



White Paper

Resilient PNT:

How to Detect, Protect and Prevent Disruption of GPS/GNSS/PNT Signals and Sources

A Review of Current and Future Technologies with Recommendations for Critical Infrastructure

By John Fischer

VP, Advanced R&D, Orolia

Resilient PNT: How to Detect, Protect and Prevent Disruption of GPS/GNSS/PNT Signals and Sources

Table of Contents

Executive Summary	3
Introduction	3
Strategies to Manage Cybersecurity Risks for PNT.....	4
Figure 1 – Various PNT Sources to Make Critical Infrastructure Resilient.....	4
Table 1 – PNT Source Technologies Applicability to Critical Infrastructure Sectors.....	5
Figure 2 – Cellular Wireless Networks and PNT.....	9
Figure 3 – Datacenter Sync Application	10
Figure 4 – Power Grid Dependency on Precise Time.....	11
Techniques for Detecting Disruptions or Manipulation of PNT Sources	12
Techniques for Recovery and Response – Making PNT Systems Resilient	13
Other Considerations.....	13
In Conclusion	15
About the Author	16
About Orolia	16

Executive Summary

For the last two decades, reliance upon GPS/GNSS for positioning, navigation and timing (PNT) by civilian applications has been an overwhelming success, providing increasingly accurate and reliable PNT information everywhere for free. However, in recent years, malicious threats have emerged have exposed the Achilles heel of GPS/GNSS: Its weak power and unencrypted signal format leave it vulnerable to jamming and spoofing. The loss of PNT information can result in rare but catastrophic events, crippling critical infrastructure that is necessary for our survival.

Fortunately, there are many alternative technologies available to augment GPS and provide accurate and reliable PNT information even under extremely adverse conditions. These include:

- Low Earth Orbit (LEO) PNT satellite signals – operating close to the Earth, with signal strengths ~1000x stronger than GPS, to overcome jamming. And, encrypted to prevent spoofing.
- Miniaturized, affordable atomic clocks to provide precise time internally – which is the foundation of every positioning system –, without connection to, or reliance on, outside sources which could corrupt the precision.
- Fiber optic network time distribution via secure, high accuracy protocols.

In this white paper, we will discuss these alternative technologies and offer recommendations for procedures and processes to manage and avoid the risks of cyberattacks, applying the best practices known today. We will focus on Resilient PNT and describe the strategies, technologies and procedures to avoid these cybersecurity risks and ensure the continuity of any critical operation.

Introduction

Counterattack approaches to the disruption of GPS/GNSS/PNT signals and sources may differ across various critical infrastructure sectors, which the federal government has defined as the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response.

To this list we should add datacenters. With the move to ubiquitous cloud computing, datacenters operate thousands of servers globally and simultaneously, using the same data. These operations require precise time synchronization. Moreover, because much of the data comes from mobile applications, positioning is crucial. The datacenters at the heart of most cloud computing – for example, Google searches, ecommerce, email services, and hosted applications – rely heavily on PNT.

Datacenters are often lumped under “communications infrastructure,” but they have their own unique issues. A specific example of datacenters would be financial services. The stock exchanges, and high-frequency trading applications in particular, need precise, sub-microsecond level time synchronization to operate.

Strategies to Manage Cybersecurity Risks for PNT

The most important strategy is to avoid reliance upon any single PNT source. GPS, as great as it is in providing the necessary PNT accuracy and coverage, is highly vulnerable to jamming and spoofing.

No other PNT source, however, is foolproof. Each has its own strengths and weaknesses. Therefore, the best strategy is to use multiple, diverse PNT sources together – sources that have different failure modes and characteristics so that the vulnerabilities of one source are counteracted by the strengths of another. Algorithms exist that can intelligently select and combine various PNT sources into a composite solution.

