ODDC Certification Guide

Complete Process Guide

Version 5.0 — February 2026 — Confidential

ODDC (Operational Design Domain Conformance) provides independent, third-party attestation that autonomous systems operate within formally declared boundaries with non-bypassable enforcement. This document is the complete guide to obtaining ODDC certification — from initial inquiry through continued monitoring. No proprietary data required. The Interlock observes your system in normal operation, auto-discovers operational boundaries, then enforces them across 72 cumulative hours of active operation. Your IP stays yours — we certify the process, not the parameters.

Field	Details
Document	ODDC Certification Guide v5.0
Classification	Confidential — Applicant Distribution
Effective Date	February 2026
Specification	ODDC v1.0 — Effective January 2026
Owner	Sentinel Authority — Conformance Operations
Contact	conformance@sentinelauthority.org

Independent conformance determination. Sentinel Authority is not a regulator. This document does not constitute legal advice. ODDC does not attest safety, compliance, cybersecurity, or performance.

1.1 Purpose

ODDC certification is an independent determination that an autonomous system has verifiable, enforceable runtime boundary controls. The certification is built on three pillars: the ENVELO Interlock auto-discovers operational boundaries from live telemetry (or the applicant specifies them); the Interlock enforces every parameter at runtime with a three-tier enforcement model; and the CAT-72 test generates a cryptographic, tamper-evident record proving 72 cumulative hours of in-bounds operation across active operational intervals.

IP Protection: No proprietary data is required. Your ODD specifications, model weights, source code, and decision logic are never shared with Sentinel Authority. We certify the process, not the parameters.

1.2 Framework 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 ensuring the system cannot operate outside declared ODD boundaries.
CAT-72	Conformance Authorization Test — 72 cumulative hours of active operation demonstrating bounded operation and enforcement effectiveness. Clock counts only during active operation; pauses when system is idle or powered down.

1.3 Certification Paths

Path	How ODD Is Established	Best For
Adaptive (default)	Interlock auto-discovers boundaries from operational telemetry during OBSERVE phase. Operator reviews and approves.	Systems where operators prefer not to share proprietary ODD specifications
Prescriptive	Applicant submits a complete ODD specification with quantitative boundaries.	Systems with well-documented, pre-existing ODD specifications

1.4 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

2.1 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 cumulative hours of CAT-72 testing across active operational intervals.
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. The audit chain is uninterrupted across all active operational intervals.

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

The conformance process follows seven phases:

Phase	Duration	Owner	Key Deliverable
1. Inquiry & Eligibility	1–2 weeks	Applicant	System overview, eligibility confirmation
2. Formal Application	1 week	Applicant	Application, tolerances, signed agreement
3. ODD Specification Review	5–10 days	Sentinel	ODD acceptance or revision requests
4. ENVELO Deployment + Boundary Review	< 1 hour + 1–2 days	Applicant + Sentinel	Interlock active, boundaries admin-approved, portal green
5. CAT-72 Execution	72 cumulative hours min	Automated	72-hour evidentiary telemetry record
6. Determination & Attestation	1–2 weeks	Sentinel	Certificate, report, registry entry
7. Continued Monitoring	Ongoing	Both	Annual review, continuous enforcement

3.1 Phase 1: Inquiry & Eligibility

Initial contact with Sentinel Authority to determine whether your autonomous system is a candidate for ODDC certification.

- System makes autonomous decisions that affect physical or operational outcomes
- System has a definable Operational Design Domain with measurable boundary parameters
- System has sensors, APIs, or telemetry endpoints for each ODD parameter
- Applicant has authority to deploy an enforcement interlock into the runtime environment

Outcome: Eligibility confirmed. Applicant proceeds to formal application.

3.2 Phase 2: Formal Application

Deliverable	Format	Notes
ODDC Application Form	Portal submission	System identity, version, architecture overview
ODD Specification	Template or adaptive	Quantitative boundaries — or let the Interlock discover them
Tolerance Specification	Template (provided)	Acceptable deviation ranges per parameter
System architecture diagram	PDF or image	Model inputs, outputs, decision paths, actuator connections
Signed Conformance Agreement	Digital signature	Terms, fees ($15,000 base), timeline acknowledgment

Note: Tolerance specifications are locked at submission and cannot be amended during testing.

3.3 Phase 3: ODD Specification Review

Sentinel conducts an independent review of the Operational Design Domain — whether auto-discovered by the Interlock or submitted by the applicant — to verify it is complete, internally consistent, measurable, and enforceable.

- Each ODD parameter for measurability and precision
- Tolerance specifications for internal consistency
- All boundaries can be monitored by the ENVELO Interlock at runtime
- Three-tier enforcement thresholds are properly calibrated

Outcome: Accepted ODD specification. This becomes the binding reference document. No changes after acceptance.

