SA SENTINEL AUTHORITY

When Self-Certification Fails

Lessons from Boeing 737 MAX for the Age of Autonomous Systems

February 2026 — Public Document

346 people died in two Boeing 737 MAX crashes. Congressional investigators concluded these deaths were preventable. The root cause was not a software bug. It was a certification model that allowed the manufacturer to evaluate its own safety. This white paper examines the structural failure that made the 737 MAX disasters possible and introduces ODDC, the framework designed to ensure that the certification failures of aviation are never replicated in the age of autonomous systems.

Executive Summary

On October 29, 2018, Lion Air Flight 610 crashed into the Java Sea thirteen minutes after takeoff from Jakarta. On March 10, 2019, Ethiopian Airlines Flight 302 crashed six minutes after departure from Addis Ababa. All 346 people aboard both flights were killed. At the center of both crashes was the Maneuvering Characteristics Augmentation System (MCAS), a flight control system Boeing concealed from pilots and regulators.

The U.S. House Transportation and Infrastructure Committee conducted an 18-month investigation, reviewing 600,000 pages of documents and interviewing dozens of Boeing and FAA employees. The Committee's 238-page final report, released September 16, 2020, concluded that the crashes were "the horrific culmination of a series of faulty technical assumptions by Boeing's engineers, a lack of transparency on the part of Boeing's management, and grossly insufficient oversight by the FAA."

This white paper examines the structural failure that made the 737 MAX disasters possible: delegated self-certification. It identifies the same structural vulnerability in today's autonomous systems landscape—where AI-driven machines are being deployed into physical environments with no independent conformance framework. It then introduces Operational Design Domain Conformance (ODDC), the framework designed to ensure that the certification failures of aviation are never replicated in the age of autonomous systems.

1. The Boeing 737 MAX: Anatomy of a Certification Failure

1.1 What Happened

Boeing designed the 737 MAX to compete with the Airbus A320neo. To minimize costs and avoid requiring expensive simulator training for pilots transitioning from earlier 737 models, Boeing opted for a design modification rather than a clean-sheet aircraft. The new, larger engines were mounted higher and farther forward on the wing, altering the aircraft's aerodynamic characteristics. To compensate, Boeing introduced MCAS—a software system that automatically pushed the aircraft's nose down under certain conditions to maintain handling similar to previous 737 models.

MCAS relied on a single angle-of-attack sensor. When that sensor provided faulty data, MCAS activated erroneously, forcing both aircraft into catastrophic nosedives. Pilots, who had not been informed of MCAS's existence, were unable to diagnose and counteract the system before losing control.

1.2 Five Systemic Failures

The Congressional investigation identified five interconnected failures that produced this outcome. These were not isolated incidents. They were structural features of the certification system itself.

Failure Category	Finding
Production Pressures	Competition with Airbus drove Boeing to prioritize speed and cost over safety. Internal surveys revealed 3
Faulty Technical Assumptions	Boeing assumed pilots would respond to MCAS activation within four seconds. Internal testing revealed a
Culture of Concealment	Boeing withheld the ten-second test result from the FAA. MCAS was removed from pilot training manuals.
Conflicted Representation	FAA's Organization Designation Authorization (ODA) program allowed Boeing employees to perform certif
Regulatory Capture	The FAA's oversight structure ceded substantial authority to the manufacturer it was supposed to regulate

1.3 The Delegation Model

The root cause was not Boeing's culture alone. It was the regulatory architecture that made Boeing's culture consequential. Under the FAA's ODA program, Boeing was authorized to certify its own aircraft. Boeing employees acted as both advocate and evaluator. The manufacturer that stood to lose billions from training requirements was the same entity determining whether training was necessary.

> *"The problem is it was compliant and not safe. And people died. That is clear evidence that the current regulatory system is fundamentally flawed and needs to be repaired." — Representative Peter DeFazio, Chair, House Transportation and Infrastructure Committee*

This is the fundamental lesson of the 737 MAX: compliance without independence is not compliance. When the entity being evaluated controls the evaluation, the evaluation is meaningless. The system did not fail because it lacked rules. It failed because the entity subject to the rules was also the entity enforcing them.

