ODDC Standard Specification

Normative Requirements for Operational Design Domain Conformance

v1.0 · February 2026 · Public Normative Document

This document constitutes the normative specification for Operational Design Domain Conformance (ODDC). All conformance determinations issued by Sentinel Authority are made pursuant to the requirements defined herein. This specification is publicly available and subject to versioned revision with independent technical review.

Contents

1. Scope and Purpose

This specification defines the requirements for Operational Design Domain Conformance (ODDC) — an independent conformance framework for autonomous systems. ODDC provides a structured, verifiable mechanism for attesting that an autonomous system operates within its declared operational boundaries and that those boundaries are enforced at runtime by a non-bypassable execution-layer interlock.

ODDC is applicable to any autonomous system that operates within a formally declared Operational Design Domain (ODD), across all operational domains including but not limited to: autonomous vehicles, unmanned aerial systems, surgical robotics, industrial automation, energy grid management, and autonomous maritime systems.

The purpose of this specification is to establish normative requirements for:

- Formal specification of Operational Design Domains with quantitative boundaries
- Non-bypassable runtime enforcement of declared ODD boundaries (ENVELO)
- Tamper-evident telemetry and cryptographic audit chain integrity
- Conformance Authorization Testing (CAT-72) procedures and pass/fail criteria
- Certificate issuance, maintenance, suspension, and revocation
- Public registry of all conformance determinations

> ***Normative Status.*** *Requirements expressed with "shall" are mandatory for conformance. Requirements expressed with "should" are recommended. Requirements expressed with "may" are optional.*

2. Normative References

The following documents are referenced by this specification. Where versioned, the most recent published revision applies unless otherwise stated.

Document ID	Title
ODDC-STD-1.0	This document — ODDC Standard Specification
ENVELO-REQ	ENVELO Requirements Specification (current: v3.0)
CAT-72-PROC	CAT-72 Conformance Authorization Test Procedure (current: v4.0)
SA-GOV	Sentinel Authority Governance and Independence Statement
ODDC-CERT-GUIDE	ODDC Certification Guide (current: v5.0)

3. Terms and Definitions

Term	Definition
ODD	Operational Design Domain — the formally specified set of conditions, boundaries, and constraints within which an autonomous system is designed and authorized to operate.

Term	Definition
ODDC	Operational Design Domain Conformance — the verified state of an autonomous system operating within its declared ODD under active enforcement and audit.
ENVELO	Enforced Non-Violable Execution-Limit Override — a non-bypassable runtime enforcement interlock that constrains autonomous system behavior to declared ODD boundaries.
CAT-72	Conformance Authorization Test, 72 hours — the structured cumulative enforcement verification protocol used to evaluate runtime boundary integrity.
Interlock	The ENVELO software agent deployed on or alongside the autonomous system that enforces boundaries and transmits enforcement telemetry.
MRC	Minimum Risk Condition — a predefined safe state to which the system transitions upon boundary exceedance.
Conformance Determination	The formal decision by Sentinel Authority, based on CAT-72 results and audit review, that a system satisfies ODDC requirements.
Boundary Event	Any instance where system telemetry indicates approach to, contact with, or exceedance of a declared ODD boundary.
Hash Chain	A cryptographically linked sequence of enforcement event records forming a tamper-evident audit trail.
Convergence Score	A quantitative measure (≥0.00 to 1.00) of the degree to which system behavior aligns with declared ODD boundaries during CAT-72.

4. Operational Design Domain (ODD) Requirements

An applicant seeking ODDC conformance shall formally specify the Operational Design Domain within which the autonomous system is designed to operate. The ODD specification shall satisfy the following requirements.