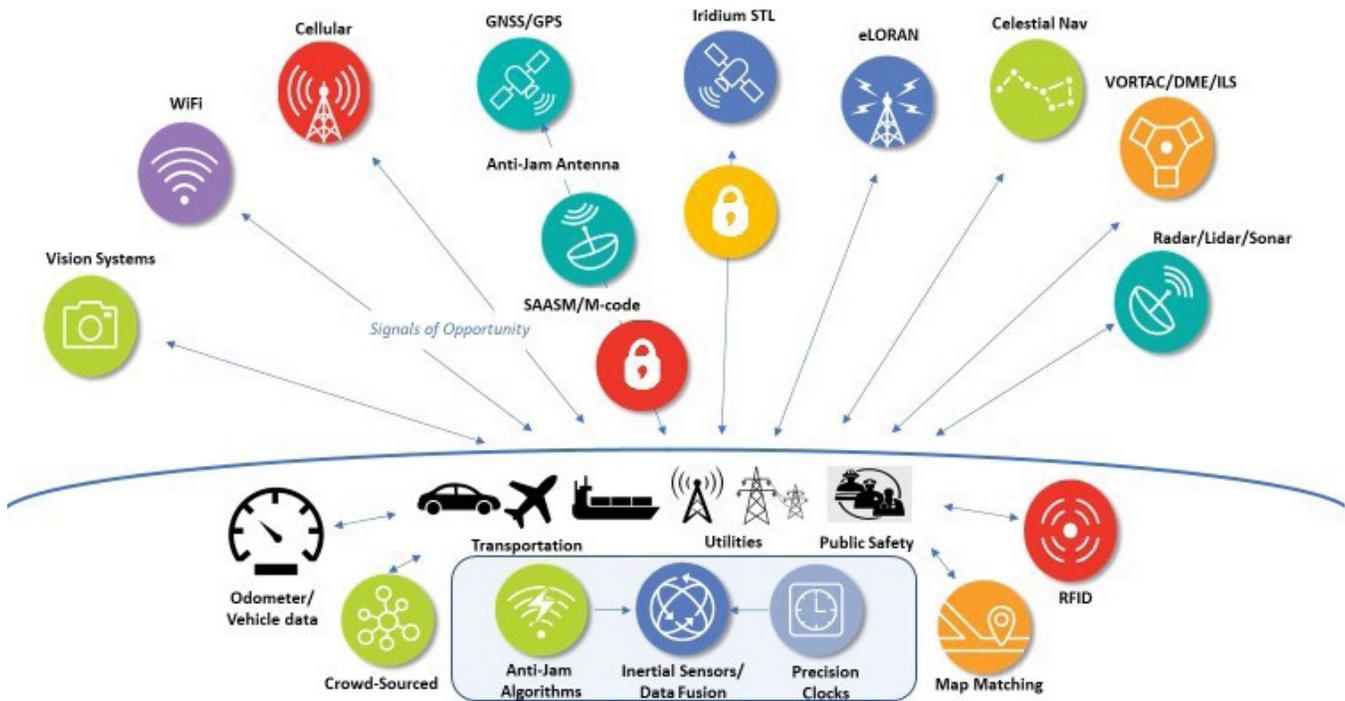


Figure 1 – Various PNT Sources to Make Critical Infrastructure Resilient

In Figure 1, we identify the many PNT technology sources available, and in Table 1 we show the applicability of each source to the critical infrastructure sectors.

As shown in the legend, a technology is either applicable or it is not. Table 1 also identifies whether an applicable technology is lacking in accuracy or coverage – in other words, it can be used, but improved accuracy or coverage is highly desirable.

In other cases, a technology may not be applicable because, for example, it provides positioning only when timing is required, or because accuracy or coverage is insufficient to meet even minimal requirements. These classifications are very general, and there are always exceptions and special cases, but it is a starting point for where each technology is primarily used.

Table 1 – PNT Source Technologies Applicability to Critical Infrastructure Sectors

PNT Technologies	Automotive	Air Nav	Sea Nav	Rail	Pedestrian	Telecom	Data Centers	Power Grid	Precision Ag	Public Safety
PNT RF Sources										
GPS	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
Other GNSS	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
LEO PNT	▲	▲/■	▲	▲	▲	▲	▲	▲	▲/■	▲
Dedicated Terrestrial Tx	■	■	▲/■	▲/●	▲	▲/●	■	▲/●	■	▲/●
eLoran	■	▲/●	▲/●	▲/●	▲/●	▲/●	■	▲/●	■	▲/●
VOR/TAC/DME/ILS	X	▲	●	●	X	X	X	X	X	X
Signals of Opportunity										
Cellular	■	■	●	▲	▲	X	▲	▲	■	▲
WiFi	■/●	■/●	■/●	■/●	▲	■/●	■/●	■/●	■/●	■/●
Broadcast TV	■	■	●	■	▲	▲	■	▲	■	■
RFID	▲	X	X	▲	▲	X	X	X	▲	▲
Autonomous										
IMUs	▲	▲	▲	▲	▲	X	X	X	▲	▲
Atomic Clocks	X	▲	▲	▲	X	▲	▲	▲	▲	▲
Map Matching	▲	▲	▲/●	▲	▲	X	X	X	▲	▲
Networked										
Timing	X	X	X	X	X	▲	▲	▲	X	▲
Crowd Sourced/Collaborative	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
Vision										
Video and IR cameras	▲	▲	▲	▲	▲	X	X	X	▲	▲
Lidar	▲	▲	▲	▲	X	X	X	X	▲	▲
Radar	▲	▲	▲	▲	▲	X	X	X	▲	▲
Sonar	▲	▲/■	▲	▲	▲	X	X	X	▲	▲
Sensing										
Magnetic	▲/■	▲	▲	▲	▲	X	X	X	■	■/●
Celestial (Sextant) - night	▲/●	▲/●	▲/●	▲/●	●	X	X	X	▲/●	X
Sky Polarization - day	▲/■	▲/●	▲/●	▲/●	●	X	X	X	▲/●	X
Odometer/Pedometer	▲/■	X	X	▲/■	▲/■	X	X	X	▲/■	▲/●/■
Legend										
	▲	Applicable								
	■	Lacking in Accuracy								
	●	Lacking in Coverage								
	X	Not Applicable								

Technology Characteristics

- **GNSS vs. GPS** – all GNSS systems (GLONASS, Galileo, Beidou, and GPS) are very similar in operation and have similar vulnerabilities and strengths, so using multi-constellations does not offer much diversity. They all share the same few frequency bands. In general, if one system is jammed, they all are. However, using multiple constellations will yield independent verification of each system. It takes a more sophisticated spoofer to fake all constellations, but it can be done.

