Nick Clark · Published July 30, 2026 · PDF

When the Fleet Reports Healthy and the Part Is Not

A reliability engineer at a container terminal watches a straddle carrier fail on a hoist actuator her dashboard had reported green for three weeks. The unit had a component replaced during an off-hours road call by an outside service provider. She can describe what broke. She cannot establish, from what her deployment retained, whether the replacement part was authentic, which authority attested it, or whether the degradation she is now looking at began the night it was installed. That window has passed and does not reopen. U.S. Provisional Application No. 64/049,409 discloses a health monitoring primitive in which device state, mesh state, governance-chain integrity, and supply-chain provenance are emitted as governance-credentialed observations and recorded in governance chain lineage.

The 06:40 Alarm on a Unit Her Board Called Green

The reliability engineer for a mid-size container terminal operator gets the call at 06:40 on an ordinary Tuesday, before the morning vessel window opens. Straddle carrier fourteen has dropped a spreader mid-lift. Nobody is hurt. The hoist actuator on that unit has been showing green on her fleet board every shift for three weeks, including the shift that just ended.

She pulls what she has. Her board aggregates telemetry from the carrier vendor's platform, and the vendor's platform reports the actuator within nominal range on every sample it kept. Her maintenance system has one entry for that unit in the relevant window: an off-hours road call nineteen days earlier, performed by a third-party service house her operations group uses when the vendor's own technicians are more than four hours out. The line item says a hydraulic control component was replaced. It does not say which component came off the shelf, who signed for it, or what the technician's authority to touch that unit was that night.

By 09:00 she is expected to say whether the other eleven carriers in her yard are safe to run. What she can actually say is narrower. She can say that the four units that received similar service from the same provider in the same period look green on the same board that called unit fourteen green.

What She Cannot Rebuild Afterward

The spreader is repairable. The shift is a throughput number her operations director will absorb. What does not come back is the record.

For the nineteen days between that road call and the drop, her deployment produced telemetry samples that were attributed to a platform, not to an authority. Nothing in what she retained binds a statement about that actuator's condition to the credential of whoever made the statement, at the moment it was made. She can ask her carrier vendor for logs, and whatever arrives would arrive under whatever retention window that vendor has set for her account. She can call the service house and ask what part they installed, and the answer she gets would reach her now, nineteen days after the fact, from a party with an interest in the answer.

That is the loss, in her terms. The question she has to answer is a question about the past, and the past is where her instrumentation is thinnest. She can improve her monitoring tomorrow. She cannot go back and cause unit fourteen to have emitted, on

the night of the road call, a credentialed statement about which part was seated in it and whose authority admitted that part. The observations her deployment never made under attribution are not observations she can make under attribution now. Every day she runs without that, in her setup, is another day of history she will not be able to reconstruct if a unit fails and someone asks her to.

There is a second edge to it. Because her incident file will not resolve the provenance question, her recommendation at 09:00 has to be conservative for reasons that have nothing to do with the actual condition of the other eleven units. She may stand down carriers that are fine. In her yard, uncertainty spends the same as failure.

Why Another Dashboard Would Not Close Her Gap

The shape of her problem is not resolution. Her board samples the actuator often enough. The shape is that four different things could have been unhealthy about unit fourteen, and her deployment treats them as four unrelated subjects.

One is the device itself: pressure, duty cycle, thermal behavior, the ordinary content of her telemetry. A second is the path that telemetry took, since on her board a sample that never arrived and a sample that arrived nominal look alike once the gap is smoothed. A third is governance: whether the technician's credential was current that night, whether her operator's revocation list had reached the systems that admitted him, whether the policy version his handheld enforced matched the one her terminal believed was in force. A fourth is provenance: whether the component he seated was an authentic part with an intact attestation chain back to a manufacturer, a refurbished part, or a part with no attestation at all.

In her deployment, the device data lives in her carrier vendor's platform, the link data lives with her network group, the credential data lives in a badge system nobody on her staff correlates with equipment records, and the provenance data lives on a paper work

order. Composing them is a manual act she performs after something breaks, and she performs it from whatever survived.

