SENTINEL AUTHORITY

ODDC Certification Guide

Complete Applicant Roadmap for Operational Design Domain Conformance

Version 4.0 · February 2026 · Applicant Distribution

Table of Contents

1. Executive Summary

The ODDC Certification Guide provides a complete roadmap for organizations seeking independent conformance determination for their autonomous systems. This guide covers every phase of the certification process—from initial eligibility through continued monitoring—and provides the operational details applicants need to prepare for and complete certification.

Who This Document Is For

Engineering teams responsible for deploying autonomous systems, compliance officers managing regulatory requirements, operations teams responsible for system monitoring, and executive leadership evaluating conformance certification.

Certification at a Glance

Item	Detail
Duration	Approximately 4–8 weeks from eligibility to conformance determination
Cost	$12,000 initial certification; $12,000 annual renewal
Outcome	Binary: CONFORMANT or NON-CONFORMANT
Validity	One year from conformance determination date
Ongoing	Continuous Interlock monitoring + annual surveillance review

2. What ODDC Is (and Is Not)

ODDC Is:

- An independent conformance determination framework for autonomous physical systems
- Runtime behavioral verification that systems operate within declared boundaries
- A certification body—analogous to UL for autonomous systems
- Quantitative, evidence-based, and independently verifiable

ODDC Is Not:

- A safety certification (ODDC verifies enforcement, not boundary adequacy)
- A process audit (that is ISO 42001, NIST AI RMF, SOC 2)
- A consulting engagement (Sentinel Authority does not advise operators)
- Software (ENVELO is a requirements specification; operators implement)

3. Phase 1: Eligibility Review

Timeline: 3–5 business days | Owner: Sentinel Authority

The eligibility review determines whether the applicant's system is appropriate for ODDC certification. Sentinel Authority evaluates the system type, operational context, and readiness for conformance assessment.

Applicant Provides:

- System description and operational purpose
- Deployment environment and infrastructure overview
- Available telemetry sources and data formats
- Regulatory context (applicable standards, jurisdiction)
- Organizational contact and technical point of contact

Sentinel Authority Evaluates:

Whether the system is an autonomous physical system (as opposed to purely digital/software), whether the system produces adequate telemetry for boundary discovery and enforcement, and whether the operator can support the technical requirements of Interlock deployment.

Sentinel SLA: Eligibility decision within 5 business days of complete submission.

4. Phase 2: ODD Definition

Timeline: 5–10 business days | Owner: Applicant

The operator defines the Operational Design Domain—the specific parameters, ranges, conditions, and boundaries within which the system is designed to operate. This is the applicant's most important contribution: the ODD defines what "conformance" means for this specific system.

ODD Parameter Examples by Vertical

Domain	Example Parameters
Autonomous Vehicle	Geographic geofence, speed limits per road type, weather limits (rain, snow, fog), sensor visibility thresholds, traffic density maximums
Healthcare AI	Approved diagnostic categories, confidence thresholds, data quality requirements, patient population parameters, response latency limits
Industrial Automation	Force/torque limits, workspace geofence, payload limits, human proximity zones, emergency stop latency

Parameters must be expressed as quantitative values with defined ranges, units, and tolerances. Vague or unmeasurable boundaries cannot be enforced and will be rejected during documentation review.

5. Phase 3: Documentation Review

Timeline: 5–7 business days | Owner: Sentinel Authority

Sentinel Authority reviews the ODD specification for completeness, internal consistency, testability, and enforceability. This is not a judgment on whether the boundaries are appropriate—that is a domain-specific regulatory question. The review confirms that the boundaries are technically enforceable.

Common Review Findings:

- **Unmeasurable parameters.** Boundaries expressed in qualitative terms that cannot be converted to quantitative telemetry thresholds.
- **Missing tolerances.** Parameters defined without acceptable ranges or error margins.
- **Internal contradictions.** Boundaries that conflict with each other or create impossible conditions.
- **Incomplete coverage.** Operational scenarios not addressed by any boundary parameter.

Sentinel SLA: Review complete within 7 business days. Revisions do not restart the clock.

6. Phase 4: ENVELO Interlock Deployment

Timeline: 3–5 business days | Owner: Applicant (with Sentinel support)

The ENVELO Interlock is deployed onto the operator's infrastructure. The Interlock is available as a Docker container, standalone binary, or through cloud marketplace. Deployment does not require changes to the autonomous system's core software.

Deployment Steps

1. Install the Interlock on the operator’s infrastructure (Docker, binary, or marketplace).

2. Configure telemetry source connections (YAML configuration file defines endpoints, protocols, and data formats).

3. Run pre-flight validation (7-point checklist: connectivity, telemetry flow, boundary loading, authentication, TLS, hash-chain initialization, state reporting).