The ENVELO Interlock is deployed into the system's runtime environment — outbound-only, non-bypassable. In adaptive mode, the Interlock enters OBSERVE phase, learning operational boundaries from live telemetry before enforcement begins.

3.4.1 Security Architecture

Guarantee	Detail
Zero Listening Ports	Interlock opens no inbound ports. Only outbound HTTPS to api.sentinelauthority.org.
Customer Controlled	Applicant deploys, configures, and terminates. Sentinel cannot start, stop, or modify remotely.
TLS 1.3 + Pinning	All communications encrypted with certificate pinning. Data encrypted at rest.
Your ODD Stays Yours	Source code, model weights, and decision logic are never accessed. Only operational telemetry is transmitted.
No PHI/PII	No personally identifiable information transmitted. HIPAA/BAA compatible.

3.4.2 System Requirements

Requirement	Specification
Operating System	Linux (Ubuntu 20.04+, RHEL 8+, Debian 11+), macOS 12+, Windows Server 2019+
Python	3.7 or higher
CPU / RAM	2 cores minimum / 512 MB minimum for ENVELO Interlock
Disk	1 GB for Interlock + logs; 10 GB recommended for CAT-72 retention
Network	Outbound HTTPS (port 443) to api.sentinelauthority.org
Clock	NTP-synchronized; accurate to +/–1 second

3.4.3 Installation

```
curl -sSL https://get.sentinelauthority.org | bash
```

The installer prompts for your Certificate ID and API Key (visible in the portal). It automatically connects, validates credentials, scans for telemetry sources, matches sources to ODD parameters, and installs the ENVELO CLI.

Validate: `envelo validate`

Start daemon: `envelo start -d`

Check status: `envelo status`

3.4.4 Admin Boundary Review (Adaptive Path)

After OBSERVE phase completes, Sentinel's Conformance Engineer reviews auto-detected boundaries before CAT-72 begins.

Step	Owner	Description
1. OBSERVE complete	Interlock	Boundaries auto-detected and submitted to Sentinel portal.

2. Admin review	Sentinel	Conformance Engineer reviews boundaries. Typically 1–2 business days.
3. Boundary approval	Sentinel	Admin approves. System transitions from OBSERVE to BOUNDED.
4. CAT-72 authorized	Sentinel	Admin authorizes test. Portal activates "Begin Test" button.
5. Test starts	Applicant	Operator initiates CAT-72. Cumulative 72-hour clock begins.

Note: CAT-72 cannot begin until admin has reviewed and approved the auto-detected boundaries.

Outcome: Interlock active, boundaries admin-approved, portal green. Ready for CAT-72.

The Conformance Authorization Test (CAT-72) is the evidentiary phase, building a cryptographic record of in-bounds operation across active operational intervals. The CAT-72 clock measures 72 cumulative hours of active operation — it pauses when the system is idle, powered down, parked, or between operational shifts.

Note: "Uninterrupted" in the CAT-72 specification refers to the audit chain and cryptographic record — the record must not gap during active operation. It does not mean the system must operate non-stop.

#	Phase	Description
01	Cumulative Enforcement Demo	72 cumulative hours of active operation across intervals. Clock pauses during idle/off periods.
02	Boundary Stress Testing	Stress testing across limits. ENVELO decelerates to Minimum Risk Condition before the wall.
03	Enforcement Proof	Verified tiered response: self-correction (Tier 1), MRC (Tier 2), hard halt at ENVELO Wall (Tier 3).

3.5.1 Pass/Fail Criteria

- Zero Tier 3 (ENVELO Wall) violations during the cumulative 72-hour window
- Tier 2 violations must trigger successful MRC within specified time
- Uninterrupted audit chain — no gaps in the cryptographic telemetry record during active operation
- All parameters must report data across all active operational intervals

Outcome: 72 cumulative hours of evidentiary telemetry record, cryptographically sealed.

3.6 Phase 6: Determination & Attestation

Sentinel's Conformance Engineers independently analyze the CAT-72 evidentiary record against the accepted ODD specification.

- ODDC Certificate with unique certificate number (ODDC-YYYY-NNNNN)
- Conformance Assessment Report detailing all findings
- Public registry entry at registry.sentinelauthority.org
- Digital badge and certificate assets for marketing use

Outcome: ODDC certificate issued. System enters CONFORMANT state. Listed in public Conformance Registry.

3.7 Phase 7: Continued Monitoring

ODDC certification is not a point-in-time assessment. The ENVELO Interlock continues operating after certification.

- ENVELO Interlock must remain active and reporting
- Annual conformance review ($12,000/year)
- Changes to system architecture, ODD parameters, or firmware require re-assessment

Certificate may be suspended or revoked if the Interlock is disabled, material violations are detected, the annual review fee is not paid, or material system changes are made without re-assessment.

