Nick Clark · Published July 30, 2026 · PDF

When an Observation Arrives With No Provenance

At shift change, a safety-assurance engineer at a container terminal has a stopped straddle carrier, a lane with nobody in it, and a log line saying her carrier received an advisory that a person was two rows ahead. What she does not have is any way to say who said it. Her carrier recorded that it acted, not which authority stood behind the input, whether that authority's credential was valid at that moment, or how much weight the input deserved against her own sensors. The advisory expired. The stop is permanent, and so is the gap in her incident file. This article describes governance-chain subject matter disclosed in U.S. Provisional Application No. 64/049,409.

The Tuesday Shift Change

The safety-assurance engineer at a mid-size container terminal comes in at the change of shift, the busiest forty minutes of the day in her yard. Twelve automated straddle carriers are working between the quay crane row and the stack. One of them decelerates hard in the middle of a lane, holds position, and does not resume.

Nobody is in the lane. Her yard cameras show nobody in the lane, and the carrier's own perception stack shows nobody in the lane. What the carrier's log shows is that it received an advisory reporting a person two rows ahead of it, that the advisory entered its planner, and that the resulting motion was a full stop.

By 07:10 she is trying to answer one question, and it is not whether the stop was correct. It is which device produced the advisory. Her yard carries a mixture of sources on the same channel: fixed sensor posts her own maintenance group installed at the blind corners, a gate system operated by the port authority, retrofit tags on the haulage contractor's tractors, and a handheld application some of the stevedores run on their phones. As her deployment is configured today, all four arrive at her carriers' radios in the same shape, and her carriers verify a signature and then treat what passes as input.

The advisory carried a validity duration and it has run out. No copy of the original survives in her yard except the carrier's own transcription of the payload it acted on. She has a timestamp, a claimed position, and a stop. She does not have a sender.

What She Cannot Get Back

Her operating consent obliges her to file a written account of an unplanned automation event, and she cannot write the sentence the account is for. She cannot say whether her carrier obeyed a device her terminal is required to obey, or a phone in a coat pocket that was being cautious, or something that was neither. For her purposes all three produced the same braking profile, and the record she holds cannot separate them.

That gap in her file does not close later. Her carrier's log is a record of effect, not of entitlement. It captured what the carrier did, not what the carrier was evaluating when it did it. There is no re-derivation available to her, because in her setup the thing that would have to be re-derived, the identity and standing of the sender at that instant, was never written down by anything. The window in which she could still have asked the sender directly has closed with the shift.

What she gives up next is operational. Without an attribution she can defend, the safest move available to her is to stop letting that class of input reach her planners at all, which means her carriers at the blind corners fall back to what their own sensors can

see around a stack of steel boxes. She trades the perception she was getting for a certainty she can write down. The moves per hour she loses at that corner are the price of the missing sentence.

And the loss compounds in a specific way. Her file will close with the word unattributed in it, and the next event of the same kind will be indistinguishable from this one, because nothing in her yard changed about how a message carries its origin. She does not get a first incident back to reconstruct once she knows what to look for.

Why Her Zone Stays Derated

The check her carriers run today resolves to yes or no. In her yard a signature verifies or it does not, and what passes is admitted. That answer is the wrong shape for the question she is being asked, because her question is not whether a message was signed but what standing the signer had in her yard at that moment. In her mixture of sources, a verified message from a contractor's retrofit tag and a verified message from the port authority's gate system are the same message, which leaves her a single control: admit the channel or close it.

Were her planners able to rank a sender, she would have intermediate options, and the incident would have been survivable as a written record even if the stop had been identical. As things stand she has no rank to appeal to, so the response she can justify is the blunt one.

Her credentialing has a second shape problem. The access her haulage contractor holds was issued once, at commissioning, and her carriers have no reason to treat a signature differently in the quarter after the contract ends than in the quarter before it. Nothing in her yard binds the standing of a device to a period of time or to a scope, so the strongest statement she can make about any sender is that it was legitimate at some point in the past.

Her fusion node adds a third. It merges tracks from several posts into a single advisory before anything reaches a carrier, and the merged advisory carries no record of which posts fed it or how they were combined. Even in the part of her yard where she does control the hardware, the source detail is consumed by the merge and is not available to her afterward.