4. Initiate LEARNING phase—Interlock begins observing telemetry and auto-discovering operational boundaries.

5. Review discovered boundaries. Operator approves, adjusts, or supplements with prescriptive boundaries.

6. Activate enforcement. System transitions from LEARNING to BOUNDED.

7. Verify BOUNDED state in the Sentinel Authority portal.

Security Model

The Interlock operates in a one-way data flow architecture. Telemetry flows outbound from the operator’s infrastructure to Sentinel Authority. No inbound commands are accepted that could alter enforcement behavior. All telemetry is HMAC-signed and hash-chain linked. Communications use TLS 1.2+ with certificate pinning.

Troubleshooting Reference

Issue	Likely Cause	Resolution
Interlock not connecting	Firewall blocking outbound HTTPS	Allow outbound 443 to Sentinel endpoints
Telemetry not flowing	Incorrect source configuration	Verify YAML endpoint URLs and authentication
Boundary discovery stalled	Insufficient telemetry variety	Ensure system is operating across representative conditions
Pre-flight check failing	TLS certificate mismatch	Verify certificate chain and pinning configuration
State not updating in portal	Network latency or proxy interference	Check proxy configuration, ensure WebSocket support

7. Phase 5: CAT-72 Execution

Timeline: 72 hours continuous + 24-hour analysis | Owner: Sentinel Authority

The CAT-72 (Conformance Authorization Test) is a 72-hour continuous assessment that validates the Interlock's enforcement capability across the system's declared operational envelope. The system must be in BOUNDED state with enforcement active throughout.

During the 72 hours, Sentinel Authority evaluates boundary detection accuracy, enforcement execution across all three tiers, response to deliberate boundary-stress scenarios, telemetry integrity (HMAC signing, hash-chain continuity), and state management accuracy.

Evidence Generated

- Complete telemetry record for the 72-hour period
- Enforcement action log with timestamps, parameters, and outcomes
- State transition log
- Boundary-stress test results (pass/fail per scenario)
- Quantitative capability scores across five assessment areas

8. Phase 6: Conformance Determination

Timeline: 2–3 business days after CAT-72 | Owner: Sentinel Authority

Sentinel Authority reviews the CAT-72 evidence and makes a binary determination:

Determination	Meaning
CONFORMANT	The system demonstrated enforcement of all declared boundaries across all assessment areas. Conformance record issued. System transitions to CONFORMANT state.
NON-CONFORMANT	The system failed to demonstrate adequate enforcement in one or more areas. Detailed findings report issued. System remains in BOUNDED state. Operator may remediate and re-test.

There is no partial certification, conditional pass, or probationary status. The conformance record documents the scope, evidence summary, validity period (one year), and cryptographic verification data.

Sentinel SLA: Determination within 3 business days of CAT-72 completion.

9. Phase 7: Continued Monitoring

Ongoing | Owner: Joint (Operator + Sentinel Authority)

After conformance is determined, the Interlock continues operating in production. It does not shut down after certification—continuous monitoring is the foundation of ongoing conformance assurance.

Ongoing Requirements:

- Maintain 95% conformance score (percentage of operational time within all boundaries)
- Interlock must remain operational and connected

- Report material changes to the system or operational environment
- Participate in annual surveillance review

Suspension Triggers:

- Conformance score drops below 95% and is not restored within 30 days
- Interlock disconnected or telemetry flow interrupted for more than 48 hours
- Material system changes without notification to Sentinel Authority
- Failure to complete annual surveillance review

Data Retention: All telemetry and enforcement records retained for 3 years minimum.

10. Post-Certification Compliance Policy

NOTICE: Certification imposes ongoing obligations. Conformance is not a one-time event—it is a continuous state maintained by the ENVELO Interlock and verified by Sentinel Authority. Failure to maintain compliance results in suspension or revocation of conformance status.

95% Conformance Threshold

Certified systems must maintain a minimum 95% conformance score at all times. This score measures the percentage of operational time during which the system operates within 100% of its declared boundary parameters. The score is calculated on a rolling 30-day window.

30-Day Correction Window

If the conformance score drops below 95%, the operator is notified immediately and granted a 30-day correction window. During this window, the operator must identify the root cause of the conformance degradation, implement corrective measures, and restore the conformance score to 95% or above. The system remains in CONFORMANT state during the correction window.

Suspension

If the conformance score is not restored within 30 days, the system transitions to PAUSED state. Autonomous operation is suspended pending remediation. To restore conformance, the operator must complete remediation and pass a new CAT-72 assessment ($12,000).

Revocation

Conformance status is revoked if the system remains in PAUSED state for more than 90 days without successful re-certification, the operator tampers with or disables the Interlock, the operator provides false or misleading information during any phase, or the operator refuses to participate in annual surveillance review.

