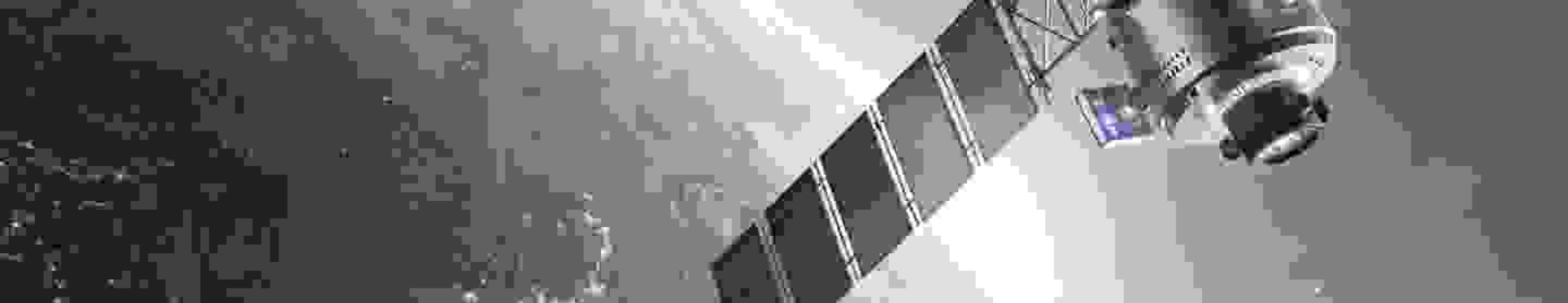


EU NIS2 GNSS Cybersecurity Compliance Solution

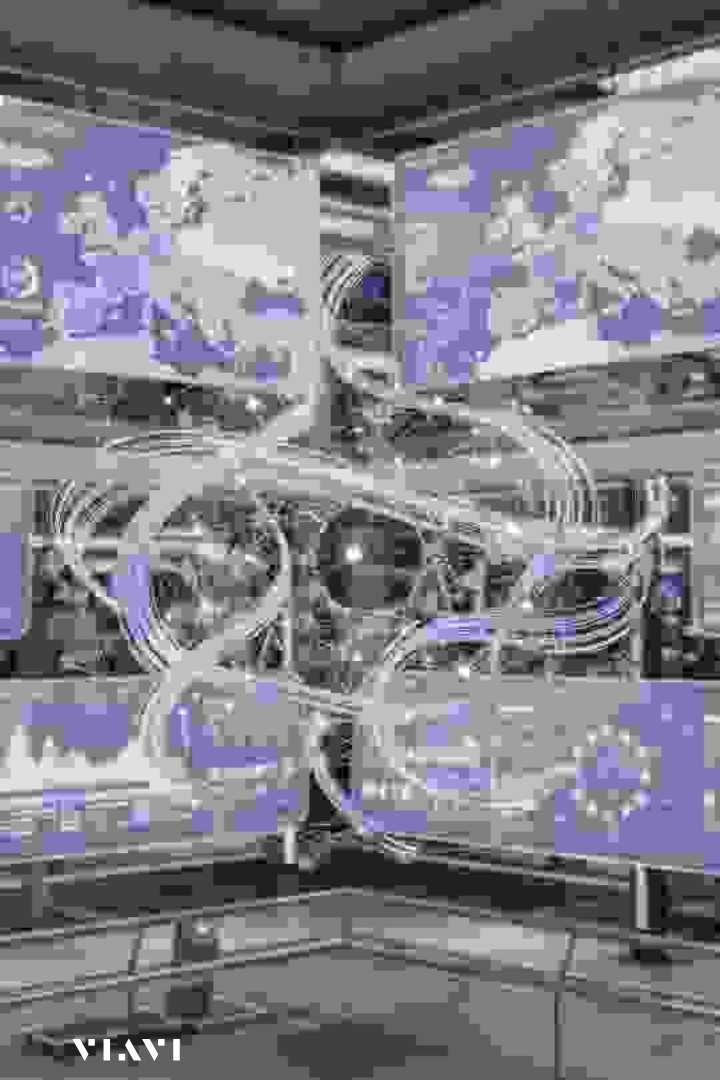
Nino De Falcis

Sr Director, Global PNT Business Development



Strengthening GNSS Resilience Under the EU Directive

Securing Critical Infrastructure Positioning, Navigation & Timing



The EU NIS2 Directive: A New Cybersecurity Era

1

Enforcement Timeline

Effective January 2023, with full transposition by October 2024

2

Expanded Scope

Extends cybersecurity obligations to more sectors, including digital infrastructure and critical services

3

Uniform Standards

Imposes consistent risk management, incident reporting and strict enforcement across EU Member States

4

GNSS Focus

Specifically targets the resilience of essential services, including GNSS-dependent infrastructure



Why GNSS Security Matters More Than Ever



GNSS provides precise timing for critical 5G telecommunications networks



Essential for synchronizing power distribution within energy grids and substations



