The Insurance Imperative

How Conformance Evidence Enables Autonomous System Coverage

February 2026 — Public Document

The Insurance Imperative Why Autonomous System Underwriting Requires Independent Conformance Data Executive Summary Insurers cannot price autonomous system risk because no independent mechanism exists to verify that these systems operate within their declared boundaries. Without standardized conformance data, the insurance industry faces a choice between pricing blind and refusing to underwrite—neither of which serves the market.

The global AI insurance market is projected to grow from $14.99 billion in 2025 to $246.3 billion by 2035, with underwriting representing the single largest AI use-case segment. Yet insurers face a structural paradox: the systems they are being asked to underwrite are the same systems whose performance data they cannot independently verify. Every autonomous system underwriting decision made today relies on manufacturer-disclosed data with no standardized format, no independent verification, and no mechanism to detect omissions.

This white paper provides a comprehensive analysis of the underwriting gap, drawing on recent case law, reinsurance research, regulatory developments across multiple jurisdictions, and actuarial methodology to demonstrate why independent conformance data is not merely useful for autonomous system underwriting—it is structurally necessary. It then presents Operational Design Domain Conformance (ODDC) as the certification infrastructure that provides the actuarial-grade evidence insurers need.

1. The Underwriting Blind Spot

Insurance underwriting depends on a fundamental capability: the ability to independently assess the risk being transferred. For over a century, insurers have built sophisticated methodologies for evaluating property risk (building inspections, fire ratings), health risk (medical examinations, actuarial tables), and driver risk (driving records, telematics). Each of these methodologies shares a common feature: the data used to price risk comes from sources independent of the party seeking coverage.

Autonomous systems break this model. When an insurer underwrites a fleet of autonomous vehicles, an industrial robot installation, or an AI-powered medical device, the performance data available to the underwriter comes almost entirely from the manufacturer or operator. There is no independent inspection mechanism. There is no standardized reporting format. There is no third-party verification of the operational boundaries the system claims to respect.

EY projects that auto premiums could decline by 30–50% in the coming decades as autonomous vehicles reduce accidents. But this projection assumes that reliable, independent performance data will exist to support actuarial pricing. Swiss Re has explicitly acknowledged that the lack of claims data will make alternative risk assessment methodologies a must-have for autonomous vehicle insurance. The question is not whether this data gap will be filled, but whether insurers will lead the solution or be disrupted by it.

1.1 The Scale of the Liability Shift

The liability landscape for autonomous systems is shifting faster than underwriting models can adapt.

Multiple landmark cases in 2024–2025 have established precedents that directly affect how insurers must evaluate autonomous system risk:

The Tesla Autopilot Verdict (Florida, 2025) A Florida jury awarded $243 million to the family of a man killed when his Tesla, operating in Autopilot mode, failed to avoid a truck. The jury found Tesla 33% liable, holding that the company had overstated the system's safety capabilities and failed to install adequate safety checks. This verdict established that manufacturers can be held partially liable for accidents involving partially autonomous systems, even when the human driver bears majority responsibility. For insurers, this means product liability exposure now overlaps with traditional auto liability in ways that existing models do not capture.

The Cruise Robotaxi Shutdown (San Francisco, 2023) A Cruise robotaxi dragged a pedestrian approximately 20 feet after the pedestrian was initially struck by a human-driven vehicle and fell into the robotaxi's path. General Motors' Cruise unit recalled nearly 1,000 vehicles and suspended all operations. The incident demonstrated that a single autonomous system failure can trigger fleet-wide operational shutdown—a correlation risk that traditional auto insurance does not model. When one vehicle's software fails, every vehicle running that software carries the same defect.

The Waymo School Bus Recalls (2025) In May 2025, Waymo recalled 1,212 robotaxis after NHTSA identified a software flaw causing collisions with stationary objects like chains, gates, and utility poles—obstacles a human driver would easily avoid. Then in December 2025, Waymo recalled 3,067 vehicles after its robotaxis were documented illegally passing stopped school buses in Austin and Atlanta. The Austin Independent School District recorded 20 separate incidents of Waymo vehicles passing buses while children were loading and unloading—including one incident where a student was still in the road. Five of these incidents occurred after Waymo claimed it had already deployed software fixes.