Her cross-authority exposure compounds this. The road call was executed by a party operating under an authority that is not hers. For her purposes, the useful record would have had to be created by that party, at that hour, in a form her terminal could later admit and evaluate on its own terms. Were her service provider's attestations expressible in the same governed form as her own units' observations, the correlation she is doing by hand at 07:30 would be something her deployment had already done at the moment of the swap.

And the timing runs against her. The failure she is investigating is, in her experience with these actuators, the kind that announces itself gradually to anything watching for the shape of the announcement rather than for a threshold crossing. As her fleet board is configured today, it reports the actuator's current value, not the slope of that value against the unit's own service history, and not the composite of that value with the authenticity status of the part producing it.

Health as a Credentialed Observation Bound to Lineage

U.S. Provisional Application No. 64/049,409 discloses, in Chapter 26, a health monitoring primitive presented as an architectural primitive of the governed spatial mesh, directed in an embodiment to the governance-chain-preserving observation, assessment, aggregation, and reporting of the operational health of physical devices, infrastructure agents, the mesh communication substrate, governance-chain integrity, and supply-chain provenance. The disclosure distinguishes this primitive from the capability envelope of Chapter 7, which characterizes what a unit can do given its current state, and describes the health primitive as observing and reporting the internal operational health of devices, infrastructure, and the governance chain themselves.

In the disclosed embodiment the primitive comprises a per-device health-observation generator producing governance-credentialed device-state observations; a per-infrastructure-agent health assessor monitoring cognitive-state integrity, capability-envelope drift, lineage-record integrity, and admissibility-evaluator performance; a mesh communication health monitor producing observations of link quality, packet reconstruction rate, interference, routing topology, and network partition; a governance-chain integrity monitor detecting credential expiration, revocation propagation failure, trust-slope anomalies, reputation drift, and governance-policy-version currency; and a supply-chain provenance integrity monitor attesting device authenticity, firmware integrity, seal status, and authorized-service history.

Section 26.8 describes that supply-chain monitor in more detail. In an embodiment it comprises a device authenticity attestation evaluator producing observations of continuously-valid, expired, revoked, or never-attested authenticity status; a firmware integrity chain monitor tracking firmware updates through the authorized-update-authority chain; a tamper-evident seal monitor producing observations of physical seal status; an authorized-service-provider history recorder producing observations of authorized maintenance, repair, and component-replacement events; a physical-unclonable-function challenge-response monitor producing observations of PUF-response consistency; a manufacturing-provenance chain evaluator verifying the device-to-manufacturer attestation chain per Chapter 24; a software bill of materials attestation verifier; and a supply-chain-health lineage recorder. The disclosure describes downstream applications including tamper-evident custody through continuously-monitored seals, firmware-integrity-gated operation in which devices refuse operation upon detected firmware tampering, and supply-chain verification enabling buyers to validate authenticity of purchased devices through governance-credentialed attestations.

Above the per-unit layer, Section 26.9 describes a fleet health aggregation mechanism producing fleet-wide and infrastructure-wide assessments from per-device and per-agent observations, with a fleet-health computation engine producing indicators

including availability rate, mean-time-between-failures, degradation trends, and cascade-risk indicators, a forecasting-kernel integration per Chapter 5 producing failure-prediction forecasts, and a cascade-propagation integration per Chapter 14 producing health-triggered cascade projections. The same section describes composite health patterns, including a device-plus-supply-chain composite in which device operational health and authenticity attestation combine to indicate trustworthiness, and a cross-agency composite in which multiple authorities' health observations combine through N-party aggregation per Chapter 21.

The filing also describes what happens with the resulting assessments. In an embodiment a fault-localization and diagnostic mechanism identifies root causes of detected health degradation, a predictive-maintenance and end-of-life management mechanism produces governance-credentialed maintenance projections, and a health-driven degradation controller produces graceful-degradation responses including load shedding, derating, and replacement coordination. Reporting is routed to authorized consumers through the observation routing primitive of Chapter 9 with privacy governance per Chapter 10. A health-monitoring lineage recorder records each observation, assessment, aggregation, localization, projection, degradation response, service event, and authority-reporting event in the governance chain lineage field. Consistent with this, FIG. 24B depicts a health monitoring element 2401f forwarding health observations to a component-lineage recorder 2401c.

