ODDC Overview

ODD Conformance Determination Framework

Version 1.1 — January 2026 — Public Document

ODDC (ODD Conformance Determination) provides independent, third-party attestation that autonomous systems operate within formally declared boundaries with non-bypassable enforcement. This document describes the framework components, attestation scope, and conformance process.

1. Introduction

1.1 Purpose

ODD Conformance Determination (ODDC) is Sentinel Authority's voluntary conformance framework for autonomous systems. ODDC provides standardized, verifiable evidence of bounded operation that serves as a first-order risk control input for underwriting review of autonomous infrastructure.

1.2 Framework Components

The ODDC framework consists of three integrated components:

Component	Description
ODD	Operational Design Domain — Formal specification of operational boundaries, including quantitative tolerances and constraints.
ENVELO	Enforced Non-Violable Execution-Limit Override — Runtime enforcement requirements ensuring the system cannot operate outside declared ODD boundaries.
CAT-72	Convergence Authorization Test — 72+ hour evidentiary procedure demonstrating bounded operation and enforcement effectiveness.

1.3 What ODDC Is Not

ODDC explicitly does not constitute:

- Regulatory approval or certification
- Safety certification (e.g., IEC 61508, ISO 26262)
- Product certification or quality mark
- Guarantee of system performance or reliability
- Insurance or warranty of any kind

2. Attestation Scope

2.1 What ODDC Attests

Upon successful conformance determination, ODDC attests that at the time of determination:

Category	Attestation
ODD Specification	Applicant has formally specified an Operational Design Domain with quantitative boundaries, tolerances, and identified constraints.
Operational Evidence	System demonstrated stable operation within declared ODD through 72+ hours of continuous CAT-72 testing.
ENVELO Enforcement	Non-bypassable enforcement mechanism is architecturally present and activates correctly on boundary approach.
Audit Trail	Tamper-evident audit records generated for all enforcement events with cryptographic integrity.

2.2 What ODDC Does Not Attest

- Functional safety of underlying system design
- Regulatory or legal compliance
- Cybersecurity posture or resilience
- System performance, accuracy, or fitness for purpose
- AI model correctness, training data quality, or algorithmic fairness

3. Conformance Process

The conformance process follows five phases:

Phase 1: Application

Submit ODD specification, system architecture, and ENVELO implementation approach.

Phase 2: Scope Assessment

Sentinel Authority reviews and determines test requirements (5-10 business days).

Phase 3: CAT-72 Testing

72+ hours of continuous monitored operation with cryptographic evidence generation.

Phase 4: Determination

Conformance determination issued with certificate hash and registry publication.

Phase 5: Maintenance

Ongoing ENVELO Agent operation with renewal testing prior to expiration.

4. Related Documents

- **ENVELO Requirements v1.1** — Runtime enforcement requirements specification
- **CAT-72 Procedure v1.1** — Convergence test requirements and format
- **Conformance Agreement** — Terms and conditions for conformance determination

— End of Document —