11. Fee Schedule

Item	Fee	Notes
Initial Certification	$12,000	Covers Phases 1–6 including CAT-72
Annual Renewal	$12,000	Covers surveillance review and continued Interlock operation
Re-Test (after failure)	$12,000	Full CAT-72 re-execution

Pricing is per-system. There are no per-unit, per-vehicle, or per-deployment licensing fees. Fleet and multi-system pricing is available for operators certifying multiple systems simultaneously.

12. Emergency Procedures

If a certified system experiences a critical safety event, boundary enforcement failure, or other emergency condition:

- The Interlock will automatically execute the appropriate enforcement tier (MRC or hard halt).
- The event is logged in the tamper-evident telemetry chain with full parameter data.
- Sentinel Authority is notified automatically via the telemetry feed.
- The operator should contact Sentinel Authority within 24 hours to initiate incident review.
- An incident report will be generated documenting the event timeline, enforcement actions, and contributing factors.

Emergency events do not automatically trigger suspension. The Interlock's response to the emergency is itself evidence of enforcement working correctly.

13. Multi-System and Fleet Certification

Operators deploying multiple instances of the same system type may pursue fleet certification. Fleet certification requires that all systems in the fleet share the same ODD definition, Interlock configuration, and enforcement parameters. CAT-72 is run on a representative sample plus any systems with unique deployment conditions.

Fleet certification reduces per-system cost and streamlines the process, but every system in the fleet must run the Interlock independently and maintain individual conformance scores. A single system's failure does not affect the fleet's certification, but fleet-wide patterns of conformance degradation may trigger a fleet-wide review.

14. Frequently Asked Questions

Q1: How long does certification take?

Approximately 4–8 weeks from eligibility submission to conformance determination, depending on the complexity of the system and how quickly the operator completes the ODD definition.

Q2: Do I need to modify my autonomous system?

No. The ENVELO Interlock operates alongside your system, observing telemetry and enforcing boundaries externally. Your system must expose operational telemetry that the Interlock can ingest, but no changes to core software, algorithms, or architecture are required.

Q3: What happens if I make changes to my system after certification?

Material changes must be reported to Sentinel Authority. Depending on the scope of changes, a partial or full re-assessment may be required. Minor changes that do not affect boundary parameters or enforcement behavior may not require re-testing.

Q4: Can I certify a system that is still in development?

No. ODDC certification requires a deployed, operational system with live telemetry. Certification of pre-production systems is not available. However, you can begin the eligibility and ODD definition phases while the system is in late-stage development.

Q5: What if my system operates in multiple environments?

Each distinct operational environment may require separate boundary definitions. A vehicle that operates in both urban and highway environments, for example, may need separate ODD specifications for each. Multi-environment certification is supported but may require expanded CAT-72 testing.

Q6: Is my conformance data confidential?

Telemetry data and internal conformance details are confidential. The conformance record (CONFORMANT/NON-CONFORMANT status, scope, and validity period) may be shared with regulators, insurers, and other stakeholders at the operator’s discretion.

Q7: Can I appeal a NON-CONFORMANT determination?

Operators may request a determination review within 30 days. The review examines the CAT-72 evidence and methodology but does not re-run the test. If the review identifies procedural errors, a re-test may be offered at no additional cost.

Q8: What jurisdiction does ODDC certification cover?

ODDC certification is jurisdiction-agnostic. The conformance determination is based on technical enforcement evidence, not regulatory requirements. Operators and regulators determine how ODDC certification applies within their specific regulatory context.

15. Glossary

Term	Definition
Boundary	A quantitative parameter defining the limit of acceptable system behavior within the Operational Design Domain.
CAT-72	Conformance Authorization Test. A 72-hour continuous assessment procedure validating enforcement capability.
Conformance Score	The percentage of operational time during which the system operates within 100% of declared boundary parameters.
Convergence Score	A measure of how consistently the system returns to nominal operating parameters after boundary approach events.
Drift Rate	The rate at which a system's operational behavior moves toward boundary limits over time.
ENVELO	Enforced Non-Violable Execution-Limit Override. The runtime enforcement mechanism specification.
Hard Halt	Tier 3 enforcement: immediate, non-negotiable system shutdown.
Interlock	The ENVELO Interlock—the deployment component that enforces boundaries on the operator's infrastructure.
MRC	Minimum Risk Condition. Tier 2 enforcement: system forced to a pre-defined safe state.
ODD	Operational Design Domain. The set of conditions under which a system is designed to operate.
ODDC	Operational Design Domain Conformance. The certification framework.
Self-Correction	Tier 1 enforcement: system autonomously adjusts to return within boundary parameters.
Stability Index	A measure of operational consistency—how much variance the system exhibits relative to its boundary margins.