Health observations are described as feeding other primitives. The filing describes health-weighted admissibility with the confidence-governed execution primitive of Chapter 6, health-derating of capability with Chapter 7, and health-scoped query filtering with the discovery primitive of Chapter 11. Section 6.9 describes a post-actuation verification mechanism that, in an embodiment, emits a governed health-monitoring observation per Chapter 26 upon repeated discrepant verifications, and Section 6.10 describes health-monitoring agents consuming actuation-state observations for per-unit operational-health assessment. The credential rotation

discussion describes a credentialing authority evaluating a device's reputation track record per Chapter 28 and the device's continuous health observations per Chapter 26 before issuing a renewed deployment credential.

Where the Disclosed Architecture Stops for Her

None of this repairs a hoist actuator. The disclosure describes observation, assessment, aggregation, localization, projection, and governed degradation responses; the wrench work in her yard remains hers.

Several things in the filing are described as governance-policy-defined, which means they are configuration decisions in her deployment rather than properties she would inherit. Thresholds, degradation responses, credential rotation intervals, and composite health patterns are all described that way. Where the disclosure conditions an outcome, the outcome follows the declared policy, so what her terminal would see depends on what her authorities declare.

The cross-domain parameterization mechanism is described as adapting health monitoring to deployment-specific authority taxonomies, which for her means the authority taxonomy of her terminal and of her service providers would have to be expressed before cross-authority correlation could do anything for her. A road call performed by a party that emits nothing governed leaves her in a version of the position she is in now.

An authenticity attestation evaluator that reports never-attested status reports a fact. It does not, in her setup, decide her commercial posture toward the provider who installed the part, and the filing does not address the contract remedies she would want next.

Reporting is described as routed to authorized consumers with privacy governance, so what she personally could see would depend on her authority level within her own deployment, and the disclosure does not settle what her operator would grant her.

Disclosure Scope

This article is a technical description of subject matter disclosed in U.S. Provisional Application No. 64/049,409, filed April 25, 2026, and specifically of the health monitoring and continuous verification subject matter disclosed in Chapter 26 of that filing. The scenario is illustrative and does not describe any actual party, deployment, or incident.

Nothing in this article characterizes the scope of any claim, present or future, in that application or in any application claiming priority to it. Descriptions here refer to embodiments as disclosed and are not statements that any feature is required, limiting, or exhaustive. Nothing in this article is an admission regarding the state of the art, and no statement here should be read as characterizing what any other system does or does not do.

Health & Supply Chain Composite (/health-monitoring)

All 49 steps → (/inventive-steps)

Governance-chain integrity unified with supply-chain provenance. Zero-trust device health.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

– Health Monitoring: Unified Governance and Supply-Chain Composite (/articles/health-monitoring-unified-governance-and-supply-chain-composite)

SECONDARY TECHNICAL

- Governance Chain Integrity Monitoring (/articles/health-monitoring/governance-chain-integrity)
- Trust Slope Anomaly Detection (/articles/health-monitoring/trust-slope-anomaly-detection)
- Revocation Propagation Evaluation (/articles/health-monitoring/revocation-propagation-evaluation)
- PUF Challenge-Response Health Verification (/articles/health-monitoring/puf-challenge-response)
- SBOM Attestation for Software Health (/articles/health-monitoring/sbom-attestation)
- Tamper-Evident Seal Monitoring (/articles/health-monitoring/tamper-evident-seal-monitoring)
- Composite Fleet Health Assessment (/articles/health-monitoring/composite-fleet-health)
- Zero-Trust Device Management (/articles/health-monitoring/zero-trust-device-management)
- Regulatory Compliance Integration (/articles/health-monitoring/regulatory-compliance-integration)

