ODDC GOVERNANCE & INDEPENDENCE STATEMENT Public Document • February 2026

Governance & Independence Statement

ODDC Certification Program — Administered by Sentinel Authority
February 2026 — Public Document

This document describes the governance structure, independence mechanisms, and operational controls that ensure the integrity of Operational Design Domain Conformance (ODDC) certifications issued by Sentinel Authority. It is intended for government procurement officers, regulatory bodies, insurance underwriters, and any party evaluating Sentinel Authority as an independent certification reference.

1. IDENTITY & STRUCTURE

1.1 Legal Identity

Sentinel Authority operates as an independent certification body organized under the laws of the Province of Ontario, Canada. Sentinel Authority does not manufacture, develop, operate, or deploy autonomous systems. It has no equity interest in, joint venture with, or contractual dependency upon any autonomous system developer, operator, or integrator.

1.2 Mission

Sentinel Authority exists to issue, maintain, and if necessary revoke Operational Design Domain Conformance (ODDC) determinations for autonomous systems. Its sole function is independent third-party attestation that a system operates within its declared operational boundaries, verified through continuous runtime enforcement.

1.3 What Sentinel Authority Is Not

- Not a technology vendor — Sentinel Authority does not build, sell, or license ENVELO software.
- Not a consulting firm — Sentinel Authority does not advise applicants on how to pass certification.
- Not an insurer — ODDC conformance is not an insurance policy or warranty.
- Not a regulator — Sentinel Authority is a private certification body; regulatory authority rests with government agencies.

2. STANDARD VS. CERTIFIER SEPARATION

ODDC is a conformance standard. Sentinel Authority is the certifier. These are structurally separate roles, and maintaining that separation is foundational to the program's credibility.

Role	Function	Analogy

ODDC (Standard)	Defines what conformance means: operational boundary declaration, runtime enforcement requirements, and minimum verification procedures.	ISO 27001 (the standard)
Sentinel Authority (Certifier)	Administers the conformance process: