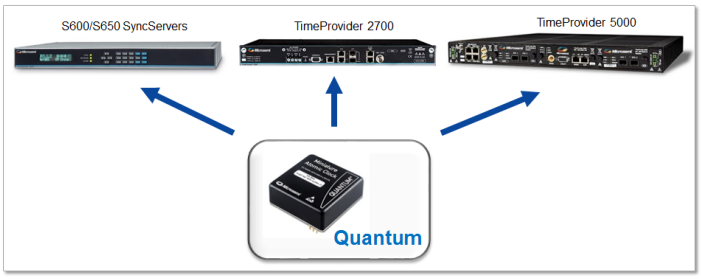
Figure 6 • Rubidium vs. OCXO Holdover Performance



This improved holdover performance provides tremendous benefits in reducing truck rolls and repair calls for Critical Infrastructure operators. The previous plot provides an example of the performance advantage of a Quantum rubidium MAC rubidium versus legacy OCXO technology.

Quantum clocks are utilized across many Microsemi system-level products providing unmatched holdover performance, maintaining reliable service over multiple days upon disruption or complete loss of GNSS.

Figure 7 • Quantum MAC for Holdover



This holdover is particularly important for Critical Infrastructure operation in support of timing and synchronization applications, including wireless base stations, wire line network infrastructure, defense systems, and test and measurement devices.

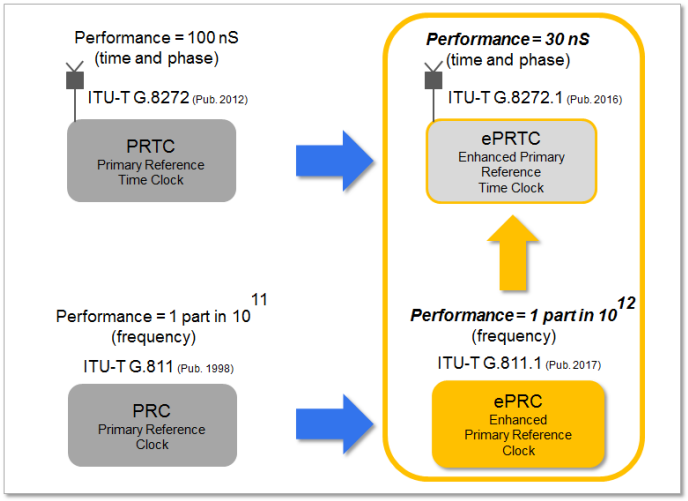
Autonomous Clocks and Timescale Technology

Cesium beam atomic clocks, such as Microsemi's 5071A and TimeCesium products, have been popular frequency standards for deployment in Critical Infrastructure for many years. The cesium clock used in communications networks is referred to as a primary reference clock (PRC) by the International Telecommunications Union (ITU-T) in the document titled "Timing characteristics of primary reference clocks" (G.811). ITU-T G.811 describes the details of a PRC and the frequency performance requirements—in particular, the accuracy being **1 part in 10^{11}**.

The ITU-T G.811 recommendation was originally created back in 1998. Now, almost 20 years later, this standard has just been modified to include a much higher level of performance, much of which has been driven by GNSS error concerns. This change has driven the performance requirement an order of magnitude higher with an accuracy specification of **1 part in 10^{12}**. This new standard from ITU is referred to as the enhanced primary reference clock (ePRC) G.811.1.

The ePRC clock performance requirement is being defined in conjunction with another new standard from ITU called the enhanced primary reference time clock (ePRTC). The ePRTC recommendation (ITU-T G.8272.1) defines a highly accurate time source that must be able to operate autonomously. The G. 8272.1 standard is an evolution of the previous PRTC standard (G.8272) that defined time and phase requirements for next generation telecom/wireless source clocks relative to GNSS. The following diagram summarizes the significant change in ITU standards for ePRC and ePRTC clocks.

Figure 8 • Primary Reference Clock Standards



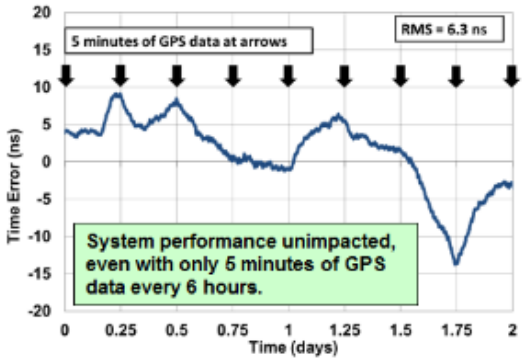
Similarly, to how an ePRC is an autonomous frequency standard, the ePRTC is an autonomous time standard. However, to construct an ePRTC to deliver autonomous time, there needs to be a way to reduce the dependency of the ePRTC on its source of time, which is typically delivered through GNSS. This is where the need for an autonomous frequency standard comes into play. By feeding an ePRTC system with an autonomous frequency standard (like cesium, as defined by the ePRC recommendation), the ePRTC system can continue to generate time, even in the absence of the GNSS signal. We refer to these types of systems as a timescale.

Timescale Technology

The timescale function is the cornerstone to generating and maintaining time for Critical Infrastructure under any failure condition. Unlike a GNSS receiver, instead of if the externally delivered time is correct, a timescale algorithm evaluates and measures its own autonomous timescale relative to the incoming time reference. In other words, the timescale algorithm slowly creates its own local time that has been aligned with the external GNSS source but is not dependent on the existence of the external source. To achieve this, the timescale maintains time by relying on an autonomous frequency standard.

The following plot is an example of a system that generates time by making measurements of 5 minutes' worth of GPS data collected every 6 hours. In this example, the autonomous timescale algorithm generates local time steered by measurements relative to an external GNSS reference.

Figure 9 • Timescale Generation Using Sparse GPS Data

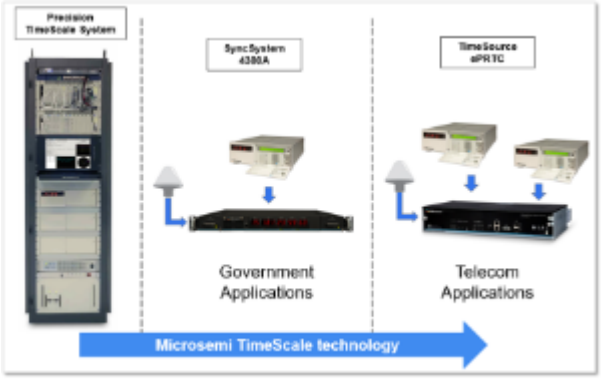


This approach is inherently resilient to GNSS outages because the local timescale continues to propagate time forward based upon phase, frequency, and aging characteristics of the reference(s) that have been measured over a prolonged period of time. This is a fundamentally different approach to traditional holdover modes in which the last frequency steer is maintained during a GNSS outage.

Microsemi's timescale technology is implemented in a number of products ranging from large metrology based systems, referred to as Precision Time Scale Systems (PTSS) to smaller rack mounted systems such as the SyncSystem 4380 (typically deployed in government networks) and the TimeSource ePRTC (deployed in telecom and mobile networks).

The Microsemi TimeScale Portfolio, shown as follows, covers a broad range of critical infrastructure sectors.

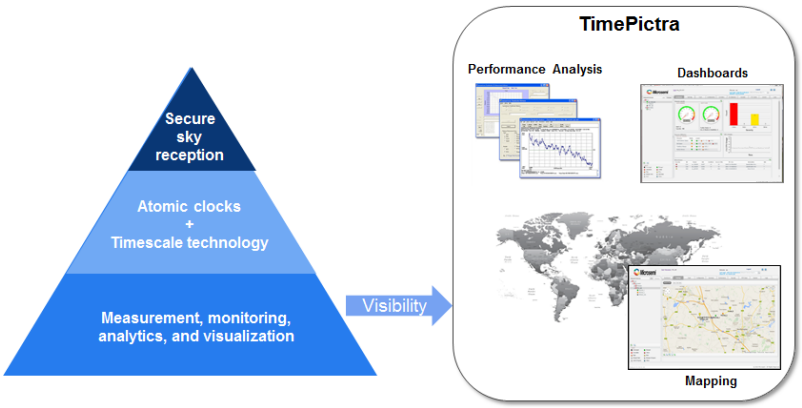
Figure 10 • Microsemi TimeScale Portfolio



Measurement and Monitoring

As timing and synchronization has grown in importance within Critical Infrastructure networks, centralized management and visibility of this vital function has become essential to network operations. Applications such as 4G/LTE (and upcoming 5G) mobile networks, Smart Grid power station control, and high-frequency trading have increased the requirements for accurate and precise timing. As a result, centralized visibility and management of network timing has become essential for ensuring reliable network performance and the successful delivery of services. Microsemi's TimePictra software platform provides measurement, monitoring, data analysis, and end-to-end visibility of networks containing critical timing needs at 10s, 100s, and 1000s of nodes.

