Positioning, Navigation and Timing (PNT)

Assured time: The foundational pillar of resilient PNT in the modern battlespace

by Brad Jeisman
Associate Director, Asia Pacific – International Business Development

Collins Aerospace
An RTX Business

Introduction: The centrality of timing in contested environments

Modern military operations, spanning air, land, maritime, and space domains, are fundamentally dependent on a continuous and trustworthy stream of positioning, navigation, and timing (PNT) information. For decades, this assurance has been almost singularly predicated on the Global Positioning System (GPS), which provides P, N, and T as a single, integrated service. This reliance, however, has created a critical vulnerability, a centralised point of failure that adversaries are now actively and skillfully exploiting.

The foundational premise of this analysis is that PNT is, in practice, a misnomer; the true and most critical component is timing. Without a precise and trusted time base, the ability to calculate position collapses, networked systems fall out of synchronisation, and the broader mission tempo fails. The contemporary battlespace demonstrates a clear strategic shift by sophisticated adversaries to target time itself, thereby transforming assured time from a secondary consideration to the central pillar of military operational effectiveness.

The escalating sophistication and proliferation of electronic warfare (EW) and cyber threats have made the vulnerability of a GPS-centric paradigm an operational hazard rather than a theoretical concern. This report will demonstrate that the future of assured PNT (APNT) is not a matter of simply maintaining position and navigation but of building multilayered, fused architectures that can guarantee a trusted time reference, even when external signals are denied or corrupted. The goal is to move beyond a simplistic view of PNT as a unified service and instead focus on the foundational role of time as the metronome that keeps every sensor, weapon system, and decision-maker in sync.

The evolving threat matrix to PNT

The contemporary threat landscape to PNT is multifaceted, encompassing a spectrum of attacks from brute-force radio-frequency (RF) jamming to insidious signal deception and sophisticated cyber intrusions. Peer and near-peer adversaries have demonstrated a high level of proficiency and strategic intent in employing these capabilities to deny, degrade, and deceive an adversary's PNT capabilities.

Jamming: the brute force of denial

Jamming is the most straightforward method of PNT disruption, achieved by overwhelming the weak signals transmitted from Global Navigation Satellite System (GNSS) satellites with high-power RF noise. GPS satellite signals, propagating from over 20,000 kilometers away, are received at extremely low power levels (~–160 dBW). Contemporary adversarial EW systems exploit this inherent vulnerability by generating powerful local radio signals on or near the satellite frequencies, thereby preventing a receiver from acquiring a satellite lock. This brute-force attack results in a complete denial of PNT data and, critically, a loss of the precise time synchronisation essential for modern operations.

One adversary has deployed several well-documented jamming systems. The R-330Zh "Zhitel" is a mobile, truck-mounted system with a documented range of up to 20 kilometers, designed to disrupt GPS and satellite communications in the 100 MHz to 2 GHz range. This system has been used extensively in Ukraine, particularly to interfere with the GPS signals relied upon by uncrewed aerial vehicles (UAVs) and precision-guided munitions. Another advanced system, the Krasukha-4, is a broadband electronic attack platform designed to degrade airborne radars and satellite downlinks. Its use in both Ukraine and Syria demonstrates a layered EW architecture, with Krasukha-4 systems positioned well behind the front lines to complicate long-range airborne sensing. Elsewhere, in the Asia-Pacific, an adversary has deployed truck-mounted and naval jammers, particularly in the South China Sea, to deny PNT access and disrupt coalition platforms.

The effects of this jamming are profound and extend beyond military platforms. The accuracy of precision-guided munitions, such as the Joint Direct Attack Munition (JDAM), is significantly compromised. With GPS, a JDAM can achieve an accuracy of 5 meters, but

under jamming, it must revert to its inertial navigation system (INS), reducing its accuracy to approximately 30 meters. Civilian systems are also heavily affected, as evidenced by widespread navigation disruptions in the Baltic and Black Seas. One adversary's jamming has also inadvertently affected its own forces, a phenomenon known as "electromagnetic fratricide," where high-power jamming signals disrupt their own satellite communications and drone operations. This strategic trade-off suggests that a persistent, widespread jamming campaign is not a viable long-term strategy but rather a sporadic, violent disruptive tactic designed to create temporary windows of vulnerability. The very act of jamming also exposes the location of the jammer, making it a viable target for kinetic counterattacks.

