THE TIMING GAP

Why GPS-Denied Environments Expose the Hidden Vulnerability in Modern Aerospace and Defense PNT Systems

Executive Summary

For decades, the T (Timing) in Position, Navigation, and Timing (PNT) was effectively a free byproduct of the Global Positioning System (GPS) and other Global Navigation Satellite Systems (GNSS). These include Galileo, BeiDou, the Global Navigation Satellite System (GLONASS), the Quasi-Zenith Satellite System (QZSS), the Navigation with Indian Constellation (NavIC), and the Satellite-Based Augmentation System (SBAS). Systems engineers designed platforms around the assumption that a GNSS receiver would always deliver an accurate, stable timing reference. This assumption is no longer valid.

Global jamming and spoofing activity have increased dramatically. Adversaries continually demonstrate the ability to deny, degrade, and deceive GPS signals at scale. When GNSS signals disappear through jamming, spoofing, or denial, systems that use GNSS timing lose their synchronization reference. Without time synchronization, positioning and navigation fail. Communication links lose coherence, sensor data fusion breaks down, and mission capability degrades or disappears entirely.

This is the timing gap: the growing and dangerous disparity between the Precision Timing that modern defense systems require and the vulnerable, GNSS-dependent timing infrastructure most of those systems rely upon.

This white paper explains why timing has moved from a secondary consideration to a mission-critical requirement. It discusses how the loss of time synchronization cascades across system architectures, and how MEMS-based Precision Timing from SiTime provides the resilience, performance, and size, weight, and power (SWaP) characteristics needed to close the timing gap in aerospace and defense applications.

Timing is the invisible foundation that position and navigation are built upon. Precision local timing is not a future upgrade; it is a crucial design decision that determines whether your platform survives the loss of its external synchronization references.

The Architecture of Assumed Timing

1.1 How GPS Became the Invisible Timing Infrastructure

GPS was designed to solve navigation problems. Embedded within its architecture is one of the most precise, globally synchronized timing systems ever built. Each GPS satellite carries multiple atomic clocks, and the signals broadcast by those satellites deliver sub-microsecond timing accuracy to Earth-based receivers. This capability, effectively free and universally available, was quickly adopted as the de facto timing reference for most defense systems. The NAVSTAR program, initiated by the United States Department of Defense (DOD) in 1973 and declared operational in 1993, established GPS as a foundational capability for synchronized navigation and Precision Timing across military systems.

Communications systems leverage GPS timing to synchronize encrypted waveforms and frequency-hopped links.

Radar and electronic warfare (EW) systems use it to align pulse timing and synchronize sensor networks. Inertial navigation systems implement GPS as a correction reference to bound accumulated drift. Command and control infrastructure integrates GPS to timestamp events and synchronize distributed operations. The list extends through virtually every domain of modern defense.

