ODDC Overview

Operational Design Domain Conformance Framework

Version 1.0 · February 2026 · Public Document

Document Purpose

This document provides a conceptual overview of the Operational Design Domain Conformance (ODDC) framework developed by Sentinel Authority. It is non-normative, intended for regulators, insurers, enterprise partners, and other stakeholders evaluating autonomous system governance.

ODDC is the first independent conformance determination framework for autonomous physical systems. It addresses a structural gap in the current autonomous systems ecosystem: the absence of standardized, independent verification that deployed autonomous systems actually operate within their declared operational boundaries.

1. The Problem

Autonomous systems are deployed across safety-critical domains—transportation, healthcare, industrial automation, energy grid management, defense, and more—without any standardized mechanism for independently verifying that these systems stay within their designed operational boundaries.

Existing governance frameworks (ISO 42001, NIST AI RMF, SOC 2) verify that organizations have the right *processes* in place. They do not verify that deployed systems actually *behave* within declared constraints. This is the distinction between process attestation and behavioral attestation.

The result: autonomous systems operate in production environments with no independent confirmation that their runtime behavior conforms to the boundaries their operators declared. When failures occur, there is no objective evidentiary basis for determining whether the system exceeded its design domain—only competing claims from interested parties.

2. What ODDC Is

ODDC is a conformance determination framework. It provides independent, evidence-based verification that an autonomous system operates within its defined Operational Design Domain (ODD)—the specific conditions, parameters, and boundaries within which the system is designed to function.

ODDC provides three things:

- **Runtime enforcement.** The ENVELO Interlock deploys onto the operator's infrastructure and enforces operational boundaries in real time. If the system approaches a boundary, self-correction is triggered. If it breaches, a Minimum Risk Condition is forced. If it reaches the enforcement wall, a hard halt is executed.
- **Independent verification.** The CAT-72 (Conformance Authorization Test) is a 72-hour continuous assessment that validates enforcement across operational regimes, including deliberate boundary-stress testing.

• **Continuous monitoring.** Post-certification, the Interlock continues operating, generating cryptographically signed telemetry that provides ongoing conformance evidence. Annual surveillance reviews confirm continued compliance.

3. What ODDC Is Not

• **Not a safety certification.** ODDC does not attest that a system is safe. It attests that a system operates within declared boundaries. Safety is determined by the boundaries themselves, which are defined by the operator and evaluated by domain regulators.

• **Not a process audit.** ODDC does not evaluate organizational governance, documentation, or management practices. It verifies runtime behavior.

• **Not a consulting engagement.** Sentinel Authority does not advise operators on how to design their systems, define their boundaries, or improve their performance. It determines conformance against declared specifications.

• **Not software.** ENVELO is a requirements specification. Sentinel Authority defines what enforcement must accomplish; operators design and implement compliant systems.

4. The ENVELO Interlock

ENVELO (Enforced Non-Violable Execution-Limit Override) is the runtime enforcement mechanism at the core of ODDC certification. The ENVELO Interlock deploys onto the operator's infrastructure and provides three tiers of enforcement:

Tier	Mechanism	Trigger
Tier 1	Self-Correction	System approaches a boundary parameter
Tier 2	Minimum Risk Condition (MRC)	System breaches a boundary
Tier 3	Hard Halt	System reaches the enforcement wall

The Interlock maps the system's operational envelope by observing live telemetry during an initial learning phase. Operators can also define boundaries prescriptively for domains that require it (defense, nuclear, FDA-mandated limits). All telemetry is HMAC-signed and hash-chain linked, creating a tamper-evident audit trail.

5. Conformance States

ODDC defines four conformance states:

State	Description
LEARNING	Telemetry collection and boundary auto-discovery. The system operates normally while the Interlock observes live behavior and maps the operational envelope.
BOUNDED	Boundaries approved, enforcement active. CAT-72 72-hour verification in progress. The system operates under active enforcement while conformance is being proven.

State	Description
CONFORMANT	Full autonomy within the verified operational envelope. Conformance independently determined. Annual surveillance reviews required.
PAUSED	Conformance suspended pending remediation. Triggered by drift detection, boundary violations, or conformance expiration.

6. The Certification Process

ODDC certification follows a structured seven-phase process:

Phase 1: Eligibility Review. Sentinel Authority reviews the applicant's system type, operational context, and readiness for conformance assessment.

Phase 2: ODD Definition. The operator defines the Operational Design Domain—the specific parameters, ranges, conditions, and boundaries within which the system is designed to operate.

Phase 3: Documentation Review. Sentinel Authority reviews the ODD specification for completeness, internal consistency, and testability.

Phase 4: ENVELO Interlock Deployment. The Interlock is deployed onto the operator's infrastructure. Telemetry collection begins. Boundary auto-discovery or prescriptive boundary loading completes.

Phase 5: CAT-72 Execution. The 72-hour Conformance Authorization Test runs continuously, testing enforcement across operational regimes including boundary-stress scenarios.

Phase 6: Conformance Determination. Sentinel Authority reviews CAT-72 evidence and makes a CONFORMANT or NON-CONFORMANT determination. Conformance records are issued with cryptographic verification.

Phase 7: Continued Monitoring. Post-certification, the Interlock continues operating. Annual surveillance reviews confirm ongoing conformance. The 95% conformance threshold applies continuously.

7. Institutional Positioning

Sentinel Authority operates as an independent certification body—not a vendor, consultant, or software company. The organizational model is analogous to UL (Underwriters Laboratories) for autonomous systems: an institution that sets conformance standards, tests against them, and certifies compliance.

ODDC certification is designed to be politically neutral. It cuts both ways: it protects compliant operators by providing objective evidence of conformance, and it exposes non-compliant operators by establishing a verifiable standard against which performance can be measured. This dual accountability makes the framework defensible regardless of which stakeholder adopts it first.

For questions about ODDC certification or to begin the eligibility process, visit sentinelauthority.org or contact info@sentinelauthority.org.