Multi-Source Corroboration

by Nick Clark | Published April 25, 2026

What It Specifies

Each detection event admits in two states: preliminary (single-source) and confirmed (multi-source corroborated). The architecture admits both states; downstream operations admit the appropriate state for their decision class.

Corroboration sources are governance-credentialed. The sources, the corroboration primitives, and the resulting confirmation states all enter lineage; downstream audit verifies the corroboration structurally.

Why It Matters Structurally

Single-source detection produces architectural vulnerability. Compromised or malfunctioning sensors generate false detections; defense operations face structural concerns about adversarial false-flag detection injection.

Multi-source corroboration produces structural defense. False detections require multi-source compromise to confirm; the attacker burden is structural rather than implementation-dependent.

How It Composes With Mesh Operation

The architecture defines the source-credentialing requirements, the corroboration primitives, and the state-transition recording. Implementations apply the architecture; sensing participants contribute corroboration within the framework.

Corroboration composes with other features. Cross-medium corroboration, byzantine-robust corroboration, and graduated-response integration all build on the corroboration primitive.

What This Enables

Defense event-confirmation operations gain structurally-supported corroboration. Civilian critical-infrastructure event confirmation gains the same.

The architecture also supports corroboration evolution. As new sensing sources mature and existing sources are deprecated, corroboration requirements update through governance procedures.