ODDC Certification Guide

Complete Process Guide

February 2026 — Public Document

S E N T I N E L A U T H O R I T Y ODDC Certification Guide Complete Process Guide Formal attestation that autonomous systems operate within their Operational Design Domain — enforced at runtime, verified independently, recorded immutably. No proprietary data required. The Interlock observes your system in normal operation, auto-discovers operational boundaries, then enforces them for 72 hours. Your IP stays yours — we certify the process, not the parameters.

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.

Field	Details
Document	ODDC Certification Guide v4.0

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

Glossary O V E R V I E W 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 Interlock deployment and CAT-72 test execution.

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 continuous hours of in-bounds operation.

IP Protection: No proprietary data is required. The Interlock observes your system in normal operation and auto-discovers operational boundaries. Your ODD specifications, model weights, source code, and decision logic are never shared with Sentinel Authority. We certify the process, not the parameters.

Version 4.0 of this guide reflects the introduction of the ENVELO CLI, which consolidates all Interlock functionality into a single command-line tool, and the adaptive certification path where boundaries are auto- discovered from operational telemetry rather than manually specified.

Who This Document Is For Engineering teams responsible for deploying the ENVELO Interlock 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
- Enterprise procurement teams evaluating AI vendor governance evidence
- Why It Matters ODDC certification solves the governance proof problem that stalls enterprise AI procurement. Enterprise buyers need governance evidence before they sign — ODDC provides independent, auditable proof that your system operates within defined boundaries. When an RFP requires governance documentation, certified vendors pass risk assessments that uncertified competitors cannot.

O V E R V I E W Certification at a Glance

Phase	Duration	Owner	Key Deliverable
1. Inquiry & Eligibility	1–2 weeks	Applicant	System overview, eligibility confirmation
2. Formal Application	1 week	Applicant	Application, tolerances, agreement
3. ODD Review	5–10 days	Sentinel	ODD acceptance or revision requests
4. ENVELO Deployment	< 1 hour	Applicant	Interlock 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

Phase	Duration	Owner	Key Deliverable
7. Continued Monitoring	Ongoing	Both	Annual review, continuous enforcement

Fee Schedule

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

All fees USD. Base rates. Request a quote at conformance@sentinelauthority.org. C O N F O R M A N C E C R I T E R I A Five Gates & Conformance States Five gates. All required for conformance.

#	Gate	Requirement	Description
01	ODD	Auto-Discovered	Operational boundaries discovered from live telemetry, or specified by applicant
02	STABLE	Enforcement Verified	72 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
05	REVOKE	Drift Protocol	Clear suspension path when boundaries are exceeded

Conformance States ● OBSERVE → ● BOUNDED → ● CONFORMANT ■ ● PAUSED

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.

State	Meaning
PAUSED	Under review. Boundary exceedance detected or material system change.

Boundary Exceedance Any state, trajectory, or enforcement failure that exceeds attested tolerances triggers immediate conformance review. The system transitions to PAUSED state until the review is resolved.

P H A S E 1 Inquiry & Eligibility Timeline: 1–2 weeks | Owner: Applicant Initial contact with Sentinel Authority to determine whether your autonomous system is a candidate for ODDC certification.

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 interlock into the runtime environment
- Applicable Verticals Healthcare AI, Clinical Decision Systems, Autonomous Vehicles, Robotics, Enterprise AI, Industrial Automation, Logistics, Energy.

O U T C O M E Eligibility confirmed. Applicant proceeds to formal application.

P H A S E 2 Formal Application Timeline: 1 week | Owner: Applicant The formal application establishes the scope, boundaries, and technical profile of the system under assessment.

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

Deliverables

Deliverable	Format	Notes
ODDC Application Form	Portal submission	System identity, version, architecture overview
ODD Specification	Template (provided) or adaptive	Quantitative boundaries — or let the Interlock discover them
Tolerance Specification	Template (provided)	Acceptable deviation ranges per parameter

Deliverable	Format	Notes
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

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

O U T C O M E Accepted application with assigned Case ID (ODDC-YYYY-NNNNN). Sentinel assigns a Conformance Engineer.