4.1 Boundary Specification

- The ODD shall be defined with quantitative boundaries that are machine-readable and enforceable at runtime.
- Each boundary parameter shall include: parameter name, data type, permissible range or enumerated values, and units of measurement where applicable.
- Boundary parameters may be adaptive (auto-discovered by the Interlock during operational observation) or prescriptive (explicitly declared by the operator prior to deployment).
- The ODD specification shall be complete — any operational condition not explicitly included in the ODD is outside the declared domain.

4.2 Sufficiency Review

Prior to CAT-72 initiation, Sentinel Authority shall conduct a Pre-CAT-72 Audit Control Review to verify that the ODD specification meets minimum sufficiency requirements. Systems that do not meet the audit threshold shall be returned to the applicant with documented findings.

Sufficiency criteria include but are not limited to: completeness of boundary enumeration, consistency between declared boundaries and enforcement configuration, and telemetry coverage of all declared boundary parameters.

4.3 Extended Verification

Higher-risk operational domains may require extended verification periods beyond the minimum 72 cumulative hours, as determined during the Pre-CAT-72 Audit Control Review. Risk classification shall be based on the operational domain, consequence severity of boundary exceedance, and the degree of human-system interaction within the declared ODD.

5. ENVELO Enforcement Architecture Requirements

ODDC conformance requires the presence and correct operation of an ENVELO-compliant runtime enforcement interlock. The interlock shall satisfy the following architectural requirements.

5.1 Non-Bypassability

The ENVELO Interlock shall be architecturally non-bypassable. No software command, configuration change, or operator action shall be capable of disabling, circumventing, or modifying enforcement behavior during certified operation. Removal or disablement of the Interlock shall automatically invalidate the associated ODDC certificate.

5.2 Tiered Enforcement Response

The Interlock shall implement a tiered enforcement architecture:

- **Self-correction zone:** System approaches ODD boundary. Interlock monitors; system self-corrects.
- **Enforcement margin:** System enters enforcement margin. Interlock actively constrains operation to prevent boundary exceedance.

- **Minimum Risk Condition:** System exceeds or threatens to exceed ODD boundary. Interlock transitions system to predefined MRC.
- **Hard halt:** System contacts ENVELO wall (absolute boundary). Interlock halts autonomous execution.

5.3 Fail-Closed Behavior

The Interlock shall exhibit fail-closed behavior. In the event of Interlock failure, communication loss, or inability to determine enforcement state, the system shall transition to MRC. No autonomous operation shall be permitted in the absence of confirmed Interlock enforcement.

5.4 Heartbeat and Liveness

The Interlock shall transmit periodic heartbeat signals at intervals not exceeding 30 seconds during active operation. A system shall be considered offline if no heartbeat is received within 120 seconds of the last transmission. Offline status during an active CAT-72 test shall pause the cumulative enforcement clock.

6. Telemetry and Audit Chain Requirements

6.1 Enforcement Telemetry

The Interlock shall record all enforcement events including: boundary approaches, enforcement interventions, MRC transitions, hard halts, heartbeats, and any modification to enforcement configuration. Each event shall include a timestamp, event type, affected boundary parameter(s), and enforcement action taken.

6.2 Hash Chain Integrity

Enforcement telemetry shall be recorded in a tamper-evident, cryptographically linked audit chain. Each record shall include a cryptographic hash of the preceding record, forming a sequential chain. Any gap, reorder, or modification in the chain shall be computationally detectable and shall be flagged during conformance review.

6.3 Telemetry Provenance

ODDC verifies enforcement behavior against telemetry as received by the Interlock. The operator bears sole responsibility for the accuracy, calibration, and integrity of sensor data entering the ENVELO Interlock. ODDC does not verify the truthfulness of underlying sensor inputs. Telemetry trust classification and sensor provenance are outside the scope of this specification.

> ***Operator Responsibility.*** *Sentinel Authority verifies that enforcement was maintained based on telemetry records. The accuracy of the telemetry source — including sensor calibration, data pipeline integrity, and environmental measurement — is the sole responsibility of the system operator.*

7. Conformance Authorization Test (CAT-72)

The Conformance Authorization Test (CAT-72) is the structured verification protocol used to evaluate runtime boundary integrity prior to ODDC conformance determination.