The other advantage of using multi-constellations is that it will catch an anomaly on an individual system. For example, the [13-microsecond GPS glitch in January 2016](#), the [error in the GLONASS system in April 2014](#), and the [Galileo timing glitch in the summer of 2019](#), would all have been detected by systems using multi-GNSS receivers with appropriate cross-checking algorithms. On the other hand, these other systems are quite new and their failure modes are still unknown. Further, dependency on non-USA sources has national security issues too.

- **LEO PNT** – the broad applicability stated here is based not only on what is available today from [STL](#) transmitting from the 66 satellite Iridium constellation, but also includes the eventual performance expected when LEO PNT signals are available on thousands of satellites from other constellations such as OneWeb, Boeing, Space-X, etc. The accuracy limitations of STL today are due to two major factors: geometric dilution, because not enough satellites are visible simultaneously, and limited signal bandwidth. Neither of these two factors should be an issue for future systems.
- **Dedicated Terrestrial Transmitters** – includes technology represented by [NextNav LLC](#), [Locata](#), [Phasor Lab](#) and others. These systems require installing a transmitting infrastructure, so are best used in specific environments such as urban centers, warehouses or test ranges. Area of coverage depends on the allowed transmitter power.
- **eLoran** – does not exist operationally today in the USA, but it is applicable for a number of sectors if a large-scale build-out were implemented. Prior to the existence of GPS, Long Range Navigation (LORAN) was used for coastal and river marine navigation in the USA. A few dozen high power stations provided this coverage until the early 2000s. With today's Digital Signal Processing (DSP) technology, better accuracy and coverage is possible. With fewer than 100 stations, complete coverage of USA populated areas should be possible; even fewer would be needed for timing applications only.
- **VOR/TAC/DME/ILS** – VHF Omnidirectional Range, Tactical Aircraft Control, Distance Measuring Equipment, and Instrument Landing Systems are all ground-based RF signals generated near and around airports for flight guidance. One can imagine these old systems being adapted for other uses, but the signal structures were developed in the early to mid-20th century for primitive wireless electronics, so much better approaches can be imagined. However, changes to these signal formats is encumbered by the massive avionics installed base, to which compatibility must be maintained.



Signals of Opportunity are RF signals that were not designed for transmitting PNT information, but with little or no modification can be used to determine position or time.

- **Cellular** includes 4G/LTE and 5G networks. Positioning from cellular is done today, achieving better than 100m accuracy. 5G can provide higher accuracy than 4G/LTE, and further improvements can be considered so that position accuracy could approach GNSS, but as of today, it is less accurate. Not included here is how cellular provides the “Assisted GNSS” function – using the data network to transport navigation messages to GNSS receivers faster and more reliably than receiving them directly from the satellite.
- **WiFi** is neither accurate nor provides enough practical coverage to be considered for anything but a pedestrian use case – typically for indoor positioning.
- **Broadcast TV** assumes that improvements would be made to synchronize existing transmissions, but further build-out would most likely not happen in the future because the bandwidth is far too valuable for 5G. Any specific build-out of this technology approach for PNT is related to the high-power case of a Dedicated Terrestrial Transmitter signal described previously.
- **RFID** provides positional proximity indication and therefore is not useful in timing applications.



Autonomous sensors refer to self-contained devices that do not rely on outside connections or signals and therefore, in general, are resistant to jamming or spoofing.

- **IMUs** an Inertial Measurement Unit (or, when combined with a navigation processing unit and a precision timekeeping device, is called an INS – Inertial Navigation System), measures forces on the object (vehicle) to determine position movement or attitude changes.
- **Atomic Clocks** are becoming smaller, lightweight, lower in power consumption and more affordable, enough to be practical in many applications today. They maintain precise time in the absence of GNSS for hours or even days, depending on the requirements. We call this interval of no access to GNSS the Holdover Time. Since timekeeping is a part of Inertial Navigation, a precise clock aids in navigation too.
- **Map Matching** is used in combination with other sensors. It provides registration to predefined lanes and can help improve accuracy. Examples are cars aligned to streets or an aircraft using terrain following from radar/lidar measurements aligned to internal digital maps to determine position and heading. As memory becomes cheaper and network connectivity becomes ubiquitous, detailed maps of the entire world can be available on-demand.

Networked schemes require connectivity to a network, either wired or wireless.

- Precise **Timing** can be transferred across a network, and this is a very effective and secure method of synchronization. The [Network Time Protocol \(NTP\)](#) and [Precision Time Protocol \(PTP\)](#) are in wide use today. The High Accuracy version of PTP, colloquially known as “White Rabbit” (WR), provides the best time distribution today, with accuracies in the one nanosecond range. Network time distribution via fiber optic is the

ideal, diverse complement to GNSS-derived time synchronization. Together, they create accurate, reliable time sync much more resilient to attack. Moreover, recently the Internet Engineering Task Force (IETF) has adopted a [Network Time Security \(NTS\) Standard](#) so that these protocols can be secure. Additionally, a [Best Current Practices](#) document has been published that goes beyond merely simple compliance with standards, and informs system design engineers on how to best avoid attacks.