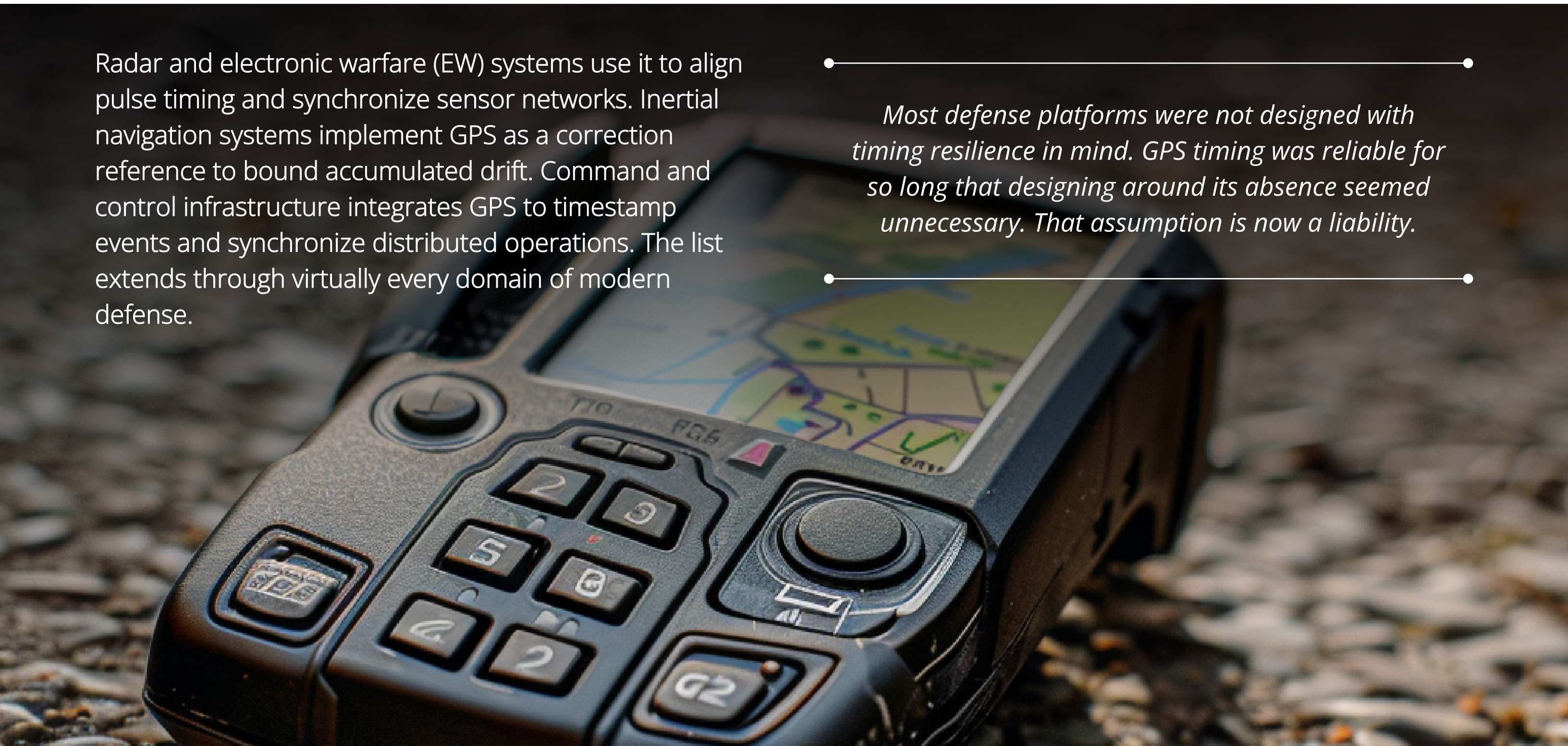
The practical result is that GPS timing is now embedded so deeply and broadly across defense architectures that it ceases to be thought of as a design choice. It is simply invisible, assumed, and taken for granted.

1.2 The Hidden Dependency

The danger of this approach is that timing criticality only becomes apparent when it fails. Most defense systems were not designed with resilient timing capabilities because the question of 'what happens to timing when GPS is unavailable' was rarely asked during the design phase. GPS is so reliable, globally available, and ubiquitous that designing around its potential absence seemed unnecessary and costly.

The result is a generation of defense platforms with a deeply embedded single point of failure at the very foundation of their operation. Remove GPS, and you do not simply remove positioning data. You remove the timing reference that entire systems depend on.

Most defense platforms were not designed with timing resilience in mind. GPS timing was reliable for so long that designing around its absence seemed unnecessary. That assumption is now a liability.



The Threat Environment Has Changed

2.1 Jamming and Spoofing at Scale

GNSS jamming and spoofing are no longer exclusive weapons of nation-states. Low-cost, commercially available hardware has put GNSS deception and denial capability in the hands of anyone willing to use it. The geographic scope of GNSS disruption has expanded significantly in recent years. Incidents of GNSS jamming affecting commercial aviation, maritime navigation, and military platforms have been documented extensively across Eastern Europe, the Middle East, the Baltic region, and the South China Sea. These are not isolated technical anomalies. They represent a deliberate, systematic exploitation of a known vulnerability—and the frequency and sophistication of these attacks are increasing.