7.1 Duration

CAT-72 requires a minimum of 72 cumulative hours of autonomous operation under active interlock enforcement within the declared ODD. Cumulative means the enforcement clock counts only active operational time — it pauses when the system is idle, powered down, or not operating within the declared ODD. Higher-risk operational domains may require extended verification periods as determined during the Pre-CAT-72 Audit Control Review.

7.2 Evaluation Criteria

During the verification period, the following shall be evaluated:

- **Sustained enforcement exposure:** The Interlock shall remain active and enforcing for the entire cumulative verification period.
- **Boundary stress evaluation:** The system shall demonstrate tiered enforcement response at defined tolerance thresholds.
- **Telemetry integrity:** The cryptographic audit chain shall be complete and unbroken across all operational intervals.

- **Convergence score:** The quantitative measure of boundary adherence shall meet or exceed the conformance threshold.

7.3 Conformance Threshold

The minimum convergence score for ODDC conformance is **0.9500 (95%)**. Systems scoring below this threshold shall not receive a conformance determination. The convergence score is computed as the aggregate measure of boundary adherence across all declared ODD parameters over the cumulative verification period.

7.4 Detailed Procedure

Detailed test procedures, including phase definitions, telemetry ingestion requirements, and evidence chain specifications, are defined in the CAT-72 Conformance Authorization Test Procedure (CAT-72-PROC).

8. Conformance Determination Criteria

Upon completion of the CAT-72 verification period, Sentinel Authority independently reviews telemetry records, validates audit chain integrity, and evaluates conformance against the requirements of this specification. A conformance determination shall require:

- Convergence score ≥ 0.9500
- Complete and unbroken cryptographic audit chain
- No unresolved Interlock failures during the verification period
- Successful Pre-CAT-72 Audit Control Review on record
- ODD specification meeting sufficiency requirements (Section 4)
- ENVELO Interlock meeting architectural requirements (Section 5)

Conformance determinations are recorded in the public ODDC registry and are independently verifiable by certificate identifier.

9. Conformance Gates

ODDC conformance is structured through five sequential gates. Each gate shall be satisfied before proceeding to the next.

Gate	Name	Requirement
01	ODD Specification	Formal specification of operational boundaries with quantitative, enforceable parameters.
02	Sustained Verification	≥72 cumulative hours of enforced operation within the declared ODD under active Interlock enforcement.
03	Enforcement Architecture	ENVELO Interlock deployed, non-bypassable, with tiered response and fail-closed behavior verified.
04	Evidence Integrity	Tamper-evident cryptographic audit chain complete across all operational intervals.
05	Drift and Revocation	Ongoing monitoring for conformance drift. Deviation beyond threshold triggers suspension or revocation.

10. Certificate Lifecycle

10.1 Issuance

Upon successful conformance determination, Sentinel Authority shall issue an ODDC certificate recorded in the public registry. The certificate shall include: certificate identifier, system identification, declared ODD summary, convergence score, issuance date, expiration date, and evidence chain hash.

10.2 Validity Period

ODDC certificates are valid for twelve (12) months from the date of issuance, subject to continuous Interlock enforcement and annual maintenance fee. Streamlined renewal (≥48 cumulative enforcement hours) may be available for applicants with clean conformance history and no system modifications.

10.3 Continuous Enforcement

Between conformance determinations, the ENVELO Interlock shall remain active and enforcing. Sentinel Authority does not monitor live telemetry — it periodically verifies that enforcement was maintained. Removal or disablement of the Interlock automatically invalidates the associated ODDC certificate.

