

Secure Your Time

Leading the World in Resilience with Assured PNT



THE THREAT IS NO LONGER THEORETICAL

GPS, and the wider family of satellite systems known as GNSS, is usually described as a positioning technology. Its most important function is time.

Every mobile network, financial transaction, power grid, data centre, and broadcast system depends on a precise, shared sense of time, delivered continuously to billions of devices by a satellite signal that reaches the Earth fainter than background noise.

Position, Navigation and Timing is often treated as three separate capabilities. In practice, timing is the foundation. Given precise time, a system can still estimate position through inertial or alternative sensors. The reverse is not true: position alone cannot generate precise time.

That foundation is now under attack at scale, and the two methods of attack differ sharply. Jamming overwhelms the signal until receivers lose lock: disruptive, but usually visible, and something well-designed networks can suppress with anti-jam antennas or ride out on high-quality holdover. Spoofing is the greater danger. It does not deny service, it deceives, feeding the receiver a convincing fake so the system keeps running while quietly believing a lie. Attackers often spoof GPS while jamming the other constellations at the same time, so the receiver cannot cross-check and is forced to trust the forgery.

For critical infrastructure, timing spoofing is the most damaging form of all. It pulls a network away from UTC slowly and deliberately, nanoseconds at first, then microseconds, then milliseconds, and by the time the drift is obvious, synchronisation between sites may already be lost. For telecoms operators this is a network resilience problem, not a navigation one: accurate timing underpins 4G and 5G synchronisation, handovers, spectrum efficiency, and backhaul. The network stays connected while service quietly degrades beneath the surface. Alarms may not trigger, traffic keeps flowing, yet the timing reference guiding the whole system can no longer be trusted.

It is Happening on Europe's Doorstep

This is no longer a distant problem. It sits on the edge of NATO airspace and shipping lanes, and it is spreading. Across the Baltic and Nordic region, interference has been near-constant since 2022, with European air traffic authorities now logging thousands of jamming events a year and no sign of the rate easing. Sustained disruption has hit Finland, the Baltic states, northern Poland, and Sweden, concentrated in the eastern Baltic and the Gulf of Finland, while regulators report deliberate spoofing scaling sharply, with suspected transmitters rising more than tenfold inside a single year. The concern is serious enough that, in early 2026, more than a dozen European governments issued a joint warning that the interference now threatens maritime safety and trade.

And it does not stop at the Baltic. Aviation authorities warn that GPS interference now stretches across a widening band of airspace, from the eastern Mediterranean and Black Sea to the Russia and Baltic region, the India and Pakistan border, Iraq and Iran, and the Korean peninsula. Around the Strait of Hormuz, the Red Sea, and the Persian Gulf it has become a routine hazard for shipping and aviation alike. What used to be an occasional nuisance is now a daily operational reality, and the people relying on that signal often have no idea it has been compromised.

From Advice to Obligation

For years, securing timing was treated as good practice. That has changed. Governments and regulators are now telling operators of telecoms networks and critical infrastructure that they are expected to act.

In the United States, Executive Order 13905 set out the responsible use of PNT, requiring that disruption or manipulation of timing has minimal effect on national security, the economy, and critical functions, with federal agencies since publishing formal best practice for resilient PNT across communications, finance, utilities, and transport. In Europe, the NIS2 Directive places resilience obligations on essential operators, increasingly including the integrity of the timing they depend on; Galileo has rolled out signal authentication so users can confirm a signal is genuine, and the European Commission is standing up services to detect and locate interference across the region. In the UK, a national PNT framework sets out resilience guidance for critical infrastructure operators, backed by significant new investment in the National Timing Centre.

The message is consistent. A single satellite signal is no longer an acceptable single point of failure. You are expected to detect interference, prove your timing is genuine, and keep running when the sky goes quiet.

Secure Your Time

The question is no longer whether GNSS will be interfered with. It is what you trust when it is. Resilience starts with verification: timing sources authenticated, cross-checked against independent references, monitored for anomalies, and backed by enough holdover to carry operations through disruption. Alternative terrestrial, geostationary, and low-Earth-orbit sources add further layers of assurance, so that trust in time no longer depends on a single signal arriving from space.

In the modern world, the challenge is no longer obtaining time. It is proving that the time you are receiving is genuine.



HOW VIAVI ASSURES YOUR TIME

VIAVI closes that gap with two ideas that run through everything on the following pages.

TrustedPNT: never trust, always verify. Rather than assume a signal is good, VIAVI systems authenticate, verify and qualify every timing source, then switch seamlessly to one they trust if another is compromised. The attack does not get a vote.