Spoofing: the insidious corruption of data

Spoofing represents a more sophisticated and deceptive threat than jamming. Rather than simply blocking signals, spoofers transmit counterfeit GNSS signals that appear legitimate but carry incorrect data. This manipulation is more dangerous precisely because it can go unnoticed, tricking the receiver into accepting "hazardously misleading information" (HMI). A spoofer can introduce a gradual time offset or falsify a platform's position, causing networked systems to desynchronise without alerting the user.

The operational use of spoofing has been widely documented. Incidents around Shanghai ports in 2019 revealed that spoofing attacks affected hundreds of vessels, causing them to show erratic movements or appear to vanish from tracking systems. In other cases, vessels in the Black Sea have been reported to show their positions hundreds of kilometers inland.

A recent and highly relevant data point is the GPS Spoofing WorkGroup Final Report published in September 2024. The report documents a 500% increase in civil aviation spoofing incidents in mid-2024, with an average of 1,500 flights per day being affected. A survey of nearly 2,000 flight crew members revealed that 70% rated their concern about the safety impact of GPS spoofing as "very high" or "extreme." This shift from denial to deception indicates a maturing adversarial doctrine. While jamming is a blunt instrument whose effects are often obvious, spoofing is an insidious threat that can lead a user to make critical, mission-ending decisions based on false data. The goal is not just to stop an adversary but to deceive them into defeating themselves.

Threat type	Mechanism	Effect on receiver	Detection difficulty	Strategic goal
Jamming	High-power RF signals overwhelm weak satellite signals	Complete signal loss (denial of service)	Often easy; triggers alarms and alerts	To deny access to PNT and time
Spoofing	Transmits counterfeit signals that mimic legitimate ones	Corrupted or falsified PNT data	Harder; receiver may operate normally with incorrect data	To deceive and corrupt operational data
Cyber exploitation	Intrusions alter firmware or ground control segments	Biased or corrupted time data; degraded satellite uploads	Requires specialised cybersecurity monitoring	To compromise systems without RF emissions
Kinetic threats	Anti-satellite (ASAT) weapons or directed energy	Temporary or permanent satellite outages; reduced constellation size	Observable but difficult to counter at scale	To degrade a region's or global PNT/timing infrastructure

Cyber and kinetic vector threats

Beyond RF manipulation, adversaries are also investing in cyber and kinetic capabilities to target PNT. Malicious cyber intrusions can alter the firmware in receivers, introducing a bias in how they interpret time, while attacks on ground control segments could degrade the accuracy of ephemeris and timing uploads to satellites. Network-based timing distribution, such as through NTP or PTP servers, can also be spoofed in cyberspace. This method of attack is more difficult to detect and attribute, as it operates outside the electromagnetic spectrum.

Furthermore, contemporary adversaries have developed and tested anti-satellite (ASAT) weapons and possess directed-energy capabilities designed to temporarily blind or permanently damage GNSS satellites. While a full-scale kinetic attack on a global constellation is a high-stakes proposition, even temporary satellite outages can reduce the number of usable satellites for receivers, making them more vulnerable to jamming and spoofing. This demonstrates a layered strategy where multiple threats are employed in concert to maximise disruptive effect.

Beyond P and N: the strategic vulnerability of timing

While discussions around Assured PNT often focus on the "P" and "N," the reality is that assured time or simply time is the foundation upon which everything else rests. Position and navigation can, in some cases, be substituted or supplemented by other technologies, but timing is a non-negotiable prerequisite for nearly all modern networked warfighting systems.

The foundational role of precise timekeeping

Precise timekeeping is the metronome of the modern battlespace, enabling a wide range of mission-critical applications. Even a millisecond-level timing error can have catastrophic consequences. Networked and encrypted communications, which rely on techniques like frequency hopping and code division, require nanosecond-level synchronisation to function. Without a synchronised clock, secure communications collapse, leading to delays or compromises in the transmission of critical information. Similarly, sensor fusion across crewed and uncrewed platforms, which combines data from multiple disparate sensors, is impossible without a precise time reference to correlate events. Timing is also essential for the synchronisation of fires and ISR, as well as for blue force tracking and coordination.

