ODDC Certification Guide

Operational Design Domain Conformance — Complete Process Guide

Version 3.0 • February 2026 • Confidential

Disclaimer

Independent conformance determination. Sentinel Authority is not a regulator. This document does not constitute legal advice. Implementations remain the responsibility of operators and licensed implementers. ODDC does not attest safety, compliance, cybersecurity, or performance.

Contents

1. Introduction

This document is the complete guide to obtaining ODDC (Operational Design Domain Conformance) certification from Sentinel Authority. It covers every phase of the certification process from initial inquiry through continued monitoring, with particular detail on ENVELO agent deployment and CAT-72 test execution.

ODDC certification proves that an autonomous system operates exclusively within its declared Operational Design Domain. The certification is built on three pillars: the applicant declares a precise ODD; the ENVELO enforcement agent monitors every declared parameter at runtime with a three-tier enforcement model; and the CAT-72 test generates a cryptographic, tamper-evident record proving 72 continuous hours of in-bounds operation.

Version 3.0 of this guide reflects the introduction of the ENVELO CLI, which consolidates all agent functionality into a single command-line tool. Deployment, monitoring, diagnostics, and infrastructure management are now handled entirely through the `envelo` command.

Who This Document Is For

- Engineering teams responsible for deploying the ENVELO agent and configuring telemetry
- Product and compliance leaders managing the certification timeline
- Executives evaluating ODDC as a trust and safety differentiator
- Legal and regulatory affairs teams preparing for autonomous systems oversight

2. Certification at a Glance

ODDC certification takes approximately 6–10 weeks from first contact to certificate issuance. The base assessment fee is $12,000 per system, with $6,000 annual maintenance.

Phase	Duration	Owner	Key Deliverable
1. Inquiry & Eligibility	1–2 weeks	Applicant	System overview, eligibility confirmation
2. Formal Application	1 week	Applicant	Application, ODD spec, tolerances, agreement
3. ODD Specification Review	2–3 weeks	Sentinel	ODD acceptance or revision requests
4. ENVELO Deployment	< 1 hour	Applicant	Agent active, pre-flight passed, portal green
5. CAT-72 Execution	72 hours min	Automated	72h evidentiary telemetry record
6. Determination	1–2 weeks	Sentinel	Certificate, report, registry entry
7. Continued Monitoring	Ongoing	Both	Annual review, continuous enforcement

Note: Phase 4 deployment time has been reduced from 1–2 weeks to under 1 hour with the one-command installer and ENVELO CLI.

3. Phase 1 — Inquiry & Eligibility

Duration: 1–2 weeks | Primary: Applicant

Initial contact with Sentinel Authority to determine whether your autonomous system is a candidate for ODDC certification. This is a low-commitment, informational phase.

Eligibility Criteria

- 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 agent into the runtime environment

Outcome:
Eligibility confirmed. Applicant proceeds to formal application.

4. Phase 2 — Formal Application

Duration: 1 week | Primary: Applicant

The formal application establishes the scope, boundaries, and technical profile of the system under assessment. This is the binding document Sentinel uses to structure the entire certification.

Deliverables

Deliverable	Format	Notes
ODDC Application Form	Portal submission	System identity, version, architecture overview
ODD Specification	Template (provided)	Quantitative boundaries: geospatial, temporal, environmental, behavioral
Tolerance Declaration	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 ($12,000 base), timeline acknowledgment

Note: Tolerance declarations are locked at submission. They define the pass/fail criteria for CAT-72 and cannot be amended during testing.

Outcome:
Accepted application with assigned Case ID (ODDC-YYYY-NNNNN). Sentinel assigns a Conformance Engineer.

5. Phase 3 — ODD Specification Review

Duration: 2–3 weeks | Primary: Sentinel

Sentinel conducts an independent review of your declared Operational Design Domain to verify it is complete, internally consistent, measurable, and enforceable by ENVELO.

What Sentinel Reviews

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

Common Review Findings

- Boundary parameters too vague to enforce (e.g., “normal operating conditions”)
- Missing environmental or temporal constraints
- Tolerances that conflict with declared ODD boundaries
- Subsystems excluded from scope that affect boundary behavior

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

6. Phase 4 — ENVELO Deployment

Duration: < 1 hour | Primary: Applicant

The ENVELO enforcement agent is deployed into your system's runtime environment. ENVELO monitors all declared ODD boundary parameters in real time and enforces fail-closed behavior on any violation. With the v2.0 one-command installer and ENVELO CLI, deployment typically takes under 10 minutes.