2.2 Real-World Operational Impact

The operational consequences of GNSS denial and degradation are no longer theoretical. Military aircraft report loss of navigation accuracy and timing anomalies in contested airspace. Unmanned aerial vehicles (UAVs) operating in GNSS-denied environments experience navigation failures and loss of mission capability. Ground vehicle navigation systems degrade in areas of active GNSS jamming. These incidents highlight a fundamental truth: the threat is present and active today, not on some future battlefield.

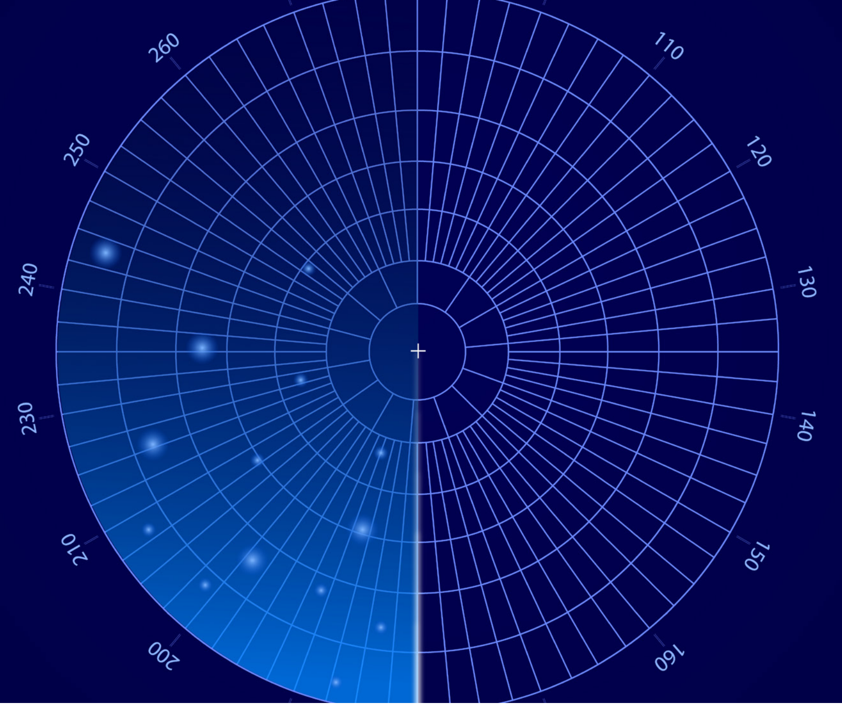
Perhaps more concerning than outright jamming is the growing prevalence of GNSS spoofing. A jammed receiver knows it has lost the signal. A spoofed receiver may continue to operate normally, reporting position and timing data with full confidence while providing corrupted information to the systems that depend on it. In time-sensitive applications, a spoofed timing reference that is off by even a few microseconds can cause cascading failures that are extremely difficult to identify.

2.3 The Policy Response

The U.S. DOD has recognized the severity of GPS vulnerability and has made assured PNT, the ability to maintain reliable position, navigation, and timing capability in GPS-denied and GPS-degraded environments, a priority across the services. Policy direction, acquisition guidance, and program requirements increasingly mandate that new platforms and systems demonstrate PNT resilience. The era of GPS dependency as an acceptable design posture is ending. Programs that do not address timing resilience during design face costly redesigns during fielding, or worse, operational failures in the field.

The United States is not alone in recognizing the severity of GNSS vulnerability. The United Kingdom (UK), Germany, Australia, and the broader European Union (EU) have all launched formal national programs to reduce GNSS dependency and build resilient PNT infrastructure. This reflects a global consensus that reliance on a single satellite-based timing and navigation source is no longer an acceptable posture for any nation's critical systems.

Assured PNT is now a global defense priority. Programs that do not engineer timing resilience into their architecture today are designing vulnerability into platforms that will be fielded for decades. New policies mandate resilience.



Why Timing Is the Most Critical Letter in PNT

3.1 The Synchronization Foundation

To understand why the loss of GNSS timing is so damaging, it is necessary to define the role synchronization plays in modern defense systems. Synchronization is the alignment of system components and distributed platforms to a common time reference. It is the operational backbone upon which coordinated, effective military operations depend.

