

Securing India's Aviation: Resilient GNSS Solution with Latest DGCA Compliance

Nino De Falcis

Sr Director, Global PNT Business Development

December 2025

SecurePNT 6200: Safeguarding India's ATC Operations Against GNSS Threats

How VIAVI's resilient multi-orbit clock enables compliance with DGCA's GPS integrity reporting requirements while protecting critical aviation infrastructure.





The Growing Challenge of GNSS Vulnerability in Indian Airspace

Regulatory Mandate

India's DGCA has issued a critical addendum requiring air traffic controllers to report GPS integrity loss within 10 minutes of detection. This directive responds to increasing spoofing and jamming incidents affecting aviation safety across Indian airspace.

Operational Reality

Recent ADS-B integrity failures near Delhi and other major airports highlight the urgent need for robust detection systems. Controllers must identify, document, and report threats while maintaining uninterrupted operations—a challenge requiring advanced technological solutions.



VIAVI SecurePNT 6200: The Solution



Real-Time Detection

Identifies spoofing and jamming attacks within seconds using multi-orbit validation across GPS, Galileo, GLONASS, BeiDou, and QZSS constellations.



Seamless Integration

Retrofits between existing GNSS antennas and ATC receivers without disrupting current infrastructure or operational workflows.



Continuous Reliability

Maintains timing accuracy during outages with advanced holdover technology, ensuring controllers can safely report incidents per DGCA requirements.

- The SecurePNT 6200 transforms ATC systems into active threat sensors, providing the detection capabilities and reporting precision mandated by India's evolving aviation security framework.

Understanding GNSS Threats to Aviation



Spoofing Attacks

Malicious transmission of false GNSS signals that deceive receivers into calculating incorrect position, navigation, or timing data. These attacks can redirect aircraft or compromise surveillance systems without obvious indicators.



Jamming Incidents

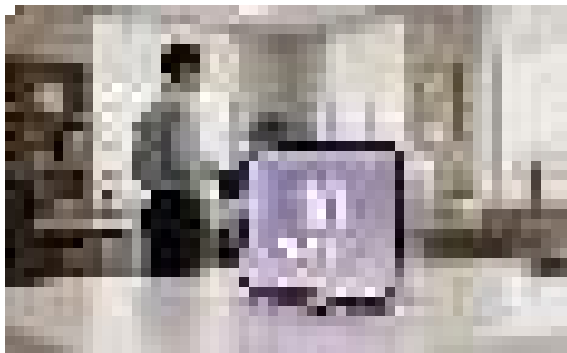
Intentional interference that overwhelms legitimate GNSS signals, causing complete loss of positioning capability. Jammers can affect multiple aircraft simultaneously across wide geographic areas, creating severe safety risks.



ADS-B Integrity Loss

Automatic Dependent Surveillance-Broadcast systems rely on accurate GNSS data. Compromised signals result in false aircraft positions appearing on ATC displays, potentially causing dangerous conflicts or confusion.

DGCA Compliance Requirements



10-Minute Reporting Window

Controllers must detect and report GPS integrity loss within 10 minutes of occurrence to maintain regulatory compliance and enable coordinated response.



Precise Incident Documentation

Reports must include exact time of detection, geographic coordinates, specific interference type, affected systems, and operational impact assessment.



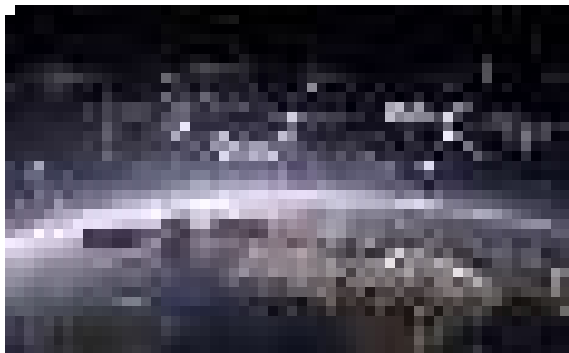
Continuous Monitoring Obligation

ATC facilities require 24/7 capability to identify anomalies, maintain service continuity during incidents, and contribute to national threat intelligence databases.

The DGCA addendum represents India's proactive approach to securing critical aviation infrastructure against evolving electronic warfare threats targeting GNSS systems.

Zero-Trust Multi-Orbit Architecture

The SecurePNT 6200 employs a revolutionary zero-trust framework that assumes no single GNSS source is inherently reliable, continuously validating inputs across multiple independent satellite systems.



MEO - GNSS Constellations

GPS, Galileo, GLONASS, BeiDou, QZSS, and NavIC operate in Medium Earth Orbit, providing global and regional positioning, navigation, and timing services with continuous cross-validation across multiple independent systems.



