GNSS-Denied Operations With Cross-Medium Sensing

by Nick Clark | Published April 25, 2026

What GNSS-Denied Operation Requires

GNSS denial is increasingly common in the operating environments where autonomous systems are deploying: defense theaters, urban canyons, indoor environments, GPS-spoofing-attack zones, and the broader category of contested-airspace and contested-spectrum scenarios. The autonomous system must operate under denial, with confidence-appropriate fallback to alternative positioning sources.

Cross-medium sensing produces the diagnostic information that decides what kind of denial is occurring. Multipath in an urban canyon is different from spoofing by an adversary; both produce GNSS anomalies, but the appropriate operational response differs. The current pattern — fall back to inertial dead-reckoning whenever GNSS is anomalous — produces confident-but-wrong positions when the cause is spoofing rather than blockage.

Why Indistinguishable Fallback Is a Structural Failure

When the autonomous system cannot distinguish 'GNSS-blocked' from 'GNSS-spoofed,' its fallback strategy is the same in both cases — typically a switch to inertial dead-reckoning with degraded-confidence position. In the blocked case, this is

appropriate; the system continues operation under degraded confidence until GNSS recovers. In the spoofed case, this is dangerous; the spoofed position before fallback may have already injected incorrect state into the planning horizon.

The architectural answer is to detect the cause of GNSS anomaly through cross-medium correlation. Adjacent-band RF anomalies, unusual propagation patterns, time-anomaly correlation, and other indicators distinguish spoofing from blockage. The system's fallback strategy then differs appropriately — discard recent positions in the spoofed case, maintain them in the blocked case.

How Cross-Medium Sensing Produces Operational Diagnosis

The disruption-modeling primitive consumes contributions from RF spectrum monitors, optical sensors, time-source authentication, and the GNSS receiver itself. Cross-medium correlation against credentialed signatures (the spoofing signature, the blockage signature, the natural-anomaly signature) produces attributed cause.

The attributed cause feeds the autonomy stack's fallback logic. Spoofing attribution triggers position-discard plus inertial fallback plus alert. Blockage attribution triggers inertial fallback without discard. Natural-anomaly attribution triggers continued operation with elevated uncertainty. The architecture supports the operational nuance that current monolithic-fallback patterns cannot.

What This Enables for Assured-PNT Programs

DARPA's STOIC program and similar assured-PNT initiatives are converging on the requirement that PNT systems detect adversarial denial structurally rather than just gracefully degrading under any anomaly. Cross-medium sensing with credentialed signatures provides the architectural foundation that assured-PNT requires.

Commercial deployments operating in increasingly GNSS-contested geographies (urban autonomous delivery, maritime in contested zones, agricultural autonomy in regions with intermittent denial) gain the same architectural capability. The patent positions the primitive at the layer that GNSS-denied autonomy requires as the operating environments where it deploys become structurally less benign.