At the most fundamental level, a modern defense system is a collection of distributed components that must interoperate with precision. Radar systems transmit and receive pulses timed to nanosecond accuracy. Electronic warfare systems synchronize their emissions and reception windows to detect and counter threats. Encrypted communications systems align their waveforms and frequency-hopping sequences to a common clock reference or the link fails. Sensor fusion systems timestamp incoming data to correlate observations from multiple sources.

3.2 The Cascade of Timing Failures

When GNSS timing is lost, the effects do not stop at navigation. They cascade across every system that depends on timing synchronization.

The cascade follows a predictable pattern that plays out across platform types and mission sets:

- Communications links that depend on GNSS timing for waveform synchronization begin to degrade. Frequency-hopped and spread-spectrum waveforms, designed for low probability of intercept in contested environments, are particularly dependent on precise timing synchronization. As timing drifts, these links fail, often when they are most needed.
- Radar and electronic warfare systems that rely on GNSS for pulse synchronization and sensor network alignment lose coherence. Coherent processing gains are degraded or lost. Target detection range decreases. The ability to distinguish targets from clutter degrades. EW systems lose the synchronization needed to effectively employ jamming and deception.
- Inertial navigation systems, which were designed to integrate GPS corrections to bound accumulated drift, begin to drift uncorrected. Navigation accuracy degrades continuously from the moment GPS is lost, at a rate determined by the quality of the inertial sensors and onboard timing reference. Imprecise onboard timing accelerates the drift.

- Data fusion systems that depend on accurate timestamps to correlate sensor observations from distributed nodes begin to produce incorrect fusion results. Targets are mislocated. Tracks are dropped. The common operating picture degrades.
- Distributed systems that rely on a common time reference for coordination including multi-ship formations, air-ground coordination networks, and space-terrestrial links lose the synchronization needed to operate as a coherent, coordinated force.

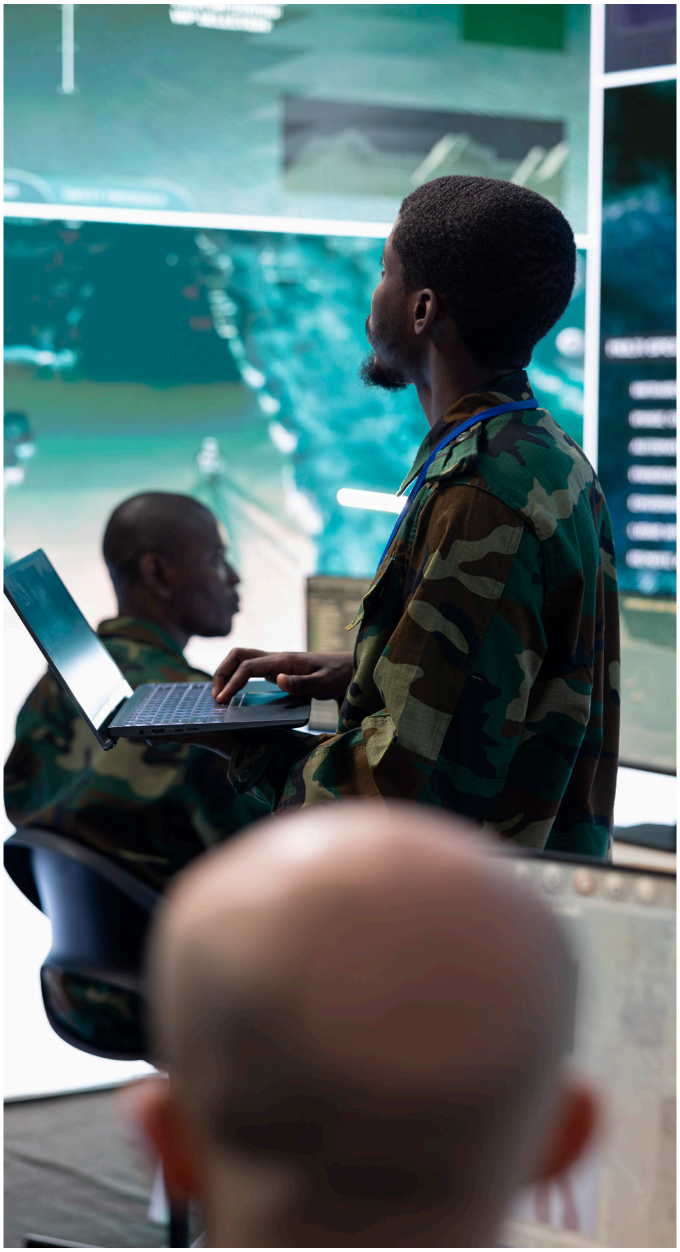
Each of these failures represents a timing failure as much as a navigation failure. Systems that were designed to assume GNSS timing availability have no controlled degradation mode when that assumption is violated. They simply fail.