These recalls illustrate a critical underwriting challenge: autonomous system failures are not random mechanical events. They are systematic software defects that affect entire fleets simultaneously.

Traditional actuarial models, built on the assumption that individual vehicle risk is largely independent, cannot capture this correlated risk without new data sources.

1.2 The Data Gap in Numbers

NHTSA reported that vehicles equipped with automated driving systems were involved in nearly 400 crashes over a single year of reporting. Tesla vehicles with Advanced Driver Assistance Systems accounted for 53.9% of all reported incidents. Waymo vehicles accounted for the highest share among fully autonomous systems. But these figures come from manufacturer self-reporting under NHTSA's Standing General Order, which requires reporting only when certain criteria are met and relies entirely on manufacturer classification of incidents.

The inadequacy of this data for actuarial purposes is demonstrated by the Waymo–Swiss Re collaboration itself. Swiss Re's study analyzed liability claims from 25.3 million fully autonomous miles, comparing them against baselines derived from over 500,000 claims and 200 billion miles of human driving exposure. The study found an 88% reduction in property damage claims and 92% reduction in bodily injury claims for Waymo vehicles. Apollo ibott, a Lloyd's of London Syndicate, described the results as providing a staggering benchmark of 90% lower claims frequency compared to human driving.

But this study, groundbreaking as it is, illustrates the problem: it was produced through a bilateral partnership between one manufacturer and one reinsurer. The data is not standardized. The methodology is not replicable across manufacturers. There is no independent verification that the miles reported are complete, that incident classification is consistent, or that the operational conditions match the baselines. Swiss Re's own researchers have acknowledged that autonomous vehicles come with inherent and complex risks and that the lack of claims data necessitates entirely new risk assessment approaches.

2. The Actuarial Challenge

2.1 Why Traditional Models Break

Traditional auto insurance pricing depends on three pillars: historical loss data aggregated across millions of drivers, demographic and behavioral risk factors validated over decades, and regulatory frameworks that require standardized reporting. Autonomous systems undermine all three:

Pricing Pillar	Traditional Model	Autonomous System Reality
Historical loss data	Millions of claims over decades, reported through standardized state systems	Manufacturer-specific data, proprietary formats, no cross-manufacturer comparability
Risk factor validation	Age, gender, driving record, vehicle type—validated across populations	Software version, ODD definition, sensor configuration—no standardized taxonomy
Standardized reporting	State-mandated accident reports, police records, claims databases	NHTSA SGO self-reporting, manufacturer-classified incidents, no independent audit
Risk independence	Individual driver risk largely independent	Fleet-wide correlated risk from shared software—one bug affects thousands
Inspection capability	Vehicle inspections, driver examinations, telematics	No standardized mechanism to verify operational boundaries

The fundamental issue is not that autonomous systems are more or less risky than human drivers. It is that insurers lack the independent data infrastructure to determine which claim is true for any specific system in any specific operational context. A Waymo operating in Phoenix during clear weather on mapped routes presents a different risk profile than a Tesla in FSD Beta operating on unmapped roads during a snowstorm. Without independent conformance data specifying operational boundaries and verifying adherence, these risk profiles are indistinguishable to the underwriter.

2.2 The Correlated Risk Problem

Perhaps the most significant underwriting challenge unique to autonomous systems is correlated risk.

In traditional auto insurance, individual vehicle risk is largely independent: one driver's accident does not increase the probability that another driver will have an accident. Portfolio diversification works because risks are distributed.

Autonomous systems invert this assumption. Every vehicle in a fleet runs the same software. A defect that causes one vehicle to fail to stop for a school bus causes every vehicle to fail to stop for a school bus. The Waymo December 2025 recall affected 3,067 vehicles simultaneously for the same software defect. The Cruise shutdown halted nearly 1,000 vehicles. These are not independent events—they are systemic exposures.