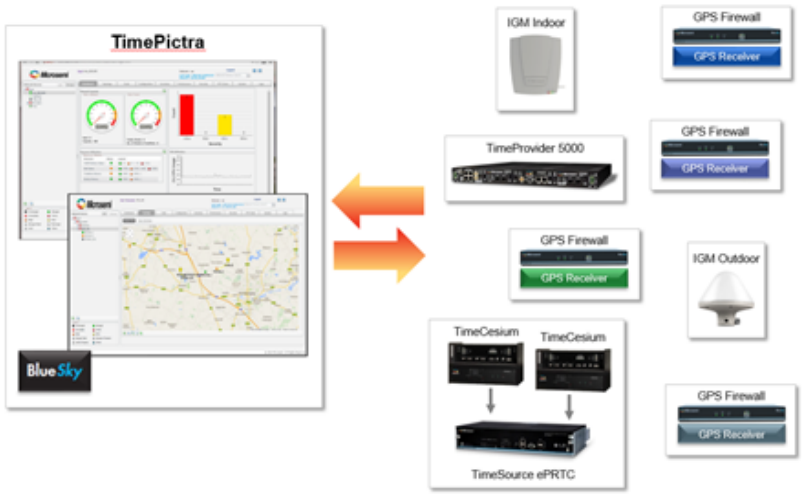
Figure 11 • Measurement and Monitoring



TimePictra is a carrier grade software solution that provides Critical Infrastructure operators with a very broad and granular visibility of the synchronization network. TimePictra allows Critical Infrastructure to manage both the clocks in the network as well as the health and performance of PTP slave clocks distributed throughout the network—including clients not supplied by Microsemi.

TimePictra has recently been enhanced to support the Blue*Sky* GPS Firewall as a managed network element including auto discovery and alarm reporting, Satellite Vehicle (SV) tracking details, latitude and longitude for mapping, and remote control. A future release of TimePictra will support the ability to dynamically upgrade validation rules within the Blue*Sky* GPS Firewall.

Figure 12 • Time and Frequency Monitoring and Management

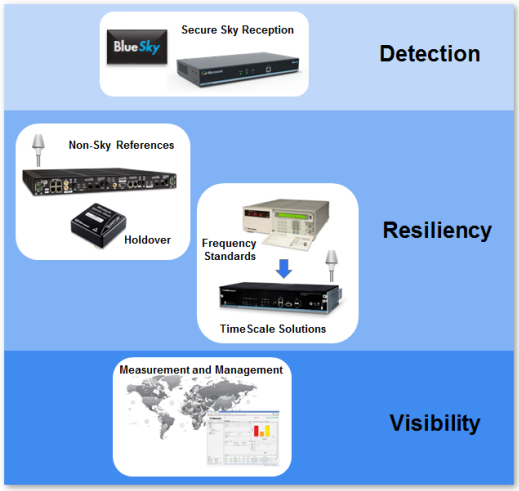


Summary and Conclusion

The dependency of Critical Infrastructure on position, navigation, and timing (PNT) continues to grow exponentially with the delivery of PNT being highly dependent on GNSS. The threat of GNSS errors has become real: signal anomalies, regional disruptions, and even global outages have already occurred. Governments across the globe are now asking their Critical Infrastructure providers for plans and solutions to defend against this serious threat.

This paper has described a strategy and solution for securing PNT (with emphasis on the use of timing) as used by Critical Infrastructure providers. The primary objective of this strategy is to provide Critical Infrastructure operators with detection, resiliency, and visibility capabilities that can scale across 10s, 100s, and 1000s of network nodes.

Figure 13 • PNT Protection for Critical Infrastructure



The solution is comprehensive and includes GNSS anti-jamming and anti-spoofing technology, network time protocol distribution, atomic clocks, timescale technology, and software management and monitoring.

Customers interested in this solution should contact their local Microsemi certified partner and/or Microsemi directly at sales@microsemi.com.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

MSCC-0104-WP-01003-1.00-0917