3.3 Timing Error Translates Directly to Operational Degradation

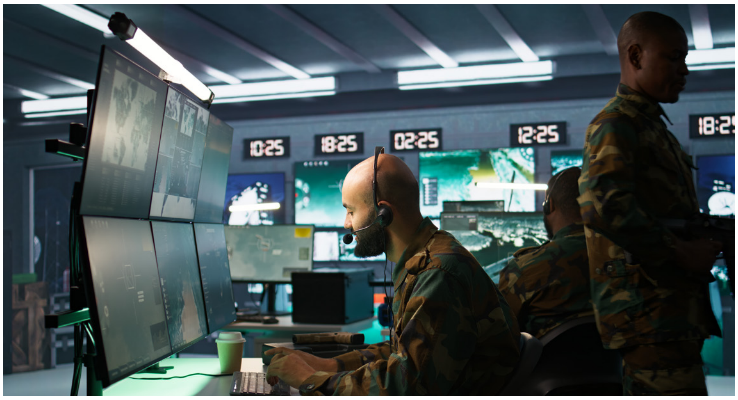
The relationship between timing accuracy and operational performance is not abstract. Every microsecond of timing error has measurable, concrete operational consequences. In navigation, one microsecond of timing error corresponds to approximately 300 meters of range uncertainty in a GPS system. In communications, timing errors of even a few microseconds can cause synchronization failures in waveforms designed for contested environments. In radar, timing errors translate directly to range resolution degradation and false target generation.

These relationships make clear that timing is not a supporting function, it is a primary determinant of operational capability. The precision of the timing reference directly determines the operational effectiveness of every system that depends on it.

Timing precision is not abstract, it has direct, measurable mission impact. Every microsecond of timing error translates to ~300 meters of range uncertainty.



Engineering the Solution: Resilient Onboard Timing



4.1 Holdover: Bridging the Gap

The solution to GPS timing vulnerability is engineering resilient local timing that maintains synchronization through a GNSS outage and bridges the gap until a trusted signal source is reacquired. Or, in fully denied environments, resilient local timing maintains operational capability for the mission profile without external timing references.

The key performance parameter for this capability is holdover which is the ability for a local oscillator to maintain accurate timing after the loss of its reference signal. Holdover performance is determined by a combination of parameters including oscillator frequency stability over temperature, aging or drift, shock and vibration (g-sensitivity), temperature changes, and the quality of the initial frequency calibration at the time of GNSS lock. The longer the outage, the greater the timing error that accumulates.

The quality of the onboard oscillator determines how long the system can maintain acceptable performance before accumulated error becomes operationally significant.

Different applications have different holdover requirements. A communications system can tolerate timing errors up to a millisecond over the course of a day. A precision navigation system often requires timing errors to remain below single microseconds for the duration of a mission (2–72 hours). A precision guided munition may require nanosecond-level timing for only a few minutes.

Understanding holdover requirements at the system architecture level is the first step in engineering timing resilience.

4.2 Why Legacy Quartz Falls Short

Quartz oscillators have served as the timing backbone of aerospace and defense platforms for decades, but their fundamental physical limitations make them increasingly inadequate for the demands of modern contested environments. Four areas of concern stand out for system engineers evaluating quartz for defense applications.

Shock and Vibration Sensitivity

Quartz resonators are inherently susceptible to acceleration forces, exhibiting significant g-sensitivity that causes frequency deviation under profiles typical of tactical aircraft, rotary wing platforms, ground combat vehicles, and munitions. Systems engineers must recognize that datasheet specifications and tests in a controlled environment can bear little resemblance to the timing performance delivered in the field.