10.4 Fee Schedule

Item	Amount
Conformance Assessment (Pre-CAT-72 Review + CAT-72 + Certificate)	$12,000 per system
Annual Maintenance (surveillance + registry + renewal)	$12,000 per system/year

11. Suspension, Revocation, and Appeals

11.1 Conformance Monitoring

Post-certification, the Interlock continues to enforce boundaries and log telemetry. Drift detection is automated. If the system's convergence score falls below the conformance threshold of 0.9500, the following process applies:

- **Below 95%:** 30-day correction window. Interlock remains active. Operator is notified with findings.
- **Not corrected within 30 days:** Certificate is suspended. Retest (new CAT-72) is required.
- **Interlock removed or disabled:** Immediate certificate invalidation. Recorded in public registry.

11.2 Revocation

Revocation is permanent and recorded in the public ODDC registry. Revocation history is accessible to any party and is maintained indefinitely. A revoked certificate cannot be reinstated — the operator must apply for a new conformance determination.

11.3 Appeals

Certificate suspension includes written notification with findings, a defined response period, independent review of submitted evidence, and a final determination recorded in the public registry. The appeals process is structurally independent from the original conformance determination.

12. Governance and Independence

ODDC is a published conformance standard. Sentinel Authority certifies against that standard — it does not own, control, or define conformance outcomes. The following governance requirements apply.

12.1 Structural Separation

The ODDC standard (this specification) is structurally separate from the certifying body (Sentinel Authority). Conformance outcomes are determined by the requirements of this specification, not by the certifier's discretion.

12.2 Auditor Independence

Conformance reviewers shall be structurally separated from business development and applicant-facing operations. No individual involved in a conformance determination shall have a financial interest in its outcome.

12.3 Conflict of Interest

Sentinel Authority shall hold no equity in, advisory relationship with, or revenue-sharing arrangement with any applicant or certified operator. Fees are fixed and non-contingent on outcome.

12.4 Public Record

All specification revisions, conformance determinations, suspensions, revocations, and governing documents are publicly archived and accessible without restriction.

13. Explicit Exclusions

ODDC explicitly does not constitute, and shall not be represented as:

- **Functional Safety Validation.** ODDC does not evaluate the adequacy or safety of declared ODD limits.
- **AI Model Evaluation.** ODDC does not evaluate model architecture, training data, or decision logic.
- **Performance Certification.** ODDC does not certify system performance, accuracy, or reliability beyond boundary adherence.
- **Cybersecurity Certification.** ODDC does not evaluate cybersecurity posture or vulnerability.
- **Regulatory Approval.** ODDC does not constitute regulatory approval, licensure, or authorization to operate in any jurisdiction. Operators are solely responsible for obtaining all required regulatory approvals.

14. Versioning and Revision Policy

This specification is versioned and publicly documented. Revisions are subject to independent technical review prior to adoption. The following revision policy applies:

- Major revisions (e.g., v1.0 → v2.0) require independent technical review and a minimum 60-day public comment period.
- Minor revisions (e.g., v1.0 → v1.1) may be issued for clarification, correction, or non-substantive changes.
- All revisions are publicly archived with full change documentation.
- Active ODDC certificates issued under a prior specification version remain valid until their expiration date.

Appendix A — Conformance Threshold Summary

Parameter	Threshold	Notes
Convergence Score	≥ 0.9500 (95%)	Minimum for conformance determination
CAT-72 Duration	≥ 72 cumulative hours	Minimum enforcement exposure; may be extended for higher-risk domains
Heartbeat Interval	≤ 30 seconds	Maximum interval between Interlock heartbeats
Offline Threshold	120 seconds	System considered offline; enforcement clock paused
Correction Window	30 days	Period to restore conformance before suspension
Certificate Validity	12 months	Subject to continuous enforcement and annual maintenance
Renewal CAT Duration	≥ 48 cumulative hours	Streamlined renewal for clean history
Audit Chain	100% integrity	No gaps, reorders, or modifications permitted

End of ODDC-STD-1.0 — ODDC Standard Specification — v1.0