Nick Clark · Published April 25, 2026 · PDF

Usage-Based Insurance Telematics: A Credentialed, Consent-Gated Operator Risk Profile for Behavior-Based Coverage

Usage-based and behavior-based insurance depends on operator risk signals that are trustworthy, attributable, and respectful of driver privacy, yet today those signals live in siloed carrier clouds with no portable, source-attested, consent-scoped form. This article shows how that gap is closed by the Operator Intent, disclosed in U.S. Provisional Application No. 64/049,409, whose Section 18.12 specifies an operator risk profile as structured intent: per-attribute credentialed contributions from licensing authorities and insurance carriers, compound risk aggregation, privacy-tiered disclosure, and explicit operator consent.

What This Application Specifies

Usage-based insurance (UBI) and behavior-based insurance price coverage on how an operator actually behaves rather than on coarse actuarial proxies. Section 18.12 of the filed specification defines the structured object such programs need but have lacked: an operator risk profile shared as structured intent. It is a representation of an operator's persistent, risk-relevant attributes that supplements moment-to-moment intent signals with persistent context, so that a consuming agent can adjust its projection of how the contributing unit is likely to behave.

The specification enumerates the attribute forms the profile admits. They include an operating-style attribute classifying the operator as aggressive, assertive, defensive, cautious, or distracted; an experience-level attribute classifying the operator as novice, intermediate, or experienced; a violation-history attribute summarizing recent operational violations; an incident-history attribute summarizing recent at-fault and no-fault incidents with a severity profile; a medical-condition attribute, subject to explicit operator consent, indicating condition-relevant operational impact; an operating-context attribute indicating regulated-activity status such as commercial operation, emergency response, or training; and a compound-risk attribute computed by a governance-credentialed risk aggregator from the constituent attributes.

Crucially, each attribute is not free-floating. Section 18.12 specifies a per-attribute credentialing source interface that admits only governance-credentialed contributions from authorized sources, a per-attribute admissibility evaluator applying per-attribute rules, a compound risk aggregator, a privacy-tier enforcer applying the privacy governance of Chapter 10 to each emission, an operator-consent verifier confirming consent at the applicable tier, and a profile-lineage recorder that records every attribute contribution, aggregation, emission, and consumption. The named credentialing-source categories map directly onto the insurance world: licensing authorities supply license-class and violation attributes, and insurance carriers supply risk-classification attributes subject to the insured's consent, alongside fleet operators, governance-credentialed risk aggregator services, and operators themselves through self-declaration.

Why It Matters

The economic premise of behavior-based insurance is that a better risk signal should flow to better pricing and safer roads. The structural problem is that the signal has no agreed form once it leaves the device or the carrier. A score computed inside one carrier's cloud is opaque to everyone else, carries no statement of who attested to it, and

cannot be selectively disclosed. An operator who wants the benefit of a clean record at a new carrier, in a shared fleet, or to a neighboring vehicle has no way to present it that is at once portable, source-attested, and privacy-scoped.

Section 18.12 addresses exactly this. Because every attribute carries its credentialing source's authority credential, a violation-history attribute attested by a licensing authority is distinguishable from a self-declared one, and a consuming party evaluates each attribute against the source's authority and track record. Because disclosure is tiered and consent-gated, the operator controls how much is revealed. And because the privacy governance is, by the specification's own statement, typically more restrictive than for immediate-intent signals precisely because the profile encodes persistent personal attributes, the design treats a driver's risk history as the sensitive personal data it is rather than as exhaust to be harvested.

How It Composes With the Domain

Map the specification's roles onto a UBI program and the fit is direct. A state or national licensing authority acts as the credentialing source for license-class and violation attributes, signing each contribution with its authority credential. An insurance carrier acts as the credentialing source for risk-classification attributes, contributing them only with the insured's consent. A governance-credentialed risk aggregator, the role a UBI analytics provider would occupy, computes the compound-risk attribute from the constituent attributes and attests to it as a distinct, separately credentialed object rather than as an unverifiable black-box number.

Disclosure follows the three governance-policy-configurable tiers the specification names. At the minimal-disclosure tier the profile reveals only an aggregated risk category, which is enough for a counterparty to size its caution without learning anything identifying. At the structured-disclosure tier it reveals selected attributes without personally identifying information. At the full-disclosure tier it reveals the

complete profile with credentialing-source identifiers, and the specification makes this tier available only with explicit operator consent. The operator-consent verifier enforces consent at whatever tier is in play before any emission occurs.