Thermal Instability

The rate of frequency change through temperature transitions, known as df/dt, presents a further performance liability. As platforms experience rapid thermal cycling during ascent, descent, or environmental exposure, quartz oscillators struggle to maintain stable frequency output, introducing timing errors when precision is needed the most.

SWaP Incompatibility

The physical size of precision quartz oscillators, particularly temperature controlled and oven-controlled variants (TCXOs and OCXOs), presents a growing challenge as defense platforms trend toward smaller, lighter, and more power efficient architectures. The bulk of these solutions are increasingly incompatible with the SWaP constraints of UAVs, precision guided munitions, dismounted soldier systems, and small satellites.

Supply Chain Vulnerabilities

Quartz crystal production is concentrated in a small number of geographic regions and specialized suppliers, creating single source dependency and geopolitical supply risk that is fundamentally misaligned with the sustainability demands of long duration defense programs. This risk is not theoretical. In October 2020, a fire destroyed the semiconductor factory of Asahi Kasei Microdevices (AKM) in Japan, a manufacturer responsible for over 80% of the ICs used in global quartz TCXO production. The resulting shortage disrupted quartz oscillator supply chains well into 2022, exposing the fragility of a supply base that defense programs had long taken for granted.

4.3 The MEMS Timing Advantage

MEMS-based timing technology, as demonstrated by SiTime's family of oscillators, addresses the fundamental limitations of quartz through a different approach to resonator design and manufacturing. Rather than relying on the piezoelectric properties of a mechanically cut quartz crystal, MEMS timing uses silicon-based micro-electromechanical resonators fabricated through semiconductor manufacturing processes. This results in timing solutions with performance characteristics ideally matched to support the challenges of GNSS-denied and operationally stressed environments.

Superior Vibration Resilience

MEMS-based oscillators exhibit dramatically lower g-sensitivity, as low as 0.004ppb/g which is 3-10x lower compared to quartz oscillators. Where a quartz oscillator may experience significant frequency deviation under vibration, a SiTime MEMS oscillator maintains stable frequency output across the same vibration profile. This is not a marginal improvement. It is a fundamental change in the performance envelope that positions MEMS timing as the preferred solution for airborne, munitions, and vehicle applications where quartz timing cannot deliver the required performance.

Thermal Stability and Compensation

Defense platforms routinely experience temperature ranges far exceeding those of commercial electronics. SiTime's MEMS oscillators incorporate proprietary temperature sensing and compensation architectures that maintain frequency stability across the full military temperature range: –55°C to 125°C. The thermal performance of MEMS timing is not dependent on the physical characteristics of a mechanically cut crystal, making it more consistent, more predictable, and more easily compensated than quartz.

Size, Weight, and Power

Modern defense platforms such as unmanned systems, wearable soldier electronics, small satellites, and precision-guided munitions operate under extreme SWaP constraints. SiTime MEMS oscillators deliver Precision Timing performance in packages that are significantly smaller and more power-efficient compared to equivalent quartz solutions. This SWaP advantage enables Precision Timing to be incorporated into platforms and applications where the size and power requirements of legacy quartz solutions are prohibitive.

Reliability and Supply Chain Resilience

SiTime's MEMS timing products are manufactured using standard semiconductor fabrication processes in established foundries. This manufacturing approach delivers exceptional consistency, quality, and long-term availability, a critical consideration for defense programs. SiTime MEMS oscillators offer a mean time before failure (MTBF) of up to 2 billion hours compared to 30 million hours for quartz. While the difference between 2 billion and 30 million hours of MTBF may appear abstract in isolation, the operational impact becomes clear when modeled at scale. A program fielding 10,000 units per year can expect approximately three quartz oscillator failures annually compared to just 0.04 failures with SiTime MEMS, a difference that translates directly into significantly lower platform downtime, maintenance costs, and mission risk.

MEMS timing offers 3-10x better g-sensitivity than quartz, one of the most important performance parameters for timing resilience in airborne, vehicle, and munitions applications operating in GPS-denied environments. MEMS timing offers >60x better reliability compared to quartz timing.