For reinsurers, this transforms autonomous fleet coverage from a frequency-based risk (many small independent claims) to an accumulation risk (potentially massive correlated losses from a single software defect). This is structurally similar to catastrophe risk in property insurance, where a single hurricane affects thousands of policies simultaneously. Catastrophe models exist for natural disasters because independent data about building construction, location, and vulnerability is available. No comparable independent data exists for autonomous system software vulnerability.

A single software defect in an autonomous fleet is the actuarial equivalent of a hurricane hitting every policyholder simultaneously. Without independent conformance data, insurers cannot distinguish between a Category 5 fleet and a fortified one.

2.3 The Reinsurance Implications

Reinsurers face the correlated risk problem at an even larger scale. A reinsurer covering multiple autonomous vehicle operators may discover that several of their cedants are running similar or identical software stacks. Swiss Re's 2024 report on autonomous mobility explicitly warned that re/insurance solutions will gradually move from being driver-centric to vehicle-centric and that the industry will need to rethink its approach within a complex AI and data-driven environment.

Swiss Re's sigma insights report released in early 2026 focused directly on how AI adoption is reshaping the risk landscape. The motor insurance line represents approximately 40% of the total $2.2 trillion global property and casualty market. A systemic autonomous vehicle software failure could trigger losses across multiple lines simultaneously—auto liability, product liability, cyber liability, and directors and officers coverage—creating a cascading reinsurance event that current models do not anticipate.

3. The Regulatory Patchwork

The insurance industry's data problem is compounded by regulatory fragmentation. No jurisdiction has established comprehensive requirements for independent verification of autonomous system performance as a condition of insurance coverage.

3.1 United States

The NAIC's AI Model Bulletin has been adopted by 23 states and Washington, D.C. It is principle-based, requiring governance and documentation but not prescribing specific verification standards. The NAIC's Big Data and AI

Working Group held six discussions in 2025 to consider whether a comprehensive AI model law is necessary. Pilot programs for a new AI examination tool are expected in early 2026.

At the state level, the patchwork is severe. Kentucky SB 241 raised minimum insurance for autonomous trucks over 62,000 pounds from $1 million to $5 million and extended human-on-board requirements to 2031. Florida requires $1 million minimum coverage for fully autonomous vehicles under its no-fault system. Texas designates the ADS owner as the operator who can be cited for violations. California only authorized law enforcement to issue noncompliance notices to driverless vehicles starting in 2026. NHTSA's Automated Vehicle Framework, updated in April 2025, streamlined incident reporting to five days and expanded the AV exemption program, but remains voluntary.

The bipartisan Autonomous Vehicle Acceleration Act of 2025 (S. 1798) would modernize Federal Motor Vehicle Safety Standards and preempt state bans on Level 4 trucks, but it contains no independent conformance requirements. Insurance is addressed only through minimum coverage mandates, not through data quality standards for underwriting.

3.2 European Union

The EU AI Act requires conformity assessments for high-risk AI systems, including those used in transportation and critical infrastructure, with obligations becoming applicable August 2, 2026.

However, harmonized standards for performing these assessments are not ready. CEN and CENELEC were unable to meet the August 2025 deadline. The Commission proposed extending timelines in November 2025. The first harmonized AI standard—prEN 18286 for quality management systems—only entered public enquiry on October 30, 2025.

For insurers operating in the EU market, this creates a specific challenge: the regulation will require conformity evidence that the standards infrastructure cannot yet produce. Insurers who develop underwriting requirements ahead of harmonized standards gain first-mover advantage in a market where conformity data will soon be mandatory.

3.3 What This Means for Insurers

The regulatory environment is converging toward mandatory conformance requirements for autonomous systems, but the timeline is uncertain and the specifics are undefined. Insurers who wait for regulatory mandates will be reactive. Insurers who establish independent conformance requirements now will define the standard that regulators eventually adopt—exactly as fire insurance created UL, and marine insurance created classification societies.

4. What ODDC Provides

4.1 The Three-Part Verification

ODDC addresses each element of the underwriting data gap through a three-part verification framework:

Formally Specified Operational Design Domain: Every certified system has a machine-readable ODD specification defining exactly where, when, and how the system is designed to operate.