Guides airports, air traffic controllers, and sea and land transportation systems globally



Critical for accurate timestamping in banking transactions and financial services



Threats like signal jamming cause deliberate interference and disruption



Spoofing attacks inject false signals, leading to erroneous timing data and positioning



Disruptions can trigger cascading failures with catastrophic consequences across interconnected critical infrastructure

NIS2's Impact on GNSS-Dependent Sectors



1

Enhanced Security Controls

Requires robust cybersecurity controls and resilience measures for GNSS data streams to protect against manipulation

2

Verified Data Integrity

Mandates verified, secure GNSS data to prevent manipulation and ensure trustworthiness of timing signals

3

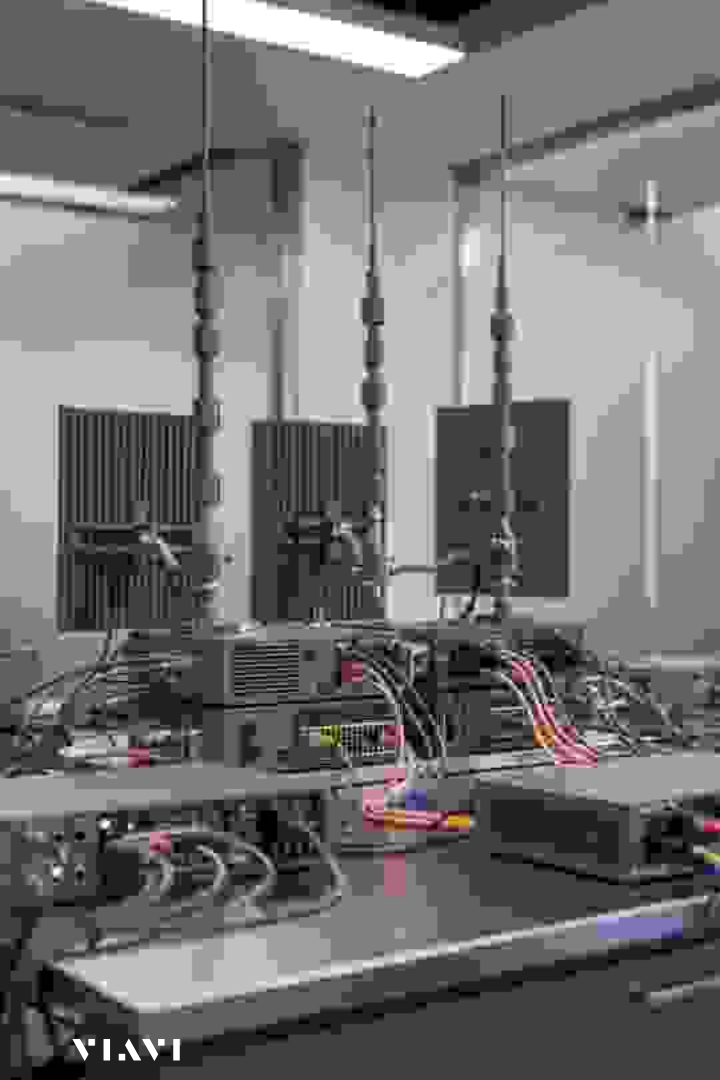
Broader Compliance Scope

Expands requirements to medium and large enterprises in critical sectors, significantly increasing compliance demands