SecureTime: more than one source. Betting everything on GPS is the problem. SecureTime adds independent, harder-to-attack sources on top of standard GNSS:

- **altGNSS LEO**, an encrypted, GNSS-independent signal delivered through Iridium's low-earth-orbit network, accurate to better than 65 nanoseconds of UTC.
- **eGNSS and altGNSS GEO**, authenticated signals delivered from geostationary orbit (powered by Fugro AtomiChron on Inmarsat) with spoofing detection built in and accuracy down to a few nanoseconds.
- **LEO positioning (LOCUS)**, GNSS-independent timing with positioning support for platforms on the move.

Together with strong holdover and terrestrial sources, that means your timing stays trustworthy even when GPS does not.



Stop the Threat at the Antenna

Front-line protection for high-value sites and platforms, before a bad signal ever reaches your receiver.

Smart AJAS-DF Phased Array Antenna

A smart antenna that suppresses jamming and rejects spoofing at the point of entry, and tells you where the threat is coming from. It protects the four key navigation bands (L1, L2, L5 and Iridium) and uses direction finding to show the bearing to a jammer or spoofer, plus true North. A built-in transcoder hands your existing equipment a clean GPS L1 signal, so it drops into legacy systems without a redesign.

Why it matters: it does not just keep PNT alive under attack, it turns your antenna into a sensor that locates the source. Rugged enough for military vehicles and high-value assets, and equally suited to civil sites like airports, power plants, data centers and cell towers.

- Up to 50 dB jammer suppression across four bands
- Direction finding to threats, plus North
- Clean GPS L1 output for plug-and-play upgrade

Assure Timing Across Your Network

The grandmaster and core clocks that keep telecoms and critical infrastructure in sync, built resilient from the ground up.



SecurePNT EdgeGM 7000

A compact, resilient grandmaster clock for the network edge. It draws timing from multiple orbits (standard multi-band GNSS plus the LEO and GEO alternatives) and from terrestrial sources, authenticates each one, and switches seamlessly to a trusted reference. All of it sits in a half-rack unit with high-speed PTP up to 25G.

Why it matters: secure, resilient timing at the edge with no trade-off on speed. When you need to move from 10G to 25G, it is a software license, not a rip-and-replace. Built for 5G and 6G, Open RAN, AI data centers and private 5G.

- Multi-orbit resilient timing (GNSS, LEO and GEO)
- Up to 25G PTP grandmaster and NTP server
- Half-rack form factor, software upgrade path



SecurePNT 6200

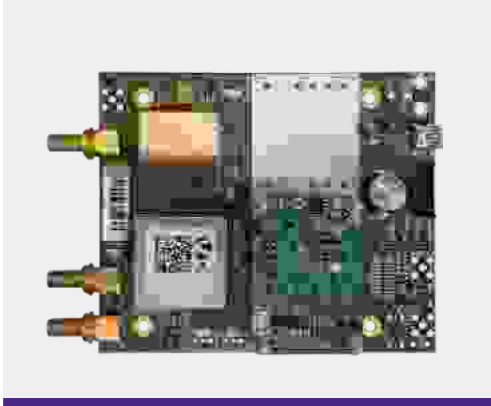
A resilient PNT clock for critical infrastructure, running on a zero-trust, multi-source platform. It blends GNSS with the LEO and GEO alternative sources and strong holdover, and it can also harden a legacy clock by sitting in-line and feeding it a clean, trusted signal.

Why it matters: resilience for sites that cannot tolerate a timing failure, and a way to protect existing clocks at a fraction of the cost of replacing them. Holdover options keep you running even when every signal is gone.

- Zero-trust, multi-source switching
- Built-in retrofit transcoder for legacy clocks
- Rubidium or oven-controlled holdover, meets PRTC-A and NEBS

Resilience Without Replacement

You do not have to tear out equipment that still works. These add modern resilience to the GPS clocks and receivers you already run.



Secure μ PNT-440 Module

An embeddable module that sits between the antenna and a legacy GPS clock and feeds it a clean GPS L1 signal built from trusted alternative sources. The legacy clock carries on as normal, even when GPS is jammed or spoofed.

Why it matters: add resilience to existing kit with no system redesign, in a footprint small enough to embed almost anywhere.

- In-line retrofit between antenna and clock
- Multi-source: GNSS, LEO and GEO
- Precision holdover, fully embeddable



RSR Transcoder 2.0

A rugged unit that takes modern assured PNT inputs (M-Code, SAASM, inertial systems and other signals of opportunity) and converts them into the standard GPS RF that existing receivers already understand. Designed for vehicles, aircraft and portable tactical use.

Why it matters: it bridges the gap between modern secure PNT sources and the huge installed base of legacy GPS receivers, with time transfer better than 5 nanoseconds and support for covert, lights-out operation.

- Converts M-Code, SAASM and inertial inputs to GPS L1/L2 RF
- Tactical and rugged, tested to MIL-STD-810
- Auto-detects common military and commercial receivers

Build Resilience Into Your Own Products

For integrators and OEMs who need assured timing inside their own systems. Frequency standards and receiver modules in small, low-power, embeddable forms.