- **Crowd-Sourced/Collaborative** methods work on the idea that if other nodes on a network to which you are connected know their positions, and you have some indication of your relative proximity to them, you can infer your own position. Indications of proximity include RF signal strength on a wireless network, or roundtrip packet delay on a wired network. Analogously for the time sync situation, multiple nodes on a network can consensually sync together without necessarily being connected to a master source like GPS. The more participants on the network, the better the probability of resulting in a PNT solution, and the smaller the error ellipse will be. Of course, collaboration is not a PNT source itself, but when combined with diverse sources, it is a powerful estimation method.

Vision systems provide positional awareness much the same way as humans are made aware of their locations – through visual cues to recognized landmarks. However, they do not help with time determination.

- **Camera** imaging combined with map matching provides both position and attitude determination.
- **Lidar** uses laser range finding to create a 3D point map of a surrounding area.
- **Radar** operates similarly to lidar but with much less angular resolution. It is less impacted by smoke/fog/rain/snow than optical methods, and recent advances in semiconductors have made it very affordable.
- **Sonar** is not viable for high speed aircraft, but it provides proximity detection for use with other methods.

Sensing is like Vision but with these unique characteristics:

- Sensing the Earth's **magnetic** field is not a very accurate method for heading determination, but it can provide an approximate initial state for inertial navigation.
- **Celestial** navigation is an ancient form of navigation for mariners that has been automated with cameras and image recognition processing. However, stars are only visible on clear nights or at extremely high altitudes.
- **Sky Polarization** sensing takes advantage of the phenomenon where the sun's light is polarized differently at various angles of incidence with the atmosphere. By knowing the date and time and a rough estimate of your latitude and longitude, you can obtain a precise estimate of north orientation. Combined with celestial navigation, this can provide compass direction in both day and night conditions, though it does not operate well under all sky conditions with cloud cover.



Infrastructure Sector Characteristics

- **Automotive** has two main requirements:
 1. Steering the vehicle for autonomous driving. This is a safety of life concern and GNSS is not reliable enough to be part of this function.
 2. Navigation – knowing where the car is and directing where it should go. This includes both the driver and driverless cases. Example: summoning a rideshare car.
- **Air Navigation** has its own unique instrumentation systems (see VOR/TAC above), but two growing factors of concern are:
 1. ADS-B – the Automatic Dependent Surveillance-Broadcast system is dependent on accurate and reliable position indications derived from GPS. The integrity of these position reports will determine its safe operation. Moreover, the ADS-B signal itself can be spoofed, creating an additional risk.
 2. UAVs – the growing use of UAVs in more applications is driving the need to integrate them into the National Air Space. Accurate, reliable and high integrity PNT is paramount for this to happen.
- **Sea Navigation** relies heavily on GNSS, and in recent years has been subject to several spoofing and jamming attacks worldwide. GNSS position reports feed the Automatic Identification System (AIS), which communicates with other entities in the area, so inaccurate reports can cause widespread confusion. The International Maritime Organization (IMO) is investigating new methods for resilient navigation.
- **Rail** needs PNT for Positive Train Control (PTC) to enhance safety and for efficient operations.
- In this chart we assume that the **pedestrian** does not have critical accuracy, reliability or integrity requirements and the use is primarily indoor.
- **Telecom** has had two traditional uses for PNT:
 1. For the wireless cellular network as shown in Figure 2:

Cellular Network's Dependence on GNSS

GNSS receivers at each cellular basestation provides two services:

1. Time sync so all the cells transmit at the same time
2. Precise frequency so they all align

This ensures clean coverage in the overlapping regions of adjacent cells

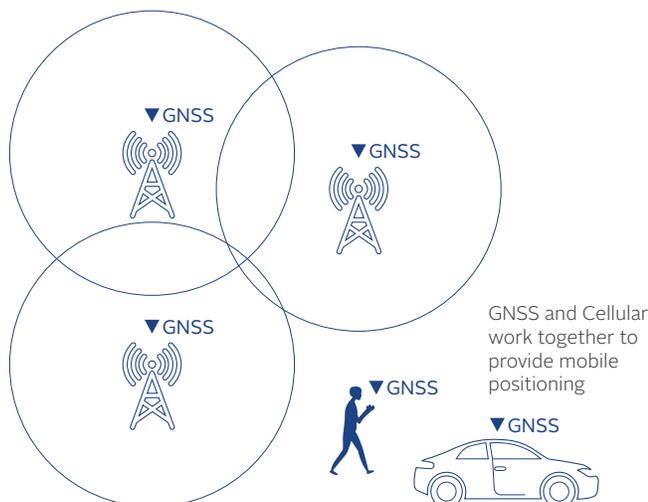


Figure 2: Cellular Wireless Networks and PNT

Cellular and GNSS Relationships

current

1. Adjacent cell time and frequency sync
2. Assisted GNSS - nav msgs, time of day, and gross location received over cellular network (Mbps) instead of GNSS channel (50 bps) to shorten GNSS acquisition time
3. e911/eCall - cellular network provides ~100 M positioning required by law through combination GNSS and sector location/time of arrival

2. For legacy wireline synchronization of the Synchronous Data Hierarchy (SDH) network. This harkens back to when “T1” lines were the interconnection backbone for data networks. A Primary Reference Clock (PRC), which was a cesium-based atomic clock, provided the master timing for the entire network. Today, this has been mostly replaced by asynchronous packet-based connections (IP/Ethernet), though some legacy systems still exist. Wireline sync for SDH should not be a driver for future resiliency requirements

Note that wireline sync for SDH (the application) should not be confused with network timing (the technology). The technology is still very viable, as previously described. It is just that the applications that use it have evolved. SDH is now obsolete and we do not need to maintain precise time for network transport.