1.4 The Accountability Gap

In January 2021, the U.S. Department of Justice announced a $2.51 billion deferred prosecution agreement with Boeing. The company was charged with one count of conspiracy to defraud the United States. The settlement included a $243.6 million criminal penalty, $1.77 billion in compensation to airline customers, and a $500 million fund for crash victims' families. Boeing admitted that its employees "chose the path of profit over candor by concealing material information from the FAA."

In May 2024, the DOJ determined that Boeing had breached the terms of this agreement by failing to implement the required compliance and ethics program. In January 2024—just two days before the deferred prosecution agreement was set to expire—a door panel blew off a Boeing 737 MAX 9 operated by Alaska Airlines, revealing that the aircraft had left Boeing's factory with key bolts uninstalled. The pattern of systemic failure continued even after 346 deaths, a Congressional investigation, and a multi-billion-dollar settlement.

The accountability gap is structural, not cultural. No amount of internal reform changes the fact that a manufacturer certifying its own safety-critical systems faces an irreconcilable conflict of interest.

2. The Autonomous Systems Parallel

2.1 A Familiar Pattern

The autonomous systems industry in 2026 faces the same structural conditions that preceded the 737 MAX disasters. Companies developing AI-driven systems for transportation, manufacturing, healthcare, energy, and infrastructure are operating in environments where:

There is no independent conformance framework. No regulatory body has established a standardized mechanism for evaluating whether autonomous systems operate within their operational boundaries. Companies define their own safety parameters, test against their own criteria, and report their own results.

Self-certification is the default. In the United States, NHTSA's approach to autonomous vehicles has been largely voluntary guidance. The Automated Vehicles 4.0 framework provides principles, not enforceable standards. Companies self-report safety data with no standardized format, no independent verification, and no mechanism to detect omissions.

Competitive pressure incentivizes concealment. Just as Boeing's competition with Airbus created pressure to minimize training costs, autonomous systems developers face intense pressure to deploy faster, claim broader operational capabilities, and minimize the appearance of limitations.

Regulators lack technical depth. The FAA’s inability to independently evaluate MCAS is mirrored across regulatory agencies today. NHTSA, OSHA, the FDA, and other agencies responsible for autonomous system safety lack the technical infrastructure to verify manufacturer claims about AI-driven system behavior.

2.2 The Scope of Exposure

The 737 MAX operated in a single domain—commercial aviation—with extensive existing regulatory infrastructure, decades of precedent, and a deeply institutionalized safety culture. Despite all of that, self-certification produced catastrophic failure. Autonomous systems are being deployed across dozens of domains simultaneously, most with far less regulatory maturity.

Domain	Current Oversight Status
Autonomous Vehicles	Voluntary federal guidance; fragmented state-level regulation; no mandatory performance standards befor
Industrial Robotics	OSHA standards assume human operators; no autonomous equipment authorization pathway exists.
Healthcare AI	FDA clearance processes designed for static devices, not continuously learning autonomous systems.
Data Center Operations	AI-managed cooling, power, and infrastructure with no independent operational boundary verification.
Energy Grid Management	AI-driven load balancing and distribution with no conformance testing for autonomous decision-making.
Construction Automation	Regulations require a “competent person” on-site; AI monitoring systems have no regulatory recognition.

Each of these domains places autonomous systems in direct contact with physical infrastructure and human safety. Each relies on some version of manufacturer self-assessment. None has an independent mechanism to verify that autonomous systems operate within their operational boundaries.

2.3 The Question

> **If delegated self-certification failed in the most regulated safety-critical industry on earth—with 60 years of precedent, a dedicated regulatory agency, and a global fleet of trained professionals—what is the realistic probability that self-certification will succeed in industries with none of these protections?**

3. ODDC: The Structural Solution

3.1 Design Principles

Operational Design Domain Conformance (ODDC) is a conformance determination framework developed by Sentinel Authority to address the structural certification gap identified in the 737 MAX investigation and now emerging across the autonomous systems landscape. ODDC is built on four principles derived directly from the Boeing failures:

Independence. The evaluating body must be structurally independent of the entity being evaluated. Sentinel Authority operates as an independent certification body—not a software vendor, not a consulting firm, not a subsidiary of any manufacturer. The entity that determines conformance has no financial interest in the outcome.