4

Multi-Layered Solutions

Drives adoption of multi-layered, multi-source PNT solutions to meet stringent regulatory standards



The Challenge: Rising Threats to GNSS Integrity



Electronic Warfare Escalation

Increasing electronic warfare and sophisticated cyberattacks targeting GNSS signals worldwide, particularly in conflict zones and near borders



Compounding Risk Factors

Accidental interference from commercial sources and natural disruptions like solar weather events compound existing vulnerabilities



Inadequate Defenses

Traditional GNSS receivers lack robust defenses against sophisticated spoofing and jamming techniques used by adversaries



Regulatory Pressure

Critical infrastructure operators face growing pressure to implement resilient, verified timing and navigation solutions immediately



Introducing VIAVI SecurePNT EdgeGM 7000

1

Industry-Leading Innovation

First Edge Grandmaster Clock with up to 25G PTP capability, setting new standards for high-speed timing

2

Multi-Orbit Resilience

Integrates MEO-GNSS and multi-orbit SecureTime altGNSS GEO/LEO service for resilient, verified and authenticated timing sources

3

Edge-Optimized Design

Compact half 19" 1U rack-mountable unit for critical infrastructure edge deployments with space constraints

EdgeGM 7000 Key Features



Multi-Band & -Constellation GNSS

Multi-band receivers supporting GPS, Galileo, Beidou, QZSS, and NavIC for maximum redundancy

Alternative Multi-Orbit Sources

Activation of GEO (outdoor) or LEO (indoor) reception through an GEO/LEO antenna when the primary GNSS signal is disrupted

High-Speed PTP

Grandmaster and NTP Time Server supporting up to 25G network speeds for modern infrastructure