APPLICATIONS · GENERAL

- Continuous Device Authenticity and Supply-Chain Provenance for Counterfeit-Part Detection in Semiconductor and Defense Procurement (/articles/health-monitoring/device-authenticity-provenance)
- Defense Fleet Readiness Health Monitoring (/articles/health-monitoring/defense-fleet-readiness)
- Industrial IoT Fleet Health Monitoring for OT Security and Compliance (/articles/health-monitoring/industrial-iot-fleet-monitoring)
- Medical Device Fleet Health Monitoring (/articles/health-monitoring/medical-device-fleet-monitoring)
- Automotive Cybersecurity Compliance Under UN ECE R155 and R156: A Fleet Health Monitoring Substrate for CSMS Evidence (/articles/health-monitoring/automotive-cybersecurity-uneces)
- Continuous Device-Integrity Evidence for CISA-Regulated Critical Infrastructure Fleets (/articles/health-monitoring/critical-infrastructure-fleet-cisa)
- Medical Device Cybersecurity Fleet Management Under FDA 524B (/articles/health-monitoring/medical-device-cybersecurity)
- AAMI TIR57 Compliance for Connected Medical Devices: An Attested Health-Monitoring Substrate (/articles/health-monitoring/aami-tir57-medical-cyber)
- CMMC 2.0 Defense Contractor Cybersecurity Compliance: Device Integrity Evidence for C3PAO Assessment (/articles/health-monitoring/cmmc-2-defense-cyber)
- DO-326A Airworthiness Security Compliance for Aircraft Fleet Cybersecurity (/articles/health-monitoring/do-326a-aviation-cyber)
- IEC 62443 Compliance for Industrial Control Systems: Architectural Device Evidence at Fleet Scale (/articles/health-monitoring/iec-62443-industrial-cyber)

- ISO 13485 Compliance for Connected Medical Device Fleets: Continuous Attestation for Post-Market Surveillance (/articles/health-monitoring/iso-13485-medical-qms)
- Continuous Device Attestation Evidence for NIST CSF 2.0 Compliance Across Device Fleets (/articles/health-monitoring/nist-csf-2-0)
- **When the Fleet Reports Healthy and the Part Is Not (/articles/health-monitoring/health-monitoring-stakes)**

APPLICATIONS · SPECIFIC

- CrowdStrike Falcon vs Governed Fleet Health Monitoring (/articles/health-monitoring/crowdstrike-falcon-fleet)
- Medtronic CareLink Alternative: Governed Cross-OEM Medical-Device Fleet Health (/articles/health-monitoring/medtronic-carelink)
- Microsoft Defender vs Cross-Vendor Governed Fleet Health (/articles/health-monitoring/microsoft-defender-fleet)
- Armis Alternative for Attested Fleet Health: Governed Device Health Monitoring (/articles/health-monitoring/armis-iot-asset)
- Claroty xDome vs Attestable Fleet-Health Device Identity (/articles/health-monitoring/claroty-ot)
- Dragos vs Attested Fleet Health: Device-Side Integrity for OT (/articles/health-monitoring/dragos-industrial)
- Nozomi Networks vs Attestation-Grounded Fleet Health (/articles/health-monitoring/nozomi-networks)
- Tenable OT Security vs Governed Fleet-Health Attestation (/articles/health-monitoring/tenable-iot-ot)
- Governed Device-Integrity Attestation Beyond AVEVA (Schneider) Industrial Software (/articles/health-monitoring/schneider-aveva)

HOW-TO GUIDES

- How to Detect a Counterfeit or Tampered Device in Your Fleet (/articles/guides/detect-counterfeit-or-tampered-devices)
- How to Meet Medical-Device and Automotive Cybersecurity Fleet Rules with Verifiable Device Lineage (/articles/guides/medical-and-automotive-cyber-fleet-compliance)
- How to Monitor the Health and Provenance of a Device Fleet (/articles/guides/monitor-device-fleet-health-and-provenance)

Health & Supply Chain Composite overview → (/health-monitoring)