Enforceability. Conformance cannot be a documentation exercise. ODDC requires deployment of the ENVELO Interlock—a non-bypassable runtime enforcement layer that wraps the autonomous system’s decision-action pipeline. The Interlock validates every autonomous action against operational boundaries in real time, applying tiered enforcement: self-correction near the boundary, controlled degradation (Minimum Risk Condition) at the enforcement margin, and hard halt at the wall. It does not advise, warn, or recommend. It enforces.

Provability. Every conformance determination produces a tamper-evident, cryptographically verifiable evidentiary record. HMAC-signed telemetry, hash-chained logging, and bounded-latency runtime state evaluation create an auditable chain of evidence that regulators, insurers, and counterparties can independently verify.

Objectivity. Conformance criteria are published, standardized, and testable. The CAT-72 (Conformance Authorization Test) is a 72-hour assessment procedure with pass/fail criteria that any qualified reviewer can evaluate against the published requirements. There is no subjective judgment. The system either operates within its defined boundaries or it does not.

3.2 How ODDC Works

The ENVELO Interlock deploys onto the operator’s infrastructure and auto-discovers the system’s operational envelope by observing live telemetry during an initial learning phase. The Interlock maps quantitative boundaries—the specific parameters, ranges, and conditions within which the system actually operates. Operators can also define boundaries prescriptively for domains that require it (defense, nuclear, FDA-mandated limits), but adaptive auto-discovery from operational telemetry is the default path.

Once boundaries are approved, the Interlock enforces them in real time. If the system approaches a boundary, the Interlock triggers self-correction. If the system breaches the boundary, the Interlock forces a Minimum Risk Condition—a controlled degradation to a safe operating state. If the system reaches the enforcement wall, the Interlock executes a hard halt, stopping autonomous operation entirely.

The CAT-72 procedure validates this enforcement over a cumulative 72-hour period, testing the system across operational regimes, including deliberate boundary-stress testing, to confirm that the Interlock performs as specified. Upon successful completion, Sentinel Authority issues a conformance record documenting the scope, evidence summary, validity period, and cryptographic verification data.

ODDC defines four conformance states that provide a common vocabulary for all stakeholders:

State	Description
LEARNING	Telemetry collection and boundary auto-discovery. The system operates normally while the Interlock observes liv
BOUNDED	Boundaries approved, enforcement active. The CAT-72 72-hour verification is in progress. The system operates u
CONFORMANT	Full autonomy within the verified operational envelope. Conformance has been independently determined. Contin
PAUSED	Conformance suspended pending remediation. Triggered by drift detection, boundary violations, or conformance

3.3 Why This Architecture Matters

The 737 MAX investigation revealed five systemic failures. ODDC addresses each one structurally:

737 MAX Failure	ODDC Structural Response
Production pressures overriding safety	The Interlock is a non-bypassable runtime enforcement layer. It cannot be overridden by management
Faulty technical assumptions	CAT-72 tests actual system behavior over 72 hours, including deliberate boundary stress testing. Assu
Culture of concealment	HMAC-signed, hash-chained telemetry is generated by the enforcement mechanism itself. Evidence ca
Conflicted representation	Sentinel Authority is structurally independent. The evaluating body has no financial relationship with th
Regulatory capture	ODDC is designed for regulatory referencing. Regulators receive the evidence; they determine policy.

4. The Regulatory Case for Independent Conformance

4.1 Cutting Both Ways

ODDC is designed to be politically neutral. It does not favor manufacturers over regulators or regulators over manufacturers. It holds every actor to the standard defined by their own operational envelope.

For manufacturers operating within their defined boundaries, an ODDC conformance record provides defensible, independently verified evidence of responsible operation. In litigation, procurement, and regulatory review, this evidence demonstrates that the system performed as specified.

For manufacturers operating outside their defined boundaries, the same framework produces evidence of non-conformance. The Interlock’s telemetry does not distinguish between accidental and intentional boundary violations. It records what happened.

This dual nature makes ODDC attractive to regulators. Adopting ODDC does not require taking a pro-industry or anti-industry stance. It requires taking a pro-evidence stance. The framework protects compliant actors and exposes non-compliant ones. That is the definition of politically defensible regulation.