New Tech Holdover

Low-cost MEMS technology replacing traditional OCXO or Rb oscillators

EdgeGM 7000 Benefits for NIS2 Compliance



Zero-Trust Architecture

TrustedPNT™ continuously authenticates, verifies and qualifies timing sources



Multi-Layered Resilience

Exceeds IEEE P1952 Level 4 standards for PNT resilience



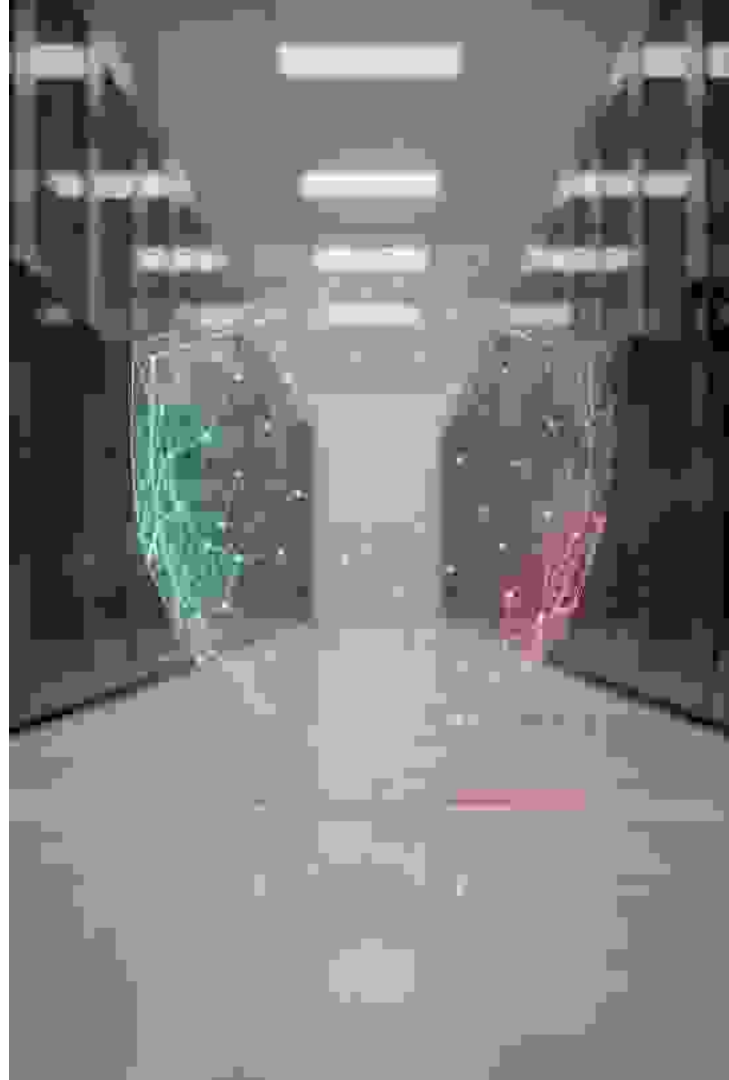
Flexible Platform

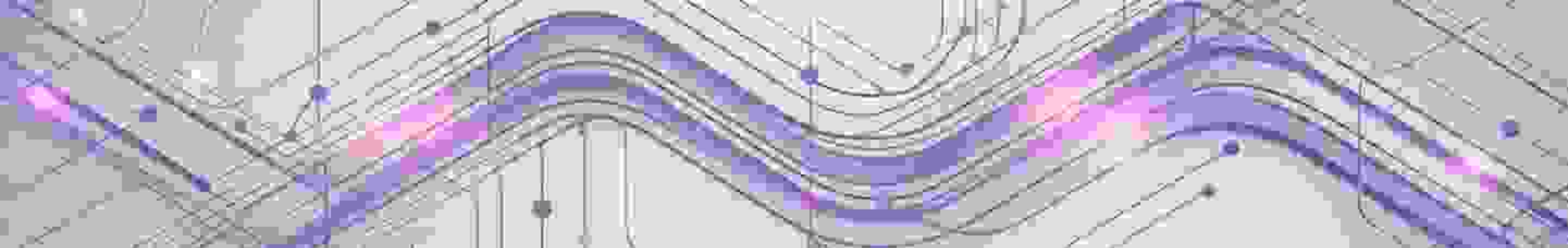
Supports SyncE, NTP, PTP profiles across telecom, enterprise, power and more



Easy Management

User-friendly SNMP and GUI for real-time visibility





Real-World Applications & Impact



Next-Gen Telecom

Secures timing for 5G/6G networks, AI hyperscale data centers, and private 5G deployments requiring microsecond precision



Energy Infrastructure

Protects critical energy grids from GNSS signal denial, spoofing, and cyberattacks that could destabilize power distribution



Transportation & Safety

Supports public safety networks and transportation systems requiring verified, resilient PNT for mission-critical operations



Future-proof platform enables simple software upgrades from 10G to 25G PTP without costly hardware replacement, protecting your investment



Meeting NIS2's Call for Resilient GNSS with VIAVI EdgeGM 7000



Regulatory Imperative

NIS2 raises the stakes for GNSS security and resilience across Europe's critical sectors



Proven Solution

VIAVI EdgeGM 7000 delivers a scalable, multi-orbit, zero-trust PNT solution designed for this new reality



Infrastructure Protection

Empower your infrastructure with trusted, verified timing and navigation to ensure compliance and operational continuity



Contact VIAVI today to future-proof your GNSS resilience and meet NIS2 cybersecurity mandates