Building a Resilient PNT Architecture

5.1 Timing as a First-Class Design Requirement

Closing the timing gap requires a fundamental shift in how system engineers approach PNT architecture. Timing must be elevated from a supporting function to a first-class design requirement with its own performance specifications, technology selection criteria, and validation testing.

This requires explicitly specifying holdover performance requirements at the system level. It means testing timing performance under operational vibration and thermal conditions, not just controlled laboratory conditions. It involves selecting timing technology based on mission profile performance, not just datasheet specifications. And it necessitates validating the end-to-end impact of timing degradation on system performance.

5.2 Layered PNT Architecture

Resilient PNT architectures do not rely on a single timing source. They layer multiple timing inputs such as GNSS, alternative low earth orbit (LEO), inertial references, and high-quality local oscillators. These references are typically fused together in a software Kalman filter, allowing the system to dynamically weight each reference and degrade in a controlled manner as external references are lost or degraded while maintaining acceptable performance as long as possible.

In this architecture, a MEMS oscillator functions as the local holdover reference, the timing anchor that maintains synchronization when GNSS and other sources are unavailable. The quality of this holdover reference determines how long the system can maintain acceptable performance in a GNSS-denied environment. A MEMS oscillator with low drift and low g-sensitivity maintains accuracy far longer than a quartz alternative, directly translating to extended operational capability in denied environments.

SiTime's MEMS timing products integrate seamlessly into this layered architecture, providing the holdover performance, environmental resilience, and SWaP characteristics needed to serve as the timing foundation for assured PNT systems.

5.3 Application Considerations Across Platform Types

Different platform types present distinct timing challenges, and the optimal MEMS timing solution varies by application.

Unmanned aerial systems operating in contested airspace require small, low-power oscillators with excellent vibration performance and limited holdover performance. Precision-guided munitions need timing solutions that can survive extreme shock and maintain accuracy through high-g launch environments but do not require long holdover.

Ground combat vehicles require oscillators with wide temperature range performance, resistance to the continuous vibration of vehicle operation, and long holdover supporting longer mission profiles. Naval systems often demand timing solutions that are less SWaP and shock/vibration concerned but require the longest holdover performance. Small satellites necessitate ultra-low SWaP timing with radiation-tolerant characteristics.

SiTime's MEMS timing portfolio spans this range of requirements, with product families optimized for each application, offering lower g-sensitivity, better thermal performance, longer holdover, and more consistent reliability than equivalent quartz solutions in smaller, more power-efficient packages.

Conclusion: Closing the Timing Gap

The timing gap is real, it is present today, and it is growing. The global threat environment has fundamentally changed the assumptions under which defense systems were designed. GPS denial is no longer a contingency to be planned for in the distant future; it is an operational reality that platforms encounter today.

The path to closing the timing gap begins with recognizing that T in PNT is no longer a free byproduct of GNSS. It is a design requirement that must be engineered into every platform operating in a contested electromagnetic environment. It requires specifying holdover performance, selecting timing technology that delivers performance in operational conditions, and validating timing resilience as part of system-level testing.

SiTime's MEMS Precision Timing technology provides the performance, resilience, and SWaP characteristics needed to close the timing gap in the most demanding aerospace and defense applications. With significantly lower g-sensitivity than quartz, superior thermal stability, and a semiconductor manufacturing foundation that delivers consistent quality and supply chain resilience, SiTime MEMS oscillators are engineered for environments where timing matters most and where the consequences of timing failure are unacceptable.

The time to engineer timing resilience is now. Not during the next platform refresh. Not when the program office mandates it. Now, when there is still design margin to do it right.

MEMS timing is not a component upgrade. It is a strategic investment in mission assurance. Platforms that engineer Precision Timing resilience today will maintain operational capability in the GNSS-denied environments of tomorrow.

SiTime®

THE TIMING GAP. Why GPS-Denied Environments Expose the Hidden Vulnerability in Modern Aerospace and Defense PNT Systems

5451 Patrick Henry Drive, Santa Clara, California 95054 • *408.328.4400* • **sitime.com/pnt-timing-solutions**