



1. Introduction

1.1 Purpose

ODD Conformance Determination (ODDC) is Sentinel Authority's voluntary conformance determination framework for autonomous systems. ODDC provides independent, third-party attestation that an autonomous system's operation is bounded by formally specified constraints with non-bypassable enforcement.

ODDC is designed to function as a first-order risk control input for underwriting review of autonomous infrastructure. By providing standardized, verifiable evidence of bounded operation, ODDC enables risk assessment that would otherwise require bespoke technical evaluation for each system.

1.2 Framework Components

The ODDC framework consists of three integrated components:

- ODD (Operational Design Domain): Formal specification of the operational boundaries within which the system is designed to operate, including quantitative tolerances and constraints.
- ENVELO (Enforcer for Non-Violable Execution & Limit Oversight): Runtime enforcement requirements ensuring the system cannot operate outside declared ODD boundaries.
- CAT-72 (Convergence Authorization Test): Evidentiary procedure demonstrating bounded operation and enforcement effectiveness over 72+ hours of continuous operation.

1.3 What ODDC Is Not

ODDC is not:

- Regulatory approval or certification
- Safety certification (e.g., not equivalent to IEC 61508, ISO 26262)
- Product certification or quality mark
- Guarantee of system performance or reliability
- Insurance or warranty

2. What ODDC Attests

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

2.1 ODD Specification

- Applicant has formally specified an Operational Design Domain
- ODD specification includes quantitative boundaries and tolerances
- All critical state variables and constraints are identified
- Safe states are defined for all operational modes



2.2 Operational Evidence

- Evidence demonstrates stable operation within declared ODD through CAT-72 completion
- System maintained bounded operation across 72+ hours of continuous demonstration
- Multi-regime performance verified including edge conditions and transitions
- Declared tolerances were not exceeded during demonstration period

2.3 Enforcement Verification

- ENVELO-compliant runtime enforcement is architecturally present
- Enforcement mechanism is non-bypassable
- Fail-closed behavior verified through intentional boundary approach
- Enforcement response times within declared specifications

2.4 Audit Capability

- Tamper-evident audit records exist
- Records are available for inspection
- Hash-chain integrity verified
- Records retained per ODDC requirements

2.5 Architectural Consonance

- Training data and safety envelope derive from common physics-based simulation
- Simulation provenance documented and attested
- No independent derivation of safety boundaries

3. What ODDC Does Not Attest

ODDC conformance explicitly does not attest:

- Functional safety of the underlying autonomous system. ODDC verifies bounded operation, not safe operation. A system may operate within bounds that are themselves unsafe.
- Regulatory compliance (safety, environmental, or otherwise). ODDC is not a regulatory approval and does not substitute for required certifications.
- Cybersecurity posture or resilience to attack. ODDC does not evaluate security controls, vulnerability to exploitation, or resilience to adversarial inputs.
- System performance, accuracy, or reliability metrics. ODDC verifies bounded operation, not operational effectiveness or quality of outcomes.
- AI model correctness or fitness for intended purpose. ODDC does not evaluate whether the control model makes good decisions, only that its actions are bounded.
- Compliance with any jurisdiction's legal requirements. Operators remain responsible for all applicable legal and regulatory compliance.



4. Conformance Process

4.1 Process Overview

ODDC conformance follows a structured seven-stage process from initial inquiry through issuance. Total timeline is typically 60-90 days depending on applicant readiness and scope complexity.

4.2 Stage 1: Initial Inquiry

Applicant contacts Sentinel Authority to discuss scope and feasibility. Initial inquiry establishes:

- System type and operational domain
- Preliminary ODD scope
- Timeline requirements
- Estimated fee range

Response time: 5 business days

4.3 Stage 2: Scope Assessment

Sentinel Authority reviews preliminary ODD specification and determines evaluation parameters:

- ODD complexity classification
- Required evidence elements
- CAT-72 configuration (duration, witness method)
- Fee quotation

Duration: 10 business days. Fee: \$2,500-\$5,000

4.4 Stage 3: Documentation Review

Applicant submits complete documentation package:

- ODD specification with all boundaries and tolerances
- ENVELO implementation documentation
- Architectural evidence (simulation identification, training data provenance, envelope derivation)
- System architecture documentation

Duration: 15-30 business days for Sentinel Authority review

4.5 Stage 4: CAT-72 Scheduling

Upon documentation approval, CAT-72 is scheduled:

- Test window coordination
- Witness arrangements (on-site or remote)
- Infrastructure verification

Scheduling within 30 days of documentation approval



4.6 Stage 5: CAT-72 Execution

72+ hour convergence authorization test:

- Continuous operation demonstration
- Multi-regime stress testing
- Fail-closed verification
- Evidentiary record generation

See CAT-72 Procedure for detailed requirements

4.7 Stage 6: Conformance Determination

Sentinel Authority reviews CAT-72 evidence and issues determination:

- Evidence completeness verification
- Compliance assessment against all requirements
- Determination: Conformant / Non-Conformant / Remediation Required

Duration: 10 business days

4.8 Stage 7: Issuance

Upon positive determination:

- Conformance record published to Sentinel Authority registry
- Unique conformance ID assigned
- Mark authorization granted
- Conformance term begins

5. Fees

5.1 Fee Schedule

Scope Assessment: \$2,500-\$5,000

Single-ODD Conformance: \$15,000-\$35,000

Multi-ODD Conformance: \$35,000-\$75,000

Enterprise/Fleet Programs: Custom quotation

On-site Witness: \$5,000 + travel expenses

Annual Maintenance: \$2,500/year

Renewal: 50% of original conformance fee

5.2 Payment Terms

50% due upon documentation submission. 50% due upon conformance determination. Fees are non-refundable upon failed determination. Applicants may re-attempt after addressing deficiencies; re-attempt fees apply.



6. Mark Authorization

Conformant operators are authorized to display the ODDC mark.

6.1 Mark Elements

The ODDC mark includes:

- Sentinel Authority brand element
- ODDC designation
- Unique conformance ID
- Optional: validity date

6.2 Mark Usage

Authorized uses include:

- Equipment labels and documentation
- System dashboards and interfaces
- Contracts and insurance submissions
- Marketing materials (with conformance ID)

6.3 Mark Restrictions

Mark use is prohibited:

- After conformance expiration or revocation
- On systems not covered by conformance determination
- In ways implying regulatory approval
- Without visible conformance ID

7. Liability

ODDC conformance does not transfer liability from the operator to Sentinel Authority.

Applicants and operators remain solely responsible for:

- Implementation quality and correctness
- Operational compliance with all applicable requirements
- System behavior and outcomes
- All regulatory obligations
- All consequences of system operation

Sentinel Authority is an independent conformance determination body. It is not a regulator, insurer, implementation partner, auditor, or guarantor.