Military application	Dependency on timing	Consequence of timing failure
Networked communications	High: required for frequency hopping and code division to enable encrypted, anti-jam communications.	Communication collapse; loss of secure data transmission.
Sensor fusion	High: required to correlate data from disparate sensors across multiple platforms.	Unreliable intelligence, surveillance, and reconnaissance (ISR) data; fragmented situational awareness.
Synchronisation of fires and ISR	High: required to coordinate coordinated strikes and intelligence gathering.	Missed targets; unintended collateral damage; loss of operational tempo.
Blue force tracking	Medium: required to provide accurate and real-time location data for friendly forces.	Situational awareness degradation; potential for friendly fire incidents.
Logistics support	Medium: required for time-stamped transactions and supply chain coordination.	Delays in resource delivery; logistical bottlenecks.

The problem of undetected anomalies

A critical vulnerability of the current system is that it is not only susceptible to malicious attack but also to naturally occurring or system-level anomalies. The reliance on a single, centralised source has led to a paradigm where even non-malicious errors can create HMI. The General Lighthouse Authorities of the U.K. and Ireland (GLA) and U.K. Ministry of Defence (MOD) trials demonstrated this by showing that even with prior knowledge, GPS service denial led to numerous alarms and the presentation of erroneous data on bridge displays. The trials noted that typical receivers often do not indicate when their position data is wrong due to interference, and in some cases, reported positions were off by several tens of kilometers.

A more profound systemic flaw is the documented occurrence of GPS and GLONASS signal-in-space (SIS) anomalies that can go undetected by users or even ground monitoring stations. Research from Stanford University reveals that ground-based monitoring networks can be plagued by data-logging errors that obscure genuine signal integrity issues. A notable example is a constellation-wide clock change in the GLONASS system on October 28, 2009, which impacted all satellites. Such an event, while not malicious, can provide the same HMI as a dedicated spoofer. The Royal Academy of Engineering has raised alarms about the Governments over-reliance on a single system and its potential vulnerabilities. These findings powerfully reinforce the argument that a paradigm based on a single, vulnerable PNT source is a critical strategic liability.

The path to resilience: a fused APNT architecture

The era of uncontested, GPS-reliant operations is over. The answer to the modern threat matrix is not a single replacement but a comprehensive, multilayered approach that integrates diverse APNT sources into a single resilient, trusted solution. The guiding principle of this fused architecture is to provide not just data but a confidence metric. A resilient system must declare with certainty its operational accuracy (known validity) and how its accuracy will predictably degrade over time (defined drift) when disconnected from external references. This transforms ambiguity into a predictable parameter for decision-makers, empowering them to act with precision even when the spectrum is being contested.

Components of a fused architecture

A truly resilient APNT solution must draw on a mix of signals and sensors to ensure no single point of failure can compromise the mission. This approach moves beyond simple redundancy to achieve a synergistic outcome where the strengths of one system compensate for the weaknesses of another.

- Modernised M-code GNSS: Modern military GPS receivers, such as those that are M-code capable, are a foundational component. These systems are designed with critical protections against adversarial denial and deception attempts and transmit at higher power to combat terrestrial jamming. The U.S. Army is already fielding systems, such as the Collins Mounted Assured Positioning, Navigation and Timing System (MAPS) Generation II and Dismounted Assured PNT System (DAPS) Generation II, which leverage M-code to enhance resilience.
- Signals of opportunity (SoPs): A key element of a fused system is the use of non-GNSS signals. This includes terrestrial signals from radio beacons, such as the R-mode Baltic, which has proven to be unaffected by GPS jamming. Emerging low-earth orbit (LEO) mega-constellations also offer a promising source of resilient PNT. While primarily for communications, these constellations can provide a resilient alternative to GNSS due to their sheer number of satellites and higher signal power.
- Inertial navigation systems (INS): INS and inertial measurement units (IMUs) are critical for holdover performance. While they are subject to drift over time, they are fundamentally non-jammable and non-decoyable. They provide an independent, uninterrupted reference for short-term operations when external signals are lost, allowing a system to maintain a predictable path.
- Celestial navigation: Acknowledging the possibility of a complete loss of PNT, some navies are considering reintroducing training in celestial navigation. This skill, which uses tools such as the sextant and the System to Estimate Latitude and Longitude Astronomically (STELLA), is non-jammable and globally available, providing a vital backup for a worst-case scenario.

- Other onboard sensors: Beyond dedicated PNT sources, a fused architecture can leverage a platform's existing sensor suite, such as cameras and radar, to provide navigation data through techniques such as visual simultaneous localisation and mapping (SLAM) and radar odometry. This approach ensures that the system is not dependent on a single class of input, further enhancing resilience.