This gives underwriters a precise, auditable description of the risk being transferred—not marketing language about capabilities, but formal boundary specifications that can be verified against actual behavior.

ENVELO Interlock (Non-Bypassable Runtime Enforcement): The ENVELO Interlock is a hardware-software enforcement layer that prevents the autonomous system from operating outside its declared ODD. It cannot be disabled by the system it governs. This provides underwriters with an enforcement mechanism equivalent to physical safety systems in property insurance—a verified, non-removable safeguard that reduces the probability of boundary exceedance.

CAT-72 Continuous Conformance Testing: The 72-hour Continuous Autonomous Testing procedure verifies that the system maintains conformance under sustained operation. Test results are cryptographically signed, tamper-evident, and independently stored. This provides underwriters with time-series behavioral data that is independent of the manufacturer's self-reporting.

4.2 Mapping ODDC to Actuarial Needs

Actuarial Requirement	Current Gap	ODDC Solution
Operational boundary definition	Self-declared in marketing materials; not machine-readable	Formal ODD specification—verifiable, auditable, standardized
Runtime boundary enforcement	Unverified internal controls; no independent audit trail	ENVELO Interlock—non-bypassable, tamper-evident, hardware-enforced
Continuous performance data	Manufacturer self-reported; proprietary formats; no audit	CAT-72 results: cryptographically signed, independently stored
Incident attribution data	Disputed across parties; no independent record of system state	Tamper-evident logs of system state at time of incident—courtroom-ready
Cross-fleet comparability	No standardized format; incomparable across manufacturers	Standardized conformance status: COMPLIANT / NON-COMPLIANT / EXPIRED
Correlated risk assessment	**No mechanism to assess fleet-wide software vulnerability**	**ODD + Interlock version tracking; conformance status per-vehicle**
Reinsurance aggregation data	No standardized exposure data across cedants	Conformance certificates provide standardized risk profiles

4.3 The Liability Shield

For the insured operator, ODDC certification provides a concrete liability defense. When a certified system is involved in an incident, the ODDC conformance record provides independently verified, tamper-evident evidence that the system was operating within its declared Operational Design Domain at the time of the event. This compresses legal review, reduces defense costs, and provides concrete evidence for claims resolution.

The inverse is equally powerful. When an uncertified system is involved in an incident, the absence of independent conformance evidence shifts the burden of proof to the operator. This creates a natural market incentive for certification without requiring regulatory mandates.

5. The Commercial Opportunity

5.1 The First-Mover Flywheel

The insurer who first integrates independent conformance data into autonomous system underwriting gains a structural competitive advantage through a self-reinforcing cycle:

First, requiring ODDC conformance data allows the insurer to offer risk-differentiated pricing—lower premiums for certified systems with verified enforcement, higher premiums or declinations for uncertified systems. Second, this pricing advantage drives demand for ODDC certification among operators seeking lower insurance costs. Third, increased certification volume generates more conformance data, enabling increasingly precise actuarial models. Fourth, better models enable tighter pricing, which attracts more policyholders, which generates more data. The flywheel accelerates.

The insurer who establishes this cycle first captures the market because competitors cannot replicate the actuarial advantage without access to the same conformance data infrastructure. This is structurally identical to how early telematics adopters gained pricing advantages that late entrants are still struggling to match.

5.2 Product Innovation Opportunities

ODDC conformance data enables insurance product innovations that are currently impossible:

Conformance-linked coverage: Policies that automatically adjust coverage limits based on real-time conformance status. If a system's ODDC certification lapses, coverage narrows. If conformance is maintained, coverage remains broad. This is the autonomous system equivalent of usage-based insurance.

Multi-party conformance policies: Policies that cover the entire autonomous system supply chain—developer, integrator, deployer—with liability allocation determined by which parties hold current ODDC certification. This resolves the finger-pointing problem before claims occur.

Reinsurance conformance treaties: Reinsurance contracts that reference ODDC conformance status as a condition of coverage, enabling reinsurers to manage correlated risk by requiring conformance verification across their portfolio.

