When Invisible Signals Halted Hundreds of Flights

A Wake-Up Call for Aviation Risk & Resilience

Lessons from the November 2025 disruption at Delhi Airport—and what it means for your operations.

WWW.PISENCE.COM

The Crisis Unfolded

In early November 2025, India's busiest airport experienced a perfect storm of technical failures that grounded operations and affected thousands of travelers.

System Failure

The Automatic Message Switching System (AMSS) experienced a critical failure, forcing air-traffic controllers to revert to manual processing—a dramatic slowdown in capacity.

Signal Interference

Confirmed GPS/GNSS spoofing and signal interference disrupted aircraft navigation systems across the Delhi region, compounding the automation crisis.

Cascading Impact

Over 200 flights delayed (some reports cite 350-400), thousands of passengers stranded, and a ripple effect across airline networks nationwide.

Why This Should Concern Every Aviation Leader

Invisible Infrastructure Is Mission-Critical

This incident exposed a harsh reality: digital messaging networks, satellite navigation, and communication links are just as essential as physical runways and aircraft. When these invisible systems fail, operations halt—even when every tangible asset is functioning perfectly.

The Financial Stakes Are Enormous

Delhi Airport processes over 1,500 movements daily. Each delay cascades through the network, costing airlines, airports, and passengers millions in lost time, fuel, rebooking, and compensation. The business impact of invisible system failure is very real—and very expensive.

Key Insight: Hidden failures in digital infrastructure can cripple operations faster than physical damage—and they're harder to predict and prevent.

Root Causes: Where Resilience Broke Down

Outdated Automation

ATC officials flagged the AMSS as lacking modern redundancy and failover capability—warnings that preceded the breakdown by months.

Electronic Warfare Threats

GPS/GNSS spoofing is an escalating threat in modern aviation, capable of misleading navigation systems and creating dangerous confusion.

No Fallback Resilience

When AMSS failed, manual workarounds drastically reduced throughput. The absence of robust backup systems turned a technical glitch into an operational catastrophe.

Translating Invisible Risk Into Business Impact

For aviation and critical infrastructure sectors, invisible signal failure equals operational gridlock. Traditional risk models often overlook these digital vulnerabilities—but the financial consequences are undeniable.

01

Expand Your Asset Inventory

Quantitative risk assessments must include signal/information systems—messaging networks, navigation data, control protocols—not just physical infrastructure.

02

Calculate True Exposure

Ask: "What's the cost if our messaging network, navigation system, or ATC automation is compromised?" Apply the formula: **SLE = Asset Value × Exposure Factor**

03

Measure Annual Loss Expectancy

Determine how often these failures could occur: **ALE = SLE × Annual Rate of Occurrence**. This transforms abstract cyber risk into concrete financial terms.

04

Justify Control Investment

Frame cybersecurity and signal resilience as business-risk mitigation with measurable ROI—not just IT overhead. Show leadership the numbers that matter.

Turn Invisible Risk Into Measurable Business Insight

At **PiSence Technologies**, we specialize in modeling hidden system failure risk—signaling systems, navigation data, messaging networks, and the digital infrastructure that keeps aviation moving.

We help you answer the critical question: *If this invisible asset fails, what's your Annual Loss Expectancy (ALE)?* And we quantify how much control investment delivers genuine ROI.

Don't wait for your own Delhi moment. Let's make invisible signal risk visible—and actionable.

Visit Pisence.com | **Contact Us**

📞 **90805 75392** | ✉️ **sales@pisence.com**