Lineage-Recorded Provenance for Every Actuation

by Nick Clark | Published April 25, 2026

What Lineage-Recorded Provenance Specifies

Each actuation event produces a lineage entry containing: the contemplated action, the composite admissibility computation that gated it (with all credentialed observations that contributed), the selected mode, any harm-minimization deviation with the policy under which it was evaluated, the actual commit, the post-actuation verification result, and the credentialing chain for each element.

The lineage is structurally tamper-evident. The credentialed observations and signatures together produce a reconstruction-grade record that survives challenge. Forensic analysis can walk the lineage to reconstruct exactly what happened, when, under what authority, with what supporting evidence.

Why Process-Level Logging Misses Architectural Provenance

Conventional autonomous-system logging records what happened operationally — sensor readings, planner outputs, actuator commands. The logging supports engineering analysis but doesn't capture the architectural provenance that legal and regulatory reconstruction require: under what credentialing authority was each step taken, with what supporting evidence, against what governance policy.

Architectural provenance is what current systems reconstruct from non-architectural sources (engineering documentation, configuration management, OTA update records). The reconstruction has structural gaps that legal challenge surfaces. Lineage-recorded provenance closes the gap.

How Lineage Composes Across the Architecture

Lineage is uniform across the spatial-mesh architecture. The same lineage primitive that records actuation provenance records observation provenance, policy update provenance, mode-selection provenance, and credential-continuity provenance. Cross-primitive forensic reconstruction operates through the unified lineage rather than through per-primitive log integration.

The lineage propagates through the mesh. A unit's lineage events are credentialed observations consumed by audit authorities through their own admissibility framework. Cross-jurisdictional audit (a state DOT auditing fleet operations in its territory, a federal regulator auditing aviation operations across state lines) operates through credentialed cross-recognition.

What This Enables for Audit and Litigation

Regulatory audit gains structural support. EU AI Act audits, FDA AI/ML SaMD post-market surveillance, NHTSA autonomous-vehicle safety review all benefit from the architectural provenance. The compliance pathway maps directly to architectural primitives.

Legal-grade reconstruction in autonomous-incident litigation gains the same structural support. The court's question — what did the system know, under what rules, at what time — has architecturally-supported answers rather than reconstructed-from-engineering-knowledge answers.