Five Properties Described for a Governed Mutation

U.S. Provisional Application No. 64/049,409 discloses, in Section 28.4 and FIG. 28D, a five-property governance chain described, in accordance with an embodiment, as imposed on each governed mutation in the architecture. In that embodiment the five properties are authority-credentialed observation 2803b, evidential weighting in a shared observation store 2803c, composite admissibility evaluation 2803d across cognitive domain fields, governed actuator execution 2803e, and lineage-recorded provenance 2803f, arranged as a sequential chain with recursive closure such that every primitive's output enters the chain and every actuation passes through every primitive's governance.

The disclosure describes the unit of exchange as the governed observation of Section 1.5. In accordance with an embodiment, and as depicted in FIG. 1J, it comprises an authority credential field 109a, a dynamic device hash field 109b encoding identity continuity of the emitting device, a spatial reference field 109c, a temporal reference field 109d, a time-to-live field 109e, a payload field 109f, and a lineage field 109g. The lineage field is described as carrying at least a contributing-device identifier, one or more source-observation references where the observation is derived from other observations, a derivation-function identifier where applicable, and a cryptographic integrity attestation over the foregoing fields. The disclosure describes the credential as carrying hierarchical trust semantics consumed by a cognitive architecture rather than a binary valid-or-invalid attribute consumed by a simple authentication check, and describes the lineage field of one governed observation as composing with the lineage fields of others to produce a cross-device, cross-authority provenance record.

Section 1.4 describes what the credential itself encodes: an issuing-authority identifier, a scope specification of the issuing authority's scope, a temporal-validity specification of the credential's validity period, a device-binding attestation binding the credential to the emitting device, and a cryptographic attestation. Consumption is governed by an authority taxonomy, which the disclosure describes as a governance-configurable hierarchical trust structure defined by a deploying authority for an operational domain. In accordance with an embodiment, each level of the taxonomy specifies a behavioral-response mapping, with the response selected from substrate-condition treatment, mandatory-mutation treatment, high-confidence-observation treatment, advisory-observation treatment, or untrusted-proposal treatment; a mutation-admission specification defining whether an observation at that level is eligible for injection into the consuming unit's planning graph; an evidential-weight specification; and a supersession specification defining whether an observation at that level supersedes conflicting observations from lower levels. Among the example taxonomies the disclosure gives is one for a warehouse or port domain, with levels including a facility-operations authority, a zone-supervisor authority, a shift-lead authority, and an individual-operator authority.

Where authority needs to move, the disclosure describes escalation and de-escalation: an entity at one level may be temporarily elevated under governance-policy-defined escalation conditions, with the escalation credential specifying those conditions, a maximum duration, a geographic or logical scope, and the conditions under which the escalation terminates. In accordance with an embodiment, each escalation event, each de-escalation event, and each operation performed under an escalation is recorded in the lineage of the escalating entity and of each receiving consumer.

Admission is not framed as a gate that opens or shuts. The composite admissibility evaluator of Chapter 4 is described as producing an admission, deferral, rejection, or graduated-mode decision, and the disclosure describes proposed actuations as permitted, gated, deferred, or suspended based on the composite evaluation, with each determination recorded in a lineage field. Evidential weight, per the terminology

chapter, is derived through composite weighting from the contributing device's authority, the sensing modality's reliability at the observed conditions, the observation's consistency with other observations, and the observation's dispositional context. Where an observation is derived from earlier observations, derived-observation lineage is described as retaining forward-and-backward-chaining links to its inputs across any number of derivation steps.

Section 26.7 describes a governance-chain integrity monitoring mechanism comprising an authority credential freshness evaluator producing observations of credential expiration and pre-expiration status, a revocation-propagation completeness evaluator detecting consumers still admitting revoked credentials, a trust-slope anomaly detector producing observations of patterns suggesting compromise or impersonation attempts, a reputation track-record drift monitor, a governance-policy-version consistency evaluator, a Sybil-pattern detector, and a governance-chain-health lineage recorder.