Outcome: Continuous conformance enforcement. Certificate active as long as Interlock runs and annual reviews are completed.

#	Gate	Requirement	Description
01	ODD	Auto-Discovered	Operational boundaries discovered from live telemetry, or specified by applicant
02	STABLE	Enforcement Verified	72 cumulative hours of enforced operation within discovered/specified bounds
03	ENVELO	Enforcement Active	Non-bypassable runtime enforcement at all times
04	AUDIT	Tamper-Evident	Cryptographic records of every enforcement check; uninterrupted audit chain during active operation
05	REVOKE	Drift Protocol	Clear suspension path when boundaries are exceeded

4.1 Conformance States

State	Meaning
OBSERVE	Interlock deployed, learning operational boundaries from telemetry. No enforcement yet.
BOUNDED	Boundaries established and enforcement active. CAT-72 in progress or pending.
CONFORMANT	Full conformance. Certificate active. Continuous enforcement and monitoring.
PAUSED	Under review. Boundary exceedance detected or material system change.

ENVELO enforces boundaries using a three-tier model. Approach triggers self-correction. Breach forces Minimum Risk Condition. Wall contact halts execution.

Tier	Name	Trigger	Action
1	Advisory (Self-Correction)	Approaching ODD boundary (within tolerance)	System self-corrects. Log warning, notify dashboard.
2	ODD Breach (MRC)	Parameter exceeds ODD boundary	Trigger Minimum Risk Condition. Decelerate to safe state within specified time.
3	ENVELO Wall (Hard Halt)	Parameter exceeds hard limit	Immediate actuation block. Non-bypassable, non-configurable, instant.

Note: Tier 3 violations during CAT-72 result in automatic test failure.

Fee	Amount	When
Conformance Assessment	$15,000	Due at application — covers ODD review, CAT-72 execution, certificate issuance. Non-refundable.
Annual Maintenance	$12,000/year	Begins at certificate issuance — continuous monitoring, registry maintenance, annual review.
Enterprise	Custom	Volume pricing, dedicated support — contact conformance@sentinelauthority.org

All fees USD. Base rates. Non-refundable. Request a quote at conformance@sentinelauthority.org.

Boundaries are stored in Sentinel Authority's database and fetched by the ENVELO Interlock at startup. In adaptive mode, boundaries are auto-discovered from operational telemetry and stored after operator approval.

Field	Type	Description
name	string	Human-readable parameter name
parameter	string	System identifier for the parameter
min_value / max_value	number	ODD bounds (inclusive)
hard_limit	number	ENVELO Wall threshold (Tier 3)
unit	string	Unit of measurement
tolerance	number	Acceptable measurement tolerance (+/–)

- Geographic: Circle (center + radius), Polygon (ordered vertices), Altitude (min/max meters)
- Temporal: Allowed operating hours, allowed days of week, timezone
- State: Allowed values list, forbidden values list

The ENVELO CLI is the single interface for all Interlock operations. Installed automatically by the one-command installer.

8.1 Running

Command	Description
`envelo start [-d]`	Start enforcement (foreground or daemon)
`envelo stop`	Stop running Interlock
`envelo restart`	Stop and restart
`envelo validate`	Pre-flight configuration check

8.2 Monitoring

Command	Description
`envelo status`	Full health check (Interlock, API, TLS, sources)
`envelo monitor`	Live terminal dashboard
`envelo events`	Violation and enforcement history
`envelo logs [-f]`	View or follow Interlock logs
`envelo cat72`	CAT-72 cumulative test status and progress

8.3 Boundaries & Sources

Command	Description
`envelo boundaries`	Show all enforced boundary definitions
`envelo resync`	Force re-fetch boundaries from Sentinel Authority
`envelo simulate`	Dry-run a boundary check (shows tier result)
`envelo test`	Test all telemetry source connections
`envelo rediscover [--all]`	Re-scan environment for telemetry sources

8.4 Infrastructure

Command	Description
`envelo service install`	Auto-start on boot (systemd / launchd)
`envelo docker`	Generate Docker deployment files
`envelo k8s`	Generate Kubernetes deployment files

`envelo diagnose`	Generate support bundle (redacted, safe to send)
`envelo export`	Auditor-ready boundary and config bundle
`envelo update`	Self-update
`envelo rollback`	Uninstall ENVELO (suspends conformance)

Document	Version	Description
ENVELO Requirements	v3.0	Runtime enforcement requirements specification
CAT-72 Procedure	v4.0	Conformance Authorization Test requirements and format
ODDC Overview	v3.0	Framework overview for regulators and evaluators
ODDC Scenarios	v3.0	Sector-specific implementation guidance
Conformance Agreement	Current	Terms and conditions for conformance determination

— End of Document —