The consuming side closes the loop in the way the specification prescribes for coordination, not pricing. Consuming agents adjust coordination margins and admissibility thresholds based on the admitted risk profile attributes. In the telematics setting, a neighboring vehicle or an infrastructure agent that admits, at minimal disclosure, a higher aggregated risk category can widen its following distance or merge gap accordingly, and the specification requires that those adjustments are themselves lineage-recorded so the decision can be audited downstream. Every step, from a licensing authority's contribution through aggregation, emission, and a consumer's margin adjustment, is captured by the profile-lineage recorder.

What This Enables

Treating the operator risk profile as a credentialed, consent-gated, privacy-tiered object lets several UBI capabilities exist that a siloed score cannot support. Portability becomes possible without surrendering provenance: an operator can present an aggregated risk category to a new carrier or a shared-fleet onboarding process, and the recipient can verify which authority stood behind each underlying attribute. Multi-source underwriting becomes auditable: a licensing authority's violation record and a carrier's claim-derived risk classification coexist in one profile, each separately attested, and the compound-risk aggregator's output is itself a credentialed attestation rather than an opaque figure.

Consent becomes structural rather than contractual. Because the consent verifier and the tier enforcer gate every emission, a driver who consents to share only an aggregated category never has individual attributes leave the device, and the medical-condition attribute is admitted only under explicit consent by the specification's own terms. Fleet and commercial programs gain a clean operating-context attribute that flags regulated-

activity status, letting a commercial operator be coordinated and rated against the right rule set. And the lineage record gives regulators and auditors a reviewable trail for both the risk attestations and the coordination decisions made from them, which is the kind of evidence behavior-based programs are increasingly asked to produce.

Boundary Conditions

The specification defines the structure and governance of the operator risk profile, not the actuarial content. It does not set premiums, prescribe scoring formulas, or fix any risk weighting; the compound-risk aggregator is specified as a governance-credentialed role, and the meaning and calibration of its output remain the province of the carrier or aggregator that operates it. Nothing here supplies benchmark figures, and none should be inferred.

The trust of any profile is bounded by its credentialing sources. An attribute is only as reliable as the authority that attested to it and that authority's track record, and self-declared attributes carry correspondingly less weight than authority-attested ones. The privacy-tier and consent mechanisms are governance-policy-configurable, so the protection an operator actually receives depends on how those policies are set in a given deployment. Finally, the regulatory and licensing framing in this article, including which bodies may act as licensing authorities and what insurance regulation requires, is external domain context; the filing supplies the credentialing-source categories and the disclosure machinery, not jurisdiction-specific rules.

Disclosure Scope

The operator risk profile mechanism described here is disclosed in U.S. Provisional Application No. 64/049,409, specifically at Section 18.12, which specifies the per-attribute credentialing source interface, the per-attribute admissibility evaluator, the compound risk aggregator, the privacy-tier enforcer, the operator-consent verifier, the profile-lineage recorder, the enumerated attribute and credentialing-source categories,

and the minimal, structured, and full disclosure tiers. Insurance carriers and licensing authorities appear in that specification as categories of credentialing source, not as named products. All usage-based insurance, telematics, underwriting, and regulatory framing in this article is external context provided to illustrate a faithful enabling implementation, and it does not expand or limit the scope of the disclosure, which is defined by the application itself.

Operator Intent (/operator-intent)

All 40 steps → (/inventive-steps)

Graduated fidelity tiers. Verification-feedback evolution. Risk versus hostility, separated.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

- Operator Intent: Graduated Fidelity Tiers for Mixed-Fleet Coordination (/articles/operator-intent-graduated-fidelity-tiers-for-mixed-fleet-coordination)

SECONDARY TECHNICAL

- Three-Tier Intent Fidelity (/articles/operator-intent/graduated-fidelity-tiers)
- Tier-Weighted Admissibility (/articles/operator-intent/tier-weighted-admissibility)
- Behavior-Inferred Intent as Governed Observation (/articles/operator-intent/inferred-intent-as-observation)
- Verification-Feedback Inference Function Evolution (/articles/operator-intent/verification-feedback-loop)
- Inference Function Evolution Under Aggregated Feedback (/articles/operator-intent/inference-function-evolution)
- Risk vs Hostility Profile Bifurcation (/articles/operator-intent/risk-vs-hostility-bifurcation)
- Due-Process Credentialing for Adverse Classifications (/articles/operator-intent/due-process-credentialing)
- Cross-Domain Adversarial Inference (/articles/operator-intent/cross-domain-adversarial-inference)
- Protective-Order Integration With Operator-Intent Inference (/articles/operator-intent/protective-order-integration)

- Counter-Action Selection Under Hostility Classification (/articles/operator-intent/counter-action-selection)