Where the Disclosed Architecture Stops

The taxonomy is governance-policy defined by a deploying authority, which means the architecture would give the engineer a place to put the answer and not the answer itself. Whether her haulage contractor sits above or below her zone supervisors, and what behavioral response each of her levels maps to, would remain her decision and her liability in her terminal.

In her deployment, credential evaluation would speak to standing rather than to correctness. A device in her yard holding a valid credential and honestly reporting a wrong reading would still, on the described mechanism, produce an admissible observation. The disclosed moderations for that case are evidential weighting and inter-source consistency feeding the composite admissibility evaluator, together with the reputation track record of Chapter 28, rather than an assurance that a credentialed reading is a true one.

Nothing described would recover the specific expired advisory from her stopped carrier. The chain is prospective in her situation: it changes what her records contain from the point her deployment adopts it, and her existing incident file would stay as written.

Coverage would remain hers to procure. Were the stevedores' handhelds and the contractor's tags outside her credentialing, the incremental deployment mechanisms of Chapter 27, including bridge devices and the wrapping of existing outputs as governed observations with derived-observation lineage, describe how such sources could be brought in, but adopting them in her yard is a commercial matter rather than an architectural one.

And the graceful degradation of Section 1.8 would not spare her the operational cost she is trying to avoid. Where governance-credentialed coverage falls away, the confidence governor is described as reducing a unit's execution readiness, which for her carriers at the blind corner would still read as fewer moves per hour. What would differ is that the derate would be a recorded consequence of a stated coverage condition rather than a judgment call she cannot document.

Disclosure Scope

This article is a technical description of subject matter disclosed in U.S. Provisional Application No. 64/049,409, titled "Governed Spatial Mesh for Physical-World Perception, Coordination, and Actuation." Mechanism names, outcome words, and reference numerals used above are those of that filing. The scenario and the party described are illustrative and do not depict any actual deployment, operator, or event. Nothing in this article characterizes the scope of any claim, and nothing in it is an admission regarding the state of the art.

Five-Property Governance Chain (/governance-chain)

All 49 steps → (/inventive-steps)

The umbrella primitive: every mutation passes through the same five-property structural test.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

- Five-Property Governance Chain: The Architectural Umbrella (/articles/five-property-governance-chain-the-architectural-umbrella)

SECONDARY TECHNICAL

- Authority-Credentialed Observations (/articles/governance-chain/authority-credentialed-observation)
- Evidential Weighting in Governance Chain (/articles/governance-chain/evidential-weighting)
- Composite Admissibility Evaluation (/articles/governance-chain/composite-admissibility)
- Governed Actuator Execution (/articles/governance-chain/governed-actuator-execution)
- Lineage-Recorded Provenance (/articles/governance-chain/lineage-recorded-provenance)
- Recursive Closure Across Governance Chain (/articles/governance-chain/recursive-closure)
- Hierarchical Governance Composition (/articles/governance-chain/hierarchical-composition)
- Technology-Neutral Governance (/articles/governance-chain/technology-neutrality)
- Structural Distinction Test for the Five-Property Governance Chain (/articles/governance-chain/structural-infringement-test)

APPLICATIONS · GENERAL

- Cross-Domain Governance: One Auditable Authority Chain Across Defense, Cyber, Health, and Finance (/articles/governance-chain/cross-domain-governance-umbrella)
- Multi-Jurisdiction Compliance Without a Single Supervening Authority: A Federated Governance Chain (/articles/governance-chain/federated-governance-umbrella)
- Multi-Jurisdictional Compliance for Cross-Border Data Pipelines: A Governance Chain Umbrella (/articles/governance-chain/multi-jurisdictional-governance-umbrella)
- AI Governance Umbrella Across Regulatory Regimes (/articles/governance-chain/ai-governance-umbrella)
- Climate Governance Umbrella (/articles/governance-chain/climate-governance-umbrella)