4.2 What Regulators Need

Today, regulators facing questions about autonomous system safety have no good options. They can issue voluntary guidance that carries no enforcement weight. They can attempt to build internal technical capacity—a resource-intensive proposition that would take years. Or they can delegate oversight to manufacturers and hope the Boeing pattern does not repeat.

ODDC offers a fourth option: reference an independent framework that provides the technical evaluation infrastructure regulators lack, without requiring regulators to build it themselves. The framework produces objective, verifiable evidence in a standardized format. Regulators determine policy; ODDC provides proof.

4.3 Precedent in Other Industries

Independent conformance determination is the established model in every mature safety-critical industry. Underwriters Laboratories (UL) provides independent product safety certification across electrical, electronic, and consumer product categories. The industry trusts UL because UL does not manufacture the products it certifies. The same principle operates in financial auditing, nuclear safety, pharmaceutical manufacturing, and food safety. Every industry that has suffered catastrophic self-certification failures has eventually adopted independent third-party evaluation.

The autonomous systems industry has not yet had its independent certification body. Given the pace of deployment and the scale of physical exposure, the question is not whether independent conformance determination will be required. It is whether it will be established before or after a catastrophic failure forces the issue—as it did in aviation.

5. Conclusion: Before, Not After

The 737 MAX investigation produced a clear, documented record of what happens when safety-critical systems are certified by the entities that build them. The failure was not unpredictable. It was structural. The incentive architecture of self-certification made concealment rational, oversight ineffective, and accountability impossible until after people died.

The autonomous systems industry is now at the same inflection point. Systems capable of physical action in the real world are being deployed at scale, governed by voluntary frameworks, and evaluated by their own manufacturers. The structural conditions are identical. The only variable is time.

ODDC exists to change the sequence. Instead of waiting for a catastrophic failure to force regulatory action—as happened in aviation—ODDC provides the independent conformance infrastructure now. The framework is published, operational, and domain-agnostic. It applies to any autonomous system controlling physical infrastructure: transportation, manufacturing, healthcare, energy, data centers, construction.

> **The lesson of the 737 MAX is not that Boeing was uniquely negligent. It is that any entity given the authority to certify its own safety will eventually prioritize other interests over safety. The structural fix is not better self-certification. It is independent certification.**

ODDC is that structural fix.

References

1. DeFazio, P.A., and R. Larsen. “Final Committee Report: The Design, Development & Certification of the Boeing 737 MAX.” U.S. House Committee on Transportation and Infrastructure, September 16, 2020.

2. U.S. Department of Justice. “Boeing Charged with 737 Max Fraud Conspiracy and Agrees to Pay over $2.5 Billion.” Office of Public Affairs, January 7, 2021.

3. U.S. Department of Justice. “United States v. The Boeing Company.” Criminal Division, updated November 2025. Includes DPA breach determination (May 2024) and non-prosecution agreement (May 2025).

4. National Transportation Safety Board. Investigation reports on Lion Air Flight 610 (October 29, 2018) and Ethiopian Airlines Flight 302 (March 10, 2019).

5. U.S. House of Representatives. H.R. 133, Division V: Aircraft Certification, Safety, and Accountability Act. 116th Congress.

6. Ullrich, L. et al. “Regulatory and Safety-Assurance Frameworks for AI-Based Automated Vehicles.” IEEE Transactions on Intelligent Vehicles, 2025.

7. European Union. Regulation (EU) 2024/1689 (AI Act). Adopted 2024, high-risk system obligations effective 2025–2027.

8. Foundation for American Innovation. “Regulatory Reform for AI and Autonomy.” 2025.

9. International AI Safety Report: First Key Update. Commissioned by 30 nations, October 2025.

10. Sentinel Authority. ODDC Overview v3.0, ENVELO Requirements v3.0, CAT-72 Procedure v3.0. Published at sentinelauthority.org.

This white paper references publicly available government reports, court filings, and legislative records. All factual claims are sourced from the Congressional investigation, Department of Justice proceedings, and regulatory agency publications cited in the References section. This document does not constitute legal advice.

— End of Document —