P H A S E 3 ODD Specification Review Timeline: 5–10 days | Owner: Sentinel 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.

What Sentinel Reviews 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
- Common Review Findings Boundary parameters too vague to enforce (e.g., "normal operating conditions")
- Missing environmental or temporal constraints
- Tolerances that conflict with ODD boundaries
- Subsystems excluded from scope that affect boundary behavior
- O U T C O M E Accepted ODD specification. This becomes the binding reference document. No changes after acceptance.

P H A S E 4 ENVELO Interlock Deployment Timeline: < 1 hour | Owner: Applicant The ENVELO Interlock is deployed into your system's runtime environment. Deployed by Sentinel as a runtime interlock on your infrastructure — outbound-only, non-bypassable. In adaptive mode, the Interlock learns operational boundaries from live telemetry before enforcement begins.

Security Architecture: Zero Trust, Zero Access Enterprise security teams ask: "Is this interlock a backdoor?" The answer is architecturally impossible.

#	Guarantee	Detail
01	Zero Listening Ports	Interlock opens no inbound ports. Only outbound HTTPS to api.sentinelauthority.org.

#	Guarantee	Detail
02	Customer Controlled	You deploy, configure, and terminate. Sentinel cannot start, stop, or modify remotely.
03	TLS 1.3 + Pinning	All communications encrypted with certificate pinning. Data encrypted at rest.
04	Your ODD Stays Yours	We never touch your source code, model weights, or decision logic. Only operational telemetry is transmitted.

Sentinel Authority cannot send commands to your system, execute code on your infrastructure, access your network, or control your autonomous systems. No remote commands. No code execution. No network access. No actuator control.

Additional guarantees: No PHI/PII transmitted. Offline enforcement supported. Source auditable. HIPAA/ BAA compatible.

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 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

Step 1: Install 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 Interlock tab). It automatically connects, validates credentials, downloads approved boundary definitions, scans your system for telemetry sources (MQTT, HTTP/REST, Prometheus, gRPC, ROS2, file sensors), matches sources to ODD parameters, writes the configuration, and installs the ENVELO CLI.

Step 2: Validate envelo validate Step 3: Start envelo start # Foreground envelo start -d # Background daemon envelo service install # Auto-start on boot (recommended for CAT-72)

Step 4: Verify in Portal

- Open your case → ENVELO Interlock tab
- Verify Interlock shows "Active" status
- Review boundary list — all parameters should show green
- Proceed to CAT-72 tab and click "Begin Test" when ready

• 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 EnveloInterlock, EnveloConfig interlock = EnveloInterlock(EnveloConfig(api_key='sa_live_...', certificate_number='ODDC-2026-XXXXX'))

interlock.start() @interlock.enforce def move_robot(speed, position): motors.actuate(speed, position)

O U T C O M E Interlock active, all boundaries enforced, portal showing green status. Ready for CAT-72.

P H A S E 5 CAT-72 Execution Timeline: 72 hours minimum | Owner: Automated 72 hours of continuous operation within defined boundaries. The Interlock auto-discovers your operational envelope, then enforces it. The Conformance Assessment Test (CAT-72) is the evidentiary phase, building a cryptographic record of continuous in-bounds operation.

Three Phases of CAT-72

#	Phase	Description
01	Continuous Demo	72-hour sustained operation. In adaptive mode, the Interlock learns operational boundaries from live telemetry before enforcement begins. Systems self-correct near ODD boundary.
02	Stress Testing	Boundary stress testing across discovered or specified limits. ENVELO intervenes — decelerating operations to Minimum Risk Condition before the wall.
03	Enforcement Proof	Verified tiered response: self-correction near ODD, MRC in enforcement margin, hard halt at ENVELO Wall.

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 specified time
- Continuous telemetry coverage — no gaps exceeding maximum allowed interval
- All parameters must report data for the full 72 hours
- O U T C O M E 72-hour evidentiary telemetry record, cryptographically sealed.