- **Datacenters** – The primary need for PNT here is to synchronize each processing element to a common time reference. This is necessary so that each element knows which transaction happened first, which happened second, etc. Examples of Datacenter operators are Google, AWS, Azure, and Verizon. In most cases, all that is needed is relative sync, not absolute sync, to Coordinated Universal Time (UTC). However, when processing elements are separated across wide areas (such as different cities or countries), GPS sync is the simplest and most accurate way to achieve it. Sync accuracy determines the efficiency of multi-processing. The more uncertain two processing elements are about their relative time references, the more “guard” or “wait” time they must use to have transactions settle before continuing or risk the probability of an error.

A secondary need for PNT is for mobile data. As more transactions are executed from mobile users and, with the emergence of the Internet of Things (IoT), more objects that physically move are executing transactions. These data packets need to be accurately geo-timestamped for meaningful processing to occur. The quality of information extracted from “Big Data” mining is very dependent upon the veracity of the PNT tag.

With 5G comes more bandwidth, enabling more real-time applications to run in the cloud. With this trend, latency and time performance monitoring will become more critical.

- The **Power Grid** depends on precise time synchronization, as shown in Figure 3. Keeping the 60 Hz AC power in phase across the grid is a challenge. The main device supporting this process is the PMU – Phase Measurement Unit. It monitors the sine wave against a reference time, usually GPS, and provides feedback to the systems controlling phase alignment. One degree of phase error in this 60 Hz sine wave is 46 microseconds, so accuracies of tens of microseconds in measurement are desired, though ~100s microsecond errors can be tolerated. The other class of devices requiring sync are the Digital Fault Recorder (DFR) and Sequence of Event Recorders (SER). To diagnose faults and determine causal relationships, you must have a common time reference to know what happened first, what happened next, etc. Just like many other sectors, the power grid only needs relative time, not absolute UTC time, but when operating over wide distances, UTC or GPS time is the easiest way to access a common clock. Two trends are occurring in the power industry that will influence its evolving need for resilient PNT:

1. **Distributed power generation** – as we move from central power generation from coal, oil, gas and nuclear stations to renewables like wind and solar, the sources of power are more distributed, more dynamic, and less controllable than before. This adds complexity to the phase controlling algorithms requiring more measurement points and stricter compliance to accuracy and reliability.