APPLICATIONS · GENERAL

- **Usage-Based Insurance Telematics: A Credentialed, Consent-Gated Operator Risk Profile for Behavior-Based Coverage (/articles/operator-intent/usage-based-insurance-telematics)**
- Intent-Bound Aviation Mission Execution (/articles/operator-intent/intent-bound-aviation-mission)
- Intent-Bound Defense Engagement: Structuring Meaningful Human Control Over Autonomous Weapons (/articles/operator-intent/intent-bound-defense-engagement)
- Binding Surgical-Robot Autonomy to Surgeon Intent for Audit-Grade Accountability (/articles/operator-intent/intent-bound-surgical-procedure)
- How to Govern Autonomous Policing Robots: Multi-Authority Intent for De-Escalation Systems (/articles/operator-intent/autonomous-policing-de-escalation)
- Authority Composition for Autonomous Research Platforms and Self-Driving Labs (/articles/operator-intent/autonomous-research-platforms)
- Who Authorizes a Care Robot's Action? Intent-Bound Elder Care and Companion Robotics (/articles/operator-intent/intent-bound-elder-care-robotics)
- Meaningful Human Control for Autonomous Weapons: An Architecture That Makes It Structural (/articles/operator-intent/meaningful-human-control-doctrine)
- Search-and-Rescue Coordinated Intent: Auditable Multi-Operator Command Across Ground, Air, and Autonomous Drone Assets (/articles/operator-intent/search-rescue-coordinated-intent)
- DoD Directive 3000.09 Compliance: Meaningful Human Control Architecture for Autonomous Weapon Systems (/articles/operator-intent/dod-3000-09-autonomous-weapons)
- EASA U-space Compliance Architecture for Drone Airspace Integration (/articles/operator-intent/easa-u-space-airspace)
- FAA UTM Strategic Deconfliction: Credentialed Operator Intent for BVLOS Drone Traffic Management (/articles/operator-intent/faa-utm-uas-traffic-mgmt)
- Meaningful Human Control for Autonomous Weapons: An Architecture for UN CCW LAWS Compliance (/articles/operator-intent/un-ccw-laws-doctrine)

APPLICATIONS · SPECIFIC

- Anduril Mission Control Lacks Architectural Intent Substrate (/articles/operator-intent/anduril-mission-control)
- Northrop ABMS Lacks Cross-Authority Intent Composition (/articles/operator-intent/northrop-abms)
- Shield AI Hivemind Lacks Operator-Intent Substrate (/articles/operator-intent/shield-ai-hivemind)

- Helsing Defense AI Lacks Operator-Intent Substrate (/articles/operator-intent/helsing-defense-ai)
- Milrem Robotics THeMIS Lacks Operator-Intent Substrate (/articles/operator-intent/milrem-robotics)
- Palantir Foundry Mission Architecture Lacks Operator-Intent Substrate (/articles/operator-intent/palantir-foundry-mission)
- Saildrone Maritime ISR Lacks Operator-Intent Substrate (/articles/operator-intent/saildrone-maritime-isr)
- Skydio Defense Lacks Operator-Intent Substrate (/articles/operator-intent/skydio-defense)
- 1X Technologies NEO Humanoid (/articles/operator-intent/1x-humanoid)
- AeroVironment Switchblade and Defense Drones (/articles/operator-intent/aerovironment-switchblade)
- AgEagle Aerial Systems Defense Drones (/articles/operator-intent/ageagle-defense)
- Anduril Bolt and Lattice-Connected Drones (/articles/operator-intent/anduril-bolt-drones)
- Autel Robotics EVO Series (/articles/operator-intent/autel-evo-defense)
- DJI Enterprise Drones (Mavic, Matrice, M30) (/articles/operator-intent/dji-enterprise)
- Figure Humanoid Robotics (/articles/operator-intent/figure-humanoid)
- Parrot Anafi Defense Drones (/articles/operator-intent/parrot-anafi-defense)
- Tesla Optimus Humanoid Robotics (/articles/operator-intent/tesla-optimus)
- Agility Robotics Digit Humanoid (/articles/operator-intent/agility-robotics-digit)
- Apptronik Apollo Humanoid (/articles/operator-intent/apptronik-apollo)
- Brinc Public Safety Drones (/articles/operator-intent/brinc-public-safety-drones)
- Sanctuary AI Phoenix Humanoid (/articles/operator-intent/sanctuary-ai-phoenix)
- Saronic Autonomous Surface Vessels (/articles/operator-intent/saronic-autonomous-maritime)
- Unitree H1 Humanoid and Go2 Quadruped (/articles/operator-intent/unitree-humanoid-quadruped)
- Vatn Systems Autonomous Undersea Vehicles (/articles/operator-intent/vatn-systems-undersea)

Operator Intent overview → (/operator-intent)