- Multi-Tier Supply Chain Provenance: One Governance Substrate for NIST 800-161, CISA SSDF, NDAA 5949, CSDDD, and DSCSA (/articles/governance-chain/supply-chain-governance-umbrella)
- A CCPA and CPRA Compliance Architecture for Verifiable Consumer Rights and ADMT (/articles/governance-chain/ccpa-cpra-privacy)
- EU CSDDD Supply-Chain Due Diligence: A Credentialed Governance-Chain Architecture (/articles/governance-chain/eu-csddd-due-diligence)
- CSRD Audit-Ready Sustainability Reporting: A Governance-Chain Architecture for ESRS Assurance (/articles/governance-chain/eu-csrd-sustainability)
- EU Data Act Compliance for Connected-Product Data: A Credentialed Data-Flow Architecture (/articles/governance-chain/eu-data-act)
- NIS2 Compliance Architecture: How to Meet EU 24-Hour Cyber Incident Reporting (/articles/governance-chain/eu-nis2-cyber)
- FedRAMP High and DoD IL5/IL6: Continuous Compliance Evidence as a System Property (/articles/governance-chain/fedramp-il5-il6)
- A GDPR Article 22 Compliance Architecture for Automated Decision-Making and Profiling (/articles/governance-chain/gdpr-article-22)
- HIPAA Security Rule Compliance for Cross-Organization ePHI Access (/articles/governance-chain/hipaa-security-rule)
- How to Produce Auditable IEEE 7000 Series Conformance Evidence (/articles/governance-chain/ieee-7000-series)
- How to Build an ISO/IEC 42001 AI Management System on a Governance-Chain Substrate (/articles/governance-chain/iso-iec-42001-ai-management)
- ITAR and EAR Export Control Compliance: Per-Access Provenance for Deemed Exports (/articles/governance-chain/itar-ear-export-controls)
- NDAA Section 1709 Compliance Architecture: Runtime China-Origin Controls for DoD Supply Chains (/articles/governance-chain/ndaa-1709-china-controls)
- NIST SP 800-53 Rev 5 Compliance for Autonomous and AI-Mediated Systems (/articles/governance-chain/nist-800-53-controls)
- **When an Observation Arrives With No Provenance (/articles/governance-chain/governance-chain-stakes)**

APPLICATIONS · SPECIFIC

- AWS IAM Cross-Account vs a Governed Cross-Authority Chain (/articles/governance-chain/aws-iam-cross-account)
- Hyperledger Fabric vs Governed Cross-Authority Composition (/articles/governance-chain/hyperledger-fabric)

- Microsoft Entra ID vs Governed Agent Execution: The Governance Chain Alternative (/articles/governance-chain/microsoft-entra-id)
- AWS Verified Permissions vs a Governed Physical-World Actuation Chain (/articles/governance-chain/aws-verified-permissions)
- CyberArk PAM vs Governed Actuator Execution: The Governance-Chain Substrate (/articles/governance-chain/cyberark-pam)
- Okta Alternative: Governed Cross-Authority Identity Beyond a Single Broker (/articles/governance-chain/okta-identity)
- Ping Identity vs Governed Actuation: A Cross-Vendor Governance Chain (/articles/governance-chain/ping-identity)
- SailPoint IGA vs the Governance Chain: Credentialed Identity Mutation (/articles/governance-chain/sailpoint-iga)
- EU eIDAS 2 and the EUDI Wallet vs a Governed Agent-Execution Chain (/articles/governance-chain/eu-eidas-2-eudi-wallet)
- What happens after Microsoft Entra Verified ID verifies a credential? (/articles/governance-chain/microsoft-entra-verified)
- Pollen Mobile vs Governed Coverage Evidence: A DePIN Governance Chain (/articles/governance-chain/pollen-mobile)

HOW-TO GUIDES

- How to Enforce a Complete Governance Chain Across an Autonomous System (/articles/guides/enforce-a-full-governance-chain-autonomous)
- How to Map a Full Governance Chain to GDPR and EU AI Act Obligations (/articles/guides/map-a-governance-chain-to-gdpr-and-eu-ai-act)
- How to Prove Every AI Action Satisfied Identity, Policy, and Audit (/articles/guides/prove-every-ai-action-was-governed)
- How to Prove Regulatory Compliance Across an Entire Fleet of Agents (/articles/guides/prove-compliance-across-an-agent-fleet)

TERMINOLOGY

- dynamic device hash (/glossary#dynamic-device-hash)
- governance chain (/glossary#governance-chain)

Five-Property Governance Chain overview → (/governance-chain)