6.1 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	2 cores minimum
RAM	512 MB minimum for ENVELO agent
Disk	1 GB for agent + logs; 10 GB recommended for CAT-72 retention
Network	Outbound HTTPS (port 443) to api.sentinelauthority.org
Clock	NTP-synchronized; accurate to ±1 second

6.2 Security Model

- **Outbound only:** ENVELO opens zero inbound ports on your network.
- **No remote access:** Sentinel cannot access your system, network, or data.
- **No commands from Sentinel:** The connection is one-way: telemetry out, nothing in.
- **No PHI/PII:** Only ODD parameter values are transmitted. No business data.
- **Signed telemetry:** Every packet is cryptographically signed and hash-chain linked.
- **Fail-closed:** If the connection drops, the agent blocks all actions (safe state).

6.3 Step 1: Install

Open a terminal on the target system and run:

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

The installer prompts for your Certificate ID and API Key (both visible in the Sentinel Authority portal under the ENVELO Agent tab). It then automatically:

- Connects to Sentinel Authority and validates credentials
- Downloads approved boundary definitions (you never edit these)
- Scans your system for telemetry sources (MQTT, HTTP/REST, Prometheus, gRPC, ROS2, file sensors)
- Matches discovered sources to ODD parameters using confidence-based fuzzy matching

- Writes the configuration file and installs the ENVELO CLI

Note: The installer requires zero external dependencies. It uses only Python standard library modules.

6.4 Step 2: Validate

Before starting enforcement, verify your configuration:

```
envelo validate
```

This checks API credentials, certificate verification, source mappings, source reachability, and fail-closed mode. If any parameters are unmapped, run:

```
envelo rediscover
```

This re-scans your environment and prompts for any sources it cannot auto-detect.

6.5 Step 3: Start

Start ENVELO enforcement:

```
envelo start
```

For production deployment, run as a background daemon:

```
envelo start -d
```

For auto-start on boot (recommended for CAT-72):

```
envelo service install
```

This installs ENVELO as a systemd service (Linux), LaunchAgent (macOS), or provides NSSM instructions (Windows).

6.6 Step 4: Verify in Portal

- Navigate to app.sentinelauthority.org
- Open your case → ENVELO Agent tab
- Verify agent shows “Active” status
- Review boundary list — all parameters should show green
- Proceed to CAT-72 tab and click “Begin Test” when ready

Note: The 72-hour CAT-72 timer starts immediately when you click Begin Test. Ensure your system is running in its normal operational environment before starting.

6.7 Alternative Deployment

Docker

```
envelo docker
cd envelo-docker && docker compose up -d
```

Kubernetes

```
envelo k8s
kubectl apply -f envelo-k8s.yaml
```

SDK Integration

```
from envelo import EnveloAgent, EnveloConfig
agent = EnveloAgent(EnveloConfig(
api_key='sa_live_...', certificate_number='ODDC-2026-XXXXX'))
agent.start()

@agent.enforce
def move_robot(speed, position):
motors.actuate(speed, position)
```

Outcome:

Agent active, all boundaries enforced, portal showing green status. Ready for CAT-72.

7. Phase 5 — CAT-72 Execution

Duration: 72 hours minimum | Primary: Automated

The Conformance Assessment Test over 72 hours (CAT-72) is the evidentiary phase. The ENVELO agent streams telemetry to Sentinel Authority, building a cryptographic record of continuous in-bounds operation.

What Happens During CAT-72

- Every declared ODD parameter is sampled at its configured poll interval
- Each sample is evaluated against the three-tier enforcement model
- Telemetry is hash-chain linked, timestamped, and signed
- Any boundary violation triggers immediate enforcement action and is logged
- The 72-hour clock runs continuously with no pause

Monitoring During CAT-72

```
envelo cat72 # Check test progress and timer
envelo monitor # Live terminal dashboard
envelo events # View enforcement events
envelo boundaries # Verify all boundaries
```

Pass/Fail Criteria

- Zero Tier 3 (ENVELO Wall) violations during the 72-hour window
- Tier 2 violations must trigger successful MRC within defined time
- Continuous telemetry coverage — no gaps exceeding maximum allowed interval
- All declared parameters must report data for the full 72 hours

Note: If CAT-72 fails, your Conformance Engineer provides a detailed failure report. Re-attempts are included in the base certification fee.

Outcome:

72-hour evidentiary telemetry record, cryptographically sealed.

8. Phase 6 — Determination & Attestation

Duration: 1–2 weeks | Primary: Sentinel

Sentinel's Conformance Engineers independently analyze the CAT-72 evidentiary record. Every data point is verified against the accepted ODD specification.

Deliverables

- ODDC Certificate with unique certificate number
- 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 listed in the public Conformance Registry.

9. Phase 7 — Continued Monitoring

Duration: Ongoing | Primary: Both

ODDC certification is not a point-in-time assessment. The ENVELO agent continues operating after certification, providing continuous runtime enforcement and telemetry.