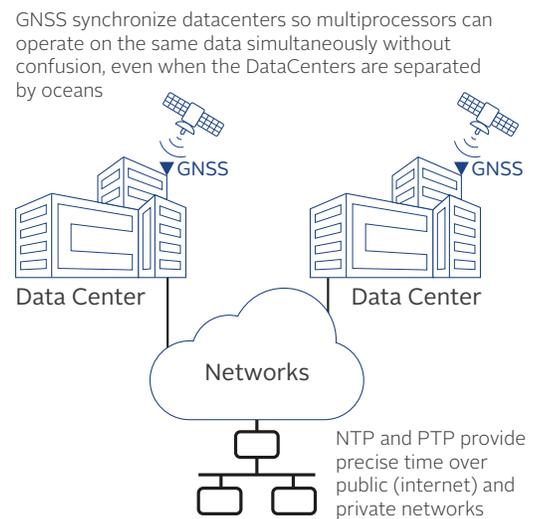


Figure 3: Datacenter Sync Application

Power Grid Dependence on PNT

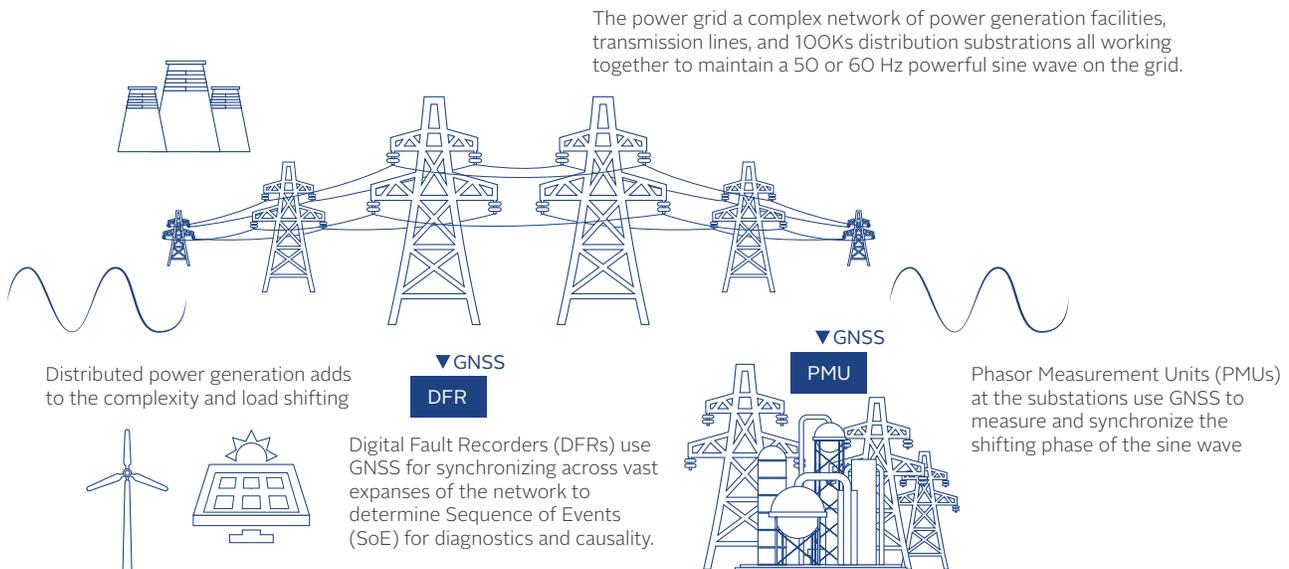


Figure 4: Power Grid Dependency on Precise Time

2. Smart Grid – a data network is being superimposed on the grid so that every device on the grid has network connectivity. For these millions of devices to be managed and to interact with each other, they need PNT information to know where these devices are and for them all to have a common time reference.
- **Precision Agriculture** requirements are similar to Automotive in that the position of the vehicle (tractor, harvester, etc.) is being controlled. However, there are some unique factors:
 - These are primarily for rural use, where fixed infrastructure is not usually available.
 - They require centimeter level accuracy for sensing operations – example are bud locations on fruit trees, moisture sensing probes, alignment with UAV cameras, crop yield measurements down to the individual plant, etc.
 - They are early adopters to driverless vehicles because they do not have the complex problem of sharing the “road” with human drivers.
 - Attitude control and sensing (pitch, roll, yaw) is necessary.

Within this sector we also include construction and surveying because they have similar requirements.

- **Public Safety** covers three major facets:
 1. Precise location and navigation for police, fire, and medical teams in emergency situations. Examples: in a burning or earthquake-damaged building, underground in a subway tunnel, when physically disabled due to injury.
 2. Frequency and Time synchronization of dedicated first responder radio networks (Simulcast).
 3. Legally traceable time sync for 911 call centers so that recordings and response times can be used as evidence in court.

Techniques for Detecting Disruptions or Manipulation of PNT Sources

After a dependent infrastructure is set up with multiple, diverse PNT sources, the best and simplest method for detection is to look for disagreement among the sources. With diverse sources, each one will have different points of vulnerabilities and different failure modes, so that failures or attacks will manifest in each source differently. Consider a timing system with three distinct sources: GNSS receiver, atomic clock, and PTP WR fiber network time. Jamming or spoofing of the GNSS signal will cause disagreement with the atomic clock and PTP-derived time; failure of the atomic clock will be detected by disagreement with GNSS and PTP time; hacking of the network with a Denial of Service (DoS) or Packet Delay attack will be detected by the GNSS and atomic clock. There is no single point failure.

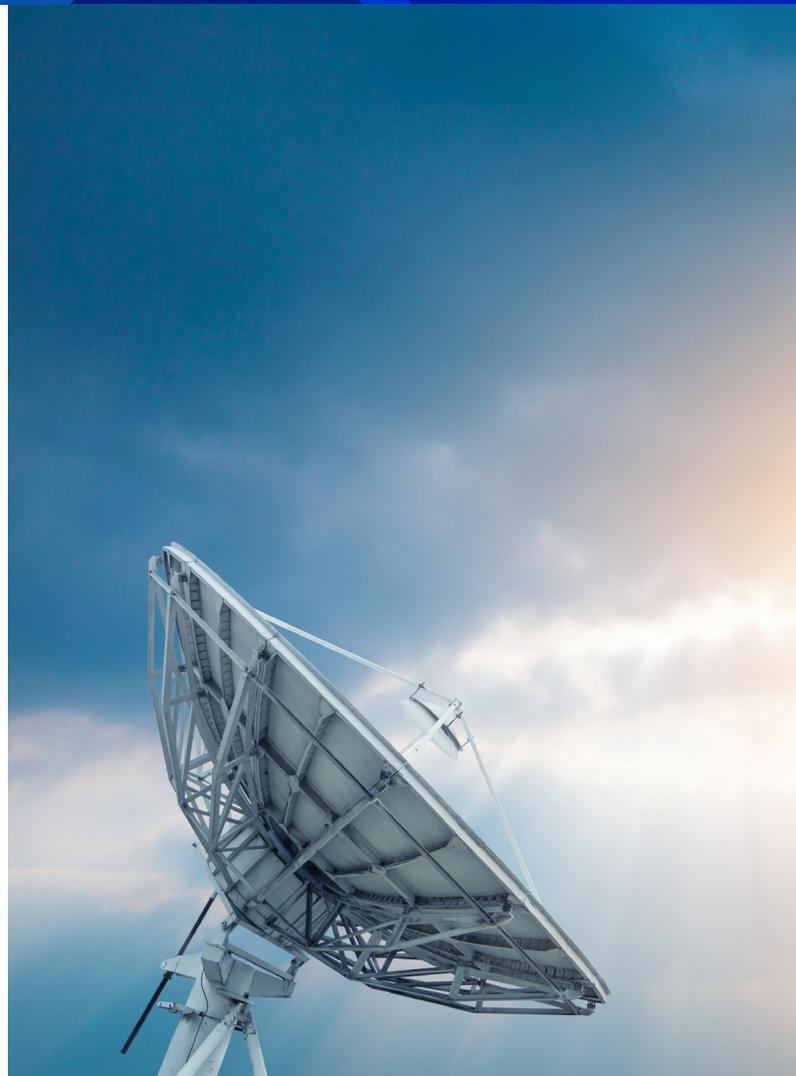
Similarly, for a positioning example, consider a vehicle with a GNSS receiver, an IMU, and an STL receiver. Jamming of the GNSS receiver would normally force the tracking to be open loop, relying on the IMU only, which would drift over time. However, with updates from the STL signals, which are 1000x stronger than GPS and more resistant to jamming, the error drift is indefinitely limited to tens of meters.

