# Anti-Spoofed Time Observations

by Nick Clark | Published April 25, 2026

## What Anti-Spoofed Time Observations Specifies

Time observation admissibility includes credential validity, offset plausibility against drift models, freshness against the consensus window, and cross-attester consistency. Observations failing any check enter rejection records.

Rejection events are governance-credentialed. The rejection criteria, the rejecting authority, and the rejected observation enter lineage; downstream audit can identify systematic rejection patterns.

## Why It Matters Structurally

GNSS time spoofing has produced operational incidents across critical infrastructure. Single-modality time defenses face structural limitations.

Multi-attester consensus with admissibility evaluation produces structural defense. A successful attack would require coordinated compromise across attesters and admissibility checks; the burden is structural.

## How It Composes With Mesh Operation

Each incoming time observation runs through the admissibility checks before contributing to consensus. Observations passing all checks enter the solver; observations failing checks enter rejection records.

Cross-modality cross-checks operate structurally. When ranging-piggyback time observations disagree with broadcast time observations, the disagreement surfaces as a diagnostic event for further investigation.

## What This Enables for Resilient Timekeeping

Defense operations under sustained time-attack pressure gain consensus that survives the attack. Critical-infrastructure operations gain the same.

The architecture also supports diagnostic differentiation. Spoofing patterns surface as systematic rejection clusters; the audit reconstruction can distinguish spoofing from clock failure or environmental anomaly.