Ongoing Requirements

- ENVELO agent must remain active and reporting
- Annual conformance review ($6,000/year)
- Changes to system architecture, ODD parameters, or firmware require re-assessment
- Sentinel may request supplementary testing if material changes are detected

Certificate Revocation

A certificate may be suspended or revoked if the ENVELO agent 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 agent runs and annual reviews are completed.

A. Appendix A — Boundary Specification Format

Boundaries are stored in Sentinel Authority's database and fetched by the ENVELO agent at startup. The applicant never edits boundary definitions directly.

Numeric Boundaries

Field	Type	Description
name	string	Human-readable parameter name (e.g., 'vehicle_speed')
parameter	string	System identifier for the parameter
min_value	number	ODD lower bound
max_value	number	ODD upper bound
hard_limit	number	ENVELO Wall threshold (Tier 3)
unit	string	Unit of measurement
tolerance	number	Acceptable measurement tolerance (±)

Geographic Boundaries

- Circle: center (lat/lon) + radius in meters
- Polygon: ordered list of vertices
- Altitude: min/max altitude in meters

Time Boundaries

- Allowed operating hours (start_hour, end_hour)
- Allowed days of week
- Timezone specification

State Boundaries

- Allowed values: list of permitted system states
- Forbidden values: list of prohibited states

B. Appendix B — ENVELO CLI Reference

The ENVELO CLI is the single interface for all agent operations. Installed automatically by the one-command installer. Available as the `envelo` command.

Running

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

Monitoring

Command	Description
envelo status	Full health check (agent, API, TLS, sources)
envelo monitor	Live terminal dashboard (refreshes every 2s)
envelo events	Violation and enforcement history
envelo logs [-f]	View or follow agent logs
envelo cat72	CAT-72 test status and progress

Boundaries

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)

Telemetry Sources

Command	Description
envelo test	Test all telemetry source connections
envelo rediscover [--all]	Re-scan environment for telemetry sources
envelo benchmark	Measure enforcement check latency

Infrastructure

Command	Description
envelo service install	Auto-start on boot (systemd / launchd)
envelo service uninstall	Remove system service
envelo docker	Generate Dockerfile + docker-compose.yml
envelo k8s	Generate Kubernetes DaemonSet + Secret

Maintenance

Command	Description
envelo diagnose	Generate support bundle (redacted, safe to send)
envelo network	Full network diagnostic (DNS, TLS, latency, proxy)
envelo export	Auditor-ready boundary and config bundle
envelo rotate-key	Rotate API key
envelo update	Self-update
envelo rollback	Uninstall ENVELO (suspends conformance)

C. Appendix C — Three-Tier Enforcement Model

ENVELO enforces boundaries using a three-tier model that provides graduated response from advisory warnings through hard actuation blocks.

Tier	Name	Trigger	Action
1	Advisory	Approaching ODD boundary (within tolerance)	Log warning, notify dashboard
2	ODD Breach	Parameter exceeds declared ODD boundary	Trigger Minimum Risk Condition (MRC)
3	ENVELO Wall	Parameter exceeds hard limit	Immediate actuation block (non-bypassable)

Tier 1: Advisory

The system is operating within its ODD but approaching a boundary. ENVELO logs an advisory event and updates the dashboard. No enforcement action is taken.

Tier 2: ODD Breach

A declared ODD boundary has been exceeded. ENVELO triggers the system's Minimum Risk Condition (MRC) — a pre-defined safe state configured during Phase 3. The MRC must complete within a declared time window.

Tier 3: ENVELO Wall

The hard limit has been reached. ENVELO directly blocks the actuator command. Non-bypassable, non-configurable, instant. The protected code never executes.

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

Simulate Enforcement

Use the CLI to test how a specific value would be evaluated:

```
envelo simulate vehicle_speed 28
# PASS: 28 within ODD [0 - 30] (Tier 1 advisory zone)

envelo simulate vehicle_speed 32
# VIOLATION: 32 > max 30 (Tier 2: MRC triggered)

envelo simulate vehicle_speed 40
# VIOLATION: 40 > wall 35 (Tier 3: HARD HALT)
```

. Glossary

CAT-72 — Conformance Assessment Test over 72 hours. The evidentiary phase proving continuous in-bounds operation.

Conformance Engineer — The Sentinel Authority engineer assigned to a certification case.

ENVELO — Enforced Non-Violable Execution-Limit Override. The runtime enforcement agent.

ENVELO CLI — Command-line interface for all agent operations.

ENVELO Wall — Tier 3 hard limit. Directly blocks actuation. Non-bypassable.

MRC — Minimum Risk Condition. The safe state a system must reach when an ODD boundary is exceeded.

ODD — Operational Design Domain. The complete set of conditions under which a system is designed to operate.

ODDC — Operational Design Domain Conformance. The certification.

Sentinel Authority — The certification body that administers ODDC certification.

Three-Tier Enforcement — ENVELO’s graduated response: Advisory, ODD Breach, ENVELO Wall.