A robust navigation and situational awareness capability relies on the seamless integration of multiple data streams; the Collins Fusion software approach exemplifies this. By combining inputs from diverse sensors and signals, the software creates a cohesive operational picture that mitigates individual system limitations. This fused methodology ensures that information is not only redundant but complementary, enabling more accurate, reliable, and resilient decision-making in complex operational environments.

The role of controlled reception pattern antennas (CRPA)

At the heart of a fused APNT architecture are controlled reception pattern antennas (CRPAs). A CRPA is not a passive component but an active, adaptive electronic warfare system designed to actively defeat jamming and spoofing in real time.

CRPAs use an array of multiple antenna elements and sophisticated digital signal processing to create a dynamic directional reception pattern. This allows the antenna to focus its gain on legitimate satellite signals while simultaneously creating "nulls" to suppress or cancel out interfering signals from jammers or spoofers. The system continuously identifies the angle of arrival of threats and adjusts its pattern to maintain connectivity and signal integrity. This capability provides a hardened, resilient navigation backbone that enables forces to operate with speed, precision and synchronisation, even in the most contested environments.

The design of a CRPA involves a key trade-off between its capabilities and its size, weight and power (SWaP) requirements. The number of antenna elements in the array (typically four to seven) is directly related to the number of simultaneous threats it can neutralise. More elements enable more nulls and offer better protection, but they also increase the complexity, size, and power consumption of the system. Modern CRPAs are increasingly being developed as integrated single enclosures and are tested with advanced software-defined radio (SDR) simulation systems to model complex, dynamic threat environments. This technology is a critical component of fielded systems such as the MAPS Generation II, demonstrating its operational maturity.

PNT source	Primary strength	Primary weakness	Role in a fused system
M-code GNSS	High accuracy, global availability; modern signals are more robust	Vulnerable to powerful EW attacks if not properly protected	Primary reference; baseline for PNT solution
Inertial navigation systems (INS)	Non-jammable, non-decoyable; provides continuous output	Drifts over time; accuracy degrades without external recalibration	Provides critical short-term holdover capability
Terrestrial SoPs (e.g., eLoran)	High signal power; unaffected by GNSS jamming	Limited range; not globally available	Backup for GNSS in regional or urban environments
LEO satellites	Large number of satellites; higher signal power than GNSS	Not a dedicated PNT service; signals may lack optimised ranging codes	Augmentation to improve overall resilience and availability
Celestial navigation	Non-jammable; globally available; no emitted signal	Labor-intensive; dependent on clear weather	Emergency backup skill set for a complete loss of PNT
Onboard sensors (e.g., visual/radar)	Leverages existing equipment; not reliant on external signals	Subject to environmental conditions (dust, fog); limited range	Complements INS for short-term accuracy; provides reference for visual odometry

Conclusion: securing the tempo of future operations

The era of uncontested, GPS-reliant operations is over. The new reality is a contested electromagnetic battlespace where assured time is the most critical and targeted resource. The cat-and-mouse dynamic of EW, coupled with the inherent vulnerabilities of a single PNT source, necessitates a fundamental shift in military doctrine and technology. A traditional approach that focuses solely on improving GPS is insufficient to meet the challenges posed by modern adversaries who have demonstrated the ability to jam, spoof, and otherwise disrupt this critical capability at will.

Collins is at the forefront of this shift, delivering advanced APNT solutions that embrace a multilayered, fused-outcomes approach that combines diverse signals and sensor data.

This architecture, grounded in the principles of known validity and defined drift, empowers commanders to make informed decisions even when traditional PNT is denied. Technologies like CRPA and the strategic integration of alternative sources; including INS, LEO constellations, and even the reemergence of celestial navigation, are not just "nice-to-have" capabilities but are mission-critical enablers. They provide the redundancy and assurance necessary to operate effectively in a degraded environment. The operational advantage of the future will belong to those who can trust their timing and positioning when others cannot. APNT, built on this resilient foundation, is the decisive enabler of mission success in a world where every second and every meter count.

Learn more at
collinsaerospace.com

Collins Aerospace
Four Coliseum Centre
2730 West Tyvola Road
Charlotte, NC 28217
USA

collinsaerospace.com

Connect with us

RTX
RTX_News
RTXCorporation
RTXCorporation
RTXCorporation

RTX.com

Collins Aerospace
An **RTX** Business