Spoofing of the GNSS signal is detected either by disagreement with STL, which is an encrypted signal that cannot be spoofed, or by the IMU, which does not sense movement in the false direction. Failure of any one of these three sources is noted by the agreement of the other two. Majority wins.

Each individual PNT source has its own detection and prevention measures. For example, there are [many jamming and spoofing detection algorithms](#) that can be applied to GNSS receivers to alert and often forewarn the infrastructure system of a possible disruption. False alarming is an issue, so using a probability-based scoring system with programmable thresholds can be helpful to keep both the false alarm and the missed detection rates low.

A simple GNSS spoofing detection technique is to use two separate receivers and antennas, spaced apart by a known distance. For example, placing one receiver/antenna combination at the fore of a ship, the other aft, will always yield two different position indications under normal operating conditions, based on their separation. If they ever indicate the same position, it is an indication of spoofing from an external source.

Detecting dropouts, discontinuities or other anomalous behavior from a particular sensor is another method of alerting. In our universe, it is impossible for an object to “jump” across the time-space continuum; it must move smoothly from one point in space-time to another and not exist at more than one point at any single instance. Therefore, an indication of discontinuity – within the bounds of measurement noise and quantization effects – is a potential failure or false manipulation of the source. Discontinuity, measurement range checking and sensor behavior monitoring can be powerful detection methods.



Techniques for Recovery and Response – Making PNT Systems Resilient

Again, with multiple diverse PNT sources feeding a composite PNT solution, detection of a compromise or fault on any one source allows it to be dropped. The earlier the detection, the quicker and more effective the recovery.

Kalman filtering, particle filtering, and artificial intelligence (AI) techniques provide for an intelligent combination of multiple PNT sources into a single solution based on probability models.

Taking preventive measures before an attack occurs can sometimes be the best response. These measures include:

- **Vulnerability Testing** – PNT systems should be analyzed and tested before they become part of critical infrastructure. For example, the University of Texas at Austin has established a standard battery of spoofing tests for GNSS receivers ([TEXBAT](#)), GNSS [Vulnerability Test Systems](#) are available from various vendors, [Certification testing](#) of GNSS receivers is available and required by some standards organizations, and the DHS (Department of Homeland Security) is establishing the [Resilient PNT Conformance Framework](#) to characterize all PNT sources and their behavior under cyberattack.
- **Protecting the Individual PNT Source** – GNSS receivers can be protected from cyberattacks using “smart antennas.” These range from expensive, multi-element Control Radiation Pattern Antennas (CRPA), which track the individual satellites with narrow beams as they move across the sky and block interference, to inexpensive horizon blocking anti-jam antennas or simple two-element null steering antennas that search and block out interference.
- **Monitoring and Logging Attack Events** – the threat landscape is dynamic and we must adapt with new strategies. Creating threat libraries as they occur and sharing these across the PNT community helps to counter them.



Other Considerations

In this section, we offer some innovative, “out-of-the-box” ideas to make PNT systems more resilient:

- **Consider the cessation of the leap second.** Though this requires the international treaty agreement to change, NIST (National Institute of Standards and Technology), along with USNO (United States Naval Observatory) and BIPM (International Bureau of Weights and Measures – France) are the recognized world leaders for timekeeping. If they took the initiative, everyone would follow. The unnecessary complexity of managing this is a security risk – every few years we risk a glitch event. For example, more systems based on atomic clocks could run autonomously from GNSS for months (and therefore be less vulnerable) if they did not have to connect with GNSS to obtain UTC time as frequently to react to possible leap second notices. At its inception, the GPS system acknowledged leap seconds as an unnecessary risk, and it does not use them internally. Instead, GPS just publishes the leap second variation data so that users can convert GPS time to UTC time. It is manageable because most systems respond properly to leap second events, but every so often, some system handles it improperly. Why not avoid stressing the system by eliminating it entirely?
- **Consider using SAASM GPS receivers** at our most vulnerable, high-valued critical infrastructure points. For example, post a USMC detachment with SAASM equipment at the NYSE exchange to protect the precise timing, manage the crypto keys, etc. The federal government has the constitutional authority to regulate

interstate commerce and this could be implemented in that context and without violating the Posse Comitatus Act if coordinated with the states. Some examples: the governors of New York or New Jersey could request the federal government to provide this protection for the financial services sector if they were aware of its availability; the Commonwealth of Virginia could authorize it for its new Amazon Data Center; etc. Moreover, as the US military moves toward activation of M-code, the older P(Y) signal has less utility for military use, and any concern about exposure to compromise by a proliferation of crypto keys in the civilian sector would eventually decrease. In the interim, Orolia has patented technology that can convert the authenticated SAASM signal to a local rebroadcast of the civilian signal, reducing the number of necessary SAASM receivers. For the long term, the P(Y) signal used on SAASM could become the secure, encrypted civilian source after the military has fully transitioned to M-code. In Europe, the Galileo program has adopted this approach by providing the Public Regulated Service (PRS) as the secure civilian signal for critical infrastructure.