6. Conclusion

The insurance industry has always been the first to require independent verification before extending coverage. Fire insurance created Underwriters Laboratories. Marine insurance created Lloyd's classification societies. Product liability insurance drove the adoption of UL, TÜV, and CSA certification.

In each case, insurers recognized that self-reported safety claims were insufficient for actuarial pricing, and they demanded independent verification infrastructure.

The autonomous systems era requires its own independent certification infrastructure. ODDC is that infrastructure. It provides the formally specified operational boundaries, non-bypassable enforcement mechanisms, and independently verified behavioral data that actuarial models require. It resolves the correlated risk problem by providing per-vehicle conformance status. It provides courtroom-ready evidence for claims resolution. And it creates a natural market incentive for safety investment without requiring regulatory mandates.

The question for insurers is not whether independent conformance data will become standard for autonomous system underwriting. The question is which insurer positions itself as the market leader before it does. The first mover captures the actuarial advantage. Everyone else pays catch-up.

REFERENCES [1] Swiss Re and Waymo. "Comparative Safety Performance of Autonomous- and Human Drivers." Analysis of 25.3 million autonomous miles against 500,000+ claims and 200 billion miles of human exposure. December 2024. [2] Swiss Re. "On the Emerging Risks of Automation: The Case for Autonomous Vehicles." September 2025. [3] Swiss Re. "Autonomous Mobility – How Demand and Supply Are Moving Closer to Equilibrium." Swiss Re Institute, August 2024. [4] Swiss Re. "Shifting Gears in a Changing Landscape – A Global Perspective of Motor (Re)Insurance." April 2025. [5] Swiss Re. sigma insights 01/2026: "AI adoption is reshaping the risk landscape." [6] EY. "The Age of Autonomous Technologies in Insurance: Separating Myth from Reality." March 2025. [7] ScienceSoft. "Artificial Intelligence for Insurance Underwriting in 2025." Global AI insurance market projections: $14.99B (2025) to $246.3B (2035). [8] BCG. Estimates 36% of total AI value for insurance captured in underwriting. 2025. [9] Fenwick. "Tracking the Evolution of AI Insurance Regulation." NAIC developments, 23 states adopting AI Model Bulletin. December 2025. [10] Florida Jury Verdict, Tesla Autopilot Fatal Accident, Key Largo. $243 million award, 33% manufacturer liability. 2025. [11] Waymo Recall of 1,212 Robotaxis. NHTSA investigation – collisions with stationary objects. May 2025. [12] Waymo Recall of 3,067 Robotaxis. School bus safety violations in Austin and Atlanta. December 2025. [13] Austin Independent School District. Letter to Waymo documenting 20 illegal school bus passes, 2025–2026 school year. [14] NHTSA. Automated Vehicle Framework, updated April 2025. Standing General Order on ADS incident reporting. [15] Cruise Robotaxi Pedestrian Incident, San Francisco. Operations suspended, ~1,000 vehicles recalled. 2023. [16] Long, B., Zhao, Z., and Cai, Q. "Comparing Tort Liability Frameworks in Autonomous Vehicle Accident Governance."

World Electric Vehicle Journal, 17(1):32, January 2026. [17] NAIC Big Data and AI Working Group. Six discussions in 2025 on whether comprehensive AI model law is needed.

Pilot programs expected early 2026. [18] Kentucky SB 241 (2025). Minimum AV truck insurance raised from $1M to $5M. [19] Autonomous Vehicle Acceleration Act of 2025 (S. 1798). Bipartisan legislation to modernize FMVSS. [20] European Union. Regulation (EU) 2024/1689 (AI Act). High-risk obligations applicable August 2, 2026. [21] European Commission. Digital Omnibus Proposal, November 19, 2025. Timeline extension for high-risk AI rules. [22] CEN/CENELEC. prEN 18286: AI Quality Management System for EU AI Act. Entered public enquiry October 30, 2025. [23] Apollo ibott (Lloyd's Syndicate). Chris Moore statement on Waymo–Swiss Re study: 90% lower claims frequency benchmark. [24] Sentinel Authority. ODDC Overview v3.0, ENVELO Requirements v3.0, CAT-72 Procedure v3.0. Published at sentinelauthority.org.