P H A S E 6 Determination & Attestation Timeline: 1–2 weeks | Owner: 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
-
- Digital badge and certificate assets for marketing use
- Enforcement Produces Intelligence Every conformance cycle maps where a model operates within its defined boundaries — and where it doesn't. Deliverables include violation mapping, conformance trending, actionable findings, and a feedback cycle that narrows the gap between defined and actual behavior.

O U T C O M E ODDC certificate issued. System listed in the public Conformance Registry. System enters CONFORMANT state.

P H A S E 7 Continued Monitoring Timeline: Ongoing | Owner: Both parties ODDC certification is not a point-in-time assessment. The ENVELO Interlock continues operating after certification, providing continuous runtime enforcement and telemetry.

Ongoing Requirements ENVELO Interlock must remain active and reporting

- Annual conformance review ($12,000/year)
- Changes to system architecture, ODD parameters, or firmware require re-assessment
- Sentinel may request supplementary testing if material changes are detected
- Boundary Exceedance & Drift Protocol Any state, trajectory, or enforcement failure that exceeds attested tolerances triggers immediate conformance review. The system transitions from CONFORMANT to PAUSED. Certificate may be suspended or revoked if the ENVELO Interlock is disabled, material violations are detected, the annual review fee is not paid, or material system changes are made without re-assessment.

O U T C O M E Continuous conformance enforcement. Certificate active as long as Interlock runs and annual reviews are completed.

A P P E N D I X A Boundary Specification Format 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. The applicant never edits boundary definitions directly.

Numeric Boundaries

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

Field	Type	Description
tolerance	number	Acceptable measurement tolerance (±)

Other Boundary Types 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
- A P P E N D I X B ENVELO CLI Reference The ENVELO CLI is the single interface for all Interlock operations. Installed automatically by the one- command installer.

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

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 test status and progress

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
envelo benchmark	Measure enforcement check latency

Infrastructure & Maintenance

Command	Description
envelo service install	Auto-start on boot (systemd / launchd)
envelo docker	Generate Dockerfile + docker-compose.yml
envelo k8s	Generate Kubernetes DaemonSet + Secret
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 update	Self-update
envelo rollback	Uninstall ENVELO (suspends conformance)

A P P E N D I X C Three-Tier Enforcement Model ENVELO enforces boundaries using a three-tier model: self-correction to hard halt. 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 operations to safe state within specified time.
3	ENVELO Wall (Hard Halt)	Parameter exceeds hard limit	Immediate actuation block. Non-bypassable, non- configurable, instant. Protected code never executes.

■ Tier 3 violations during CAT-72 result in automatic test failure. Simulate Enforcement 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)

A P P E N D I X D What ODDC Attests (and Does Not) ✓ ODDC ATTESTS ODD defined with quantitative boundaries

- Stable operation within defined ODD
- ENVELO enforcement architecturally present
- CAT-72 verification completed
- Tamper-evident audit records available
- ✕ DOES NOT ATTEST Functional safety of underlying system
- Regulatory or legal compliance
- Cybersecurity posture or resilience
- System performance or accuracy
- AI model correctness or fitness

• ODDC is an independent conformance determination focused exclusively on whether a system operates within its defined Operational Design Domain with non-bypassable enforcement. It is not a safety certification, regulatory approval, or legal compliance determination.

R E F E R E N C E Glossary

Term	Definition
Adaptive Path	Certification path where the ENVELO Interlock auto-discovers ODD boundaries from operational telemetry. Default path.
Boundary Exceedance	Any state, trajectory, or enforcement failure that exceeds attested tolerances. Triggers conformance review.
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. Three-tier enforcement from self-correction to hard halt.
ENVELO CLI	Command-line interface for all Interlock operations.
ENVELO Interlock	The deployed enforcement component that monitors and enforces ODD boundaries at runtime. Non-bypassable.
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.
Prescriptive Path	Certification path where the applicant submits a pre-defined ODD specification. Alternative to adaptive.

Term	Definition
Sentinel Authority	The independent certification body that administers ODDC certification. Not a regulator.
Three-Tier Enforcement	ENVELO's graduated response: self-correction, MRC, ENVELO Wall.