LEO Satellites

Low Earth Orbit satellite systems providing additional validation layers and enhanced resilience against localized jamming with faster signal refresh rates.



GEO Satellites

Geostationary satellites offering regional augmentation, integrity monitoring, and enhanced accuracy for specific coverage areas with fixed positioning over the equator.

Advanced Signal Validation Technology

Full-Spectrum GNSS Reception

The SecurePNT 6200 integrates full-band receivers covering L1, L2, L3, L5, and L6 frequency bands across all major constellations. This comprehensive coverage enables detection of subtle signal anomalies that single-frequency systems miss.

GEO/LEO Signal Augmentation

Beyond traditional GNSS, the system incorporates geostationary and low-Earth-orbit satellite signals, plus SecureTime altGNSS and eGNSS services for additional validation layers that dramatically increase spoofing detection probability.

Continuous Cross-Validation

Every positioning solution undergoes real-time verification against multiple independent sources. Signal mismatches, timing inconsistencies, or geometric impossibilities trigger immediate alerts before compromised data reaches ATC systems.



Real-Time Threat Detection Capabilities

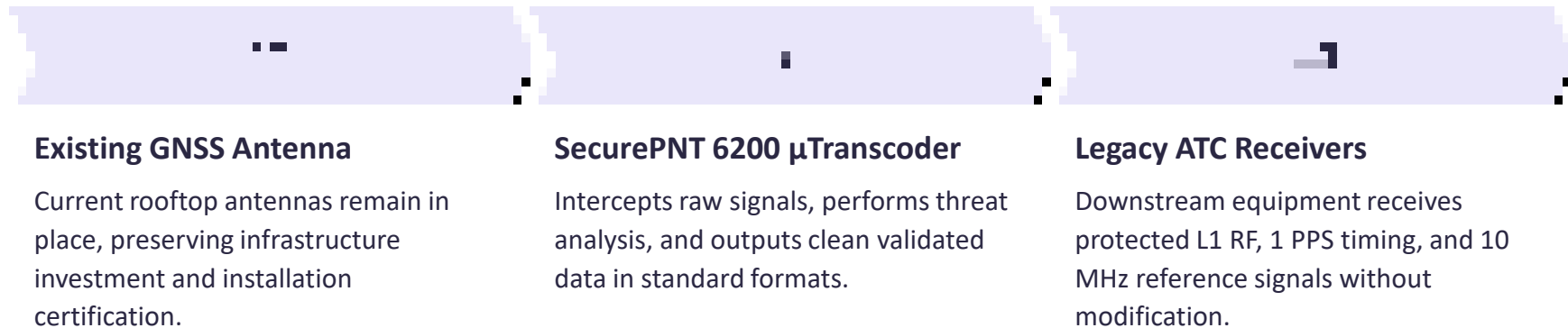
- 1 — Anomaly Detection: <30 Seconds**
Multi-orbit cross-validation identifies spoofed positions or jammed signals through statistical analysis of signal power, timing residuals, and constellation geometry.
- 2 — Threat Classification: <35 Seconds**
Advanced algorithms distinguish between spoofing (false signals) and jamming (interference), characterizing attack sophistication and geographic extent.
- 3 — Alert Generation: <40 Seconds**
System triggers multiple notification channels via status outputs, serial logs, and NMEA messages—well within the 10-minute DGCA reporting requirement.
- 4 — Data Capture: Continuous**
Complete incident documentation including precise timestamps, coordinates, interference characteristics, and affected receiver channels for regulatory compliance.



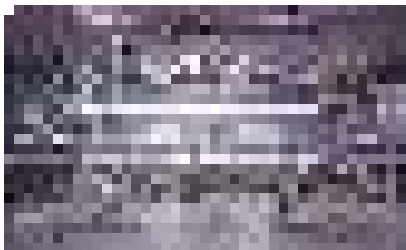


μTranscoder: Seamless ATC Integration

The SecurePNT 6200's μTranscoder technology enables rapid deployment in existing ATC infrastructure without costly system replacements or operational downtime.

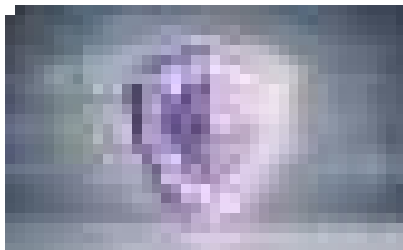


Output Integrity Under Attack



Clean Signal Delivery

Even under active spoofing or jamming, the SecurePNT 6200 outputs validated L1 RF signals, 1 PPS timing, and 10 MHz references. ATC systems get reliable data, preventing operational disruption.