LN Rubidium GPSDO

A rubidium-backed, GNSS-disciplined frequency standard for the lowest phase noise and the best stability, in a compact, low-power module with strong holdover when GNSS drops.

Why it matters: reference-grade timing where signal purity and holdover matter most, and a clean upgrade for anyone already using VIAVI's chip-scale GPSDO line.

- Ultra-low phase noise and best-in-class stability
- Sub-microsecond holdover
- Under 5.6 W

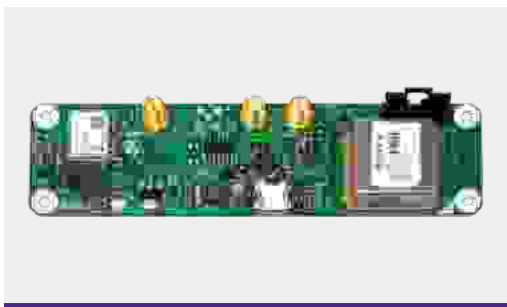


Micro-JLT GNSSDO

A next-generation GNSS-disciplined oscillator built for high volume and low cost, with the best size, weight, power and cost on the market. It is form-and-function compatible with the popular FireFly-IIA.

Why it matters: resilient timing at scale for cost-sensitive designs, with variants ready for high-shock and high-vibration environments.

- Best size, weight, power and cost in its class
- Multi-constellation GNSS
- FireFly-IIA compatible, extended-temperature and low-G variants

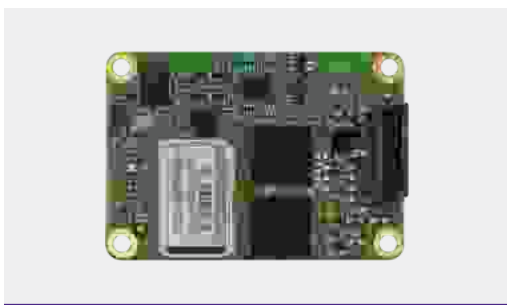


Mini-JLT

A drop-in replacement for the end-of-life Trimble Mini-T GPSDO, with better stability and phase noise and useful extras such as an external 1 PPS input, an on-board accelerometer and USB.

Why it matters: a clean upgrade path for anyone designed around the Mini-T, with no board redesign.

- Form-fit-function Trimble Mini-T replacement
- 72-channel multi-constellation GNSS
- Improved stability and phase noise

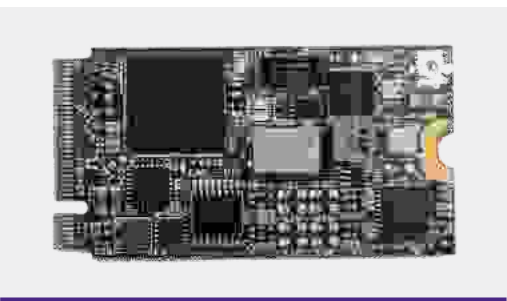


STL-2600 LEO Receiver Module

A receiver module that locks onto Iridium's low-earth-orbit STL signal for GNSS-independent timing, traceable to UTC. A strong fallback for when GPS cannot be trusted.

Why it matters: adds an independent, harder-to-jam timing source to any design.

- Iridium STL low-earth-orbit timing
- Better than 65 nanoseconds to UTC
- Low power



Secure μ PNT STL-1000 LEO Receiver Module

An ultra-small M.2 module that combines GNSS and Iridium STL reception for assured timing in space-constrained designs.

Why it matters: multi-source assured timing in the smallest possible footprint, for embedded and OEM use.

- M.2 form factor
- GNSS plus Iridium STL
- Typically under 1 W

Supporting Components

SecureTime altGNSS GEO-L Helical Antenna

The weatherproof helical antenna that brings the GEO alternative signal into VIAVI's GEO-L products, including the SecurePNT EdgeGM 7000L, the SecurePNT 6200L and the μ PNT GEOL-2600.

- GEO-L band
- IP67, built for outdoor mounting
- Pairs with VIAVI GEO-L products





SECURE YOUR TIME

The threat is here, the regulators are clear, and the fix does not have to mean starting from scratch. Whether you are assuring a national network, protecting a single critical site, or building resilience into your own products, VIAVI has a way in.

Talk to VIAVI about a proof of concept, and find out how trustable your timing is before someone else does.



viavisolutions.com

Contact Us +1 844 GO VIAVI | (+1 844 468 4284)

To reach the VIAVI office nearest you, visit viavisolutions.com/contact

© 2026 VIAVI Solutions Inc.

Product specifications and descriptions in this document are subject to change without notice.

Patented as described at viavisolutions.com/patents

secureyourtime-br-pnt-nse-ae
30195118 900 0626