- **Consider protection of GNSS spectrum via enforcement** jamming and spoofing detection equipment is available today that could be placed at airports and seaports to detect and locate bad actors so they could be engaged and disarmed. However, it has been difficult for us to identify the government agency that has a mandate for providing this surveillance and the authority to pursue the perpetrators. The FAA (Federal Aviation Association) ensures the safety at airports via air traffic management, but GPS disruption monitoring and reporting is left to the pilots. DHS has the authority for port protection, but there is no program for GNSS signal surveillance at the ports. The issue extends beyond just safety to maintaining efficient operations. Container handling at the ports depends on GNSS for locating each container for loading, unloading and processing. Disruption of GNSS can and has created chaos. It is not uncommon for truckers to use illegal “privacy” GPS jammers, which, as they pull into the port, disrupt operations. Who within the government has the mandate to address this problem? The [USCG NAVCEN](#), the [FAA](#), and the [USAF](#) all have websites for manual reporting entries, but this is too slow and cumbersome to address any dynamic threats meaningfully.
- In addition to enforcement, **setting up a network of monitoring stations** can provide the intelligence needed to mitigate any GNSS jamming or spoofing. Imagine if every cell tower had inexpensive GNSS interference sensors and reported any detected signal disruptions back to a central database. Just as NOAA (National Oceanic and Atmospheric Association) has a network of radars and publishes real-time severe weather alerts, a similar “GPS Weather” reporting system could provide real-time warnings and advisories. Infrastructure owners could react quickly to these reports, knowing where and when the trouble spots occur. A library of threats would also be built so GNSS receiver manufacturers could continually improve their designs to counter these threats. This is not a far-fetched concept. Cell towers already contain GNSS receivers for providing precise time and frequency sync. As more resilient receivers and antennas are installed, the vulnerable components can remain, acting as sensors and reporting alerts on the network. In Europe, the [STRIKE3 program](#) has been monitoring and cataloging GNSS interference events for years, providing Eurocontrol with the signal intelligence needed to maintain safe air navigation. A similar program in North America would be very valuable.
- **Consider NIST endorsing encrypted Time as a Service (TaaS).** Though no one method of providing PNT is impervious to attack, providing time sync over a public fiber optic network is a diverse and secure time distribution alternative to GNSS. NIST has been offering its ~1 millisecond [Internet Time Service](#) for years. Additionally, NIST offers a [Special Calibration Service](#), which provides a fiber optic connection to NIST, calibrated initially at installation. However, to maintain assurance, this requires repeated calibration campaigns, traveling to the client’s site with portable measurement equipment. Instead, we suggest that NIST provide some certification or endorsement of any commercial entities providing TaaS. There are two main alternatives here: a public or private offering. A completely public offering would have the US government offering TaaS to

the public for a fee; a completely private offering would have NIST endorsing the standards to be met by any company offering TaaS. A more realistic approach could be a public/private partnership where private firms provided the equipment and network operations, and the government provided the national asset facilities and certification processes to ensure quality of service. It might not be practical for private companies, for example, to deploy multiple H-maser atomic clocks around the country and network them together, but colocation of network time equipment at NIST facilities in Boulder, CO or Gaithersburg MD, or at the US Naval Observatory in Washington DC could enable a reliable TaaS. Critical infrastructure owners and operators would be assured that their time is sourced from the national time standard and transported over a secure, certified network connections.

In Conclusion

Disruption of GPS/GNSS/PNT signals and sources is a very real issue. The weak power of GPS/GNSS and its unencrypted signal format leave it vulnerable to jamming and spoofing, and the loss of PNT information can result in catastrophic events that can cripple our critical infrastructure. However, there are many alternative technologies available to augment GPS and provide accurate and reliable PNT information even under adverse conditions, including LEO PNT satellite signals, miniature atomic clocks, and fiber optic network time distribution. Taking preventive measures before an attack occurs can sometimes be the best response. The best strategy to protect critical infrastructure is to use multiple, different PNT sources together. And the earlier the detection, the quicker and more effective the recovery will be.



About the Author



For more than 15 years, John has been part of Orolia, where he works with global navigation satellite systems (GNSS), wireless, positioning navigation and timing (PNT), and specialized systems. Prior to joining Orolia, he specialized in wireless telecom as a founding member of two startups: Aria Wireless in 1990 and Clearwire Technologies in 1997. At Clearwire, he served as Chief Technology

Officer in creating wireless broadband equipment for Internet connectivity. Early in his career, John worked as a systems engineer in radar, EW and command and control systems at Sierra Research and Comptek Research. He holds Masters and Bachelor of Science degrees in electrical engineering and computing engineering from the State University of New York at Buffalo.

About Orolia

With a presence in over 100 countries, Orolia provides virtually failsafe GPS/GNSS and PNT solutions to support military and commercial applications worldwide. Orolia is the world leader in Resilient Positioning, Navigation and Timing (PNT) solutions that improve the reliability, performance and safety of critical, remote or high-risk operations.