Multi-Layer Authentication

Beyond Galileo's OSNMA, proprietary algorithms enable GPS NMA support for spoofing detection and mitigation. This multi-layered approach flags integrity failures through independent verification paths.



Non-Disruptive Alerting

Integrity warnings transmit without interrupting primary signal outputs. Controllers receive threat notifications while systems remain operational, enabling safe response.



Forensic Data Capture

Detailed logs capture exact interference characteristics—signal mismatch, frequency offsets, power levels—providing evidence for DGCA incident reports and threat actor analysis.



Holdover Technology: Continuity During Outages

<100ns

Peak-to-Peak Accuracy

DOCXO or rubidium oscillator maintains timing precision from GEO/LEO alternative source during complete GNSS denial.

24hrs

Holdover Duration

Extended autonomous operation ensures reporting capability even if all the sources – GNSS and GEO/LEO – are disrupted.

99.999%

UTC/NIST Traceability

Timing outputs remain synchronized to international standards throughout holdover periods.

When GNSS signals are completely denied, internal oscillators bridge the gap—ATC timing networks for surveillance radars, communication systems, and data links continue operating with sub-microsecond accuracy. Controllers can safely observe, document, and report incidents without position or timing errors compromising safety or regulatory compliance.

DGCA Reporting Workflow with SecurePNT 6200



1. Automatic Threat Detection

SecurePNT 6200 identifies GPS integrity loss through multi-orbit validation, triggering immediate alerts to ATC operators via visual indicators and status outputs.



3. Operator Verification

Controllers confirm threat assessment, evaluate operational impact on surveillance and navigation systems, and initiate contingency procedures per standard operating protocols.



2. Data Collection & Analysis

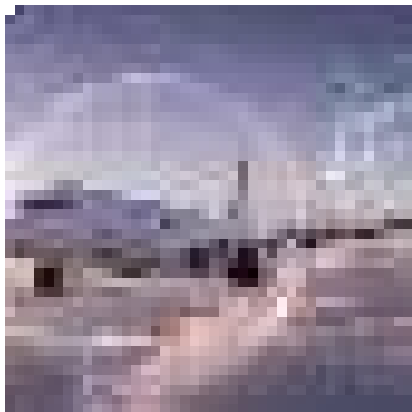
System captures precise incident details: UTC timestamp, geographic coordinates, interference type classification, signal characteristics, and affected receiver channels.



4. DGCA Report Submission

Complete documentation forwarded to Directorate General within 10-minute mandate, including forensic data for national threat intelligence and coordination with adjacent facilities.

Key Benefits for Indian ATC Operations



Enhanced Safety

Prevent compromised GNSS data from affecting aircraft separation, approach procedures, or surveillance accuracy—protecting passengers and crew across Indian airspace.



Regulatory Compliance

Meet DGCA addendum requirements with automated detection and comprehensive reporting capabilities, reducing controller workload while ensuring timely submissions.



Infrastructure Protection

Retrofit existing ATC systems without replacement costs, preserving capital investment while adding state-of-the-art threat detection and mitigation capabilities.



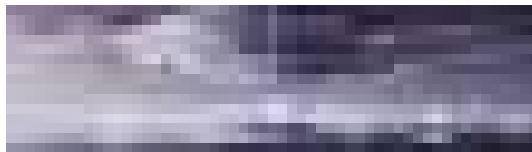
Threat Intelligence

Contribute high-quality incident data to national security databases, enabling coordinated response to evolving GNSS interference threats and electronic warfare tactics.



Securing India's Aviation Future

The VIAVI SecurePNT 6200 transforms regulatory compliance from a reporting burden into an active defense capability—protecting critical aviation infrastructure while meeting DGCA mandates with precision and reliability.



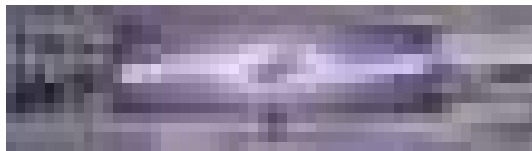
Proven Technology

Multi-orbit validation and zero-trust architecture deployed in mission-critical environments worldwide.



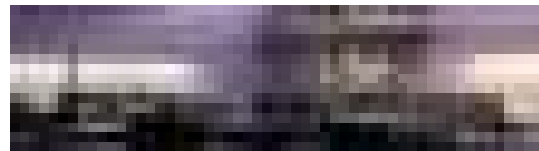
Rapid Deployment

The SecurePNT 6200 integration enables installation in existing facilities without operational disruption or extensive recertification.



Future-Ready

Continuous software updates and constellation support ensure long-term effectiveness against evolving threats to GNSS integrity.



POC Readiness

Available for proof-of-concept trials at Indian ATC facilities, demonstrating real-world threat detection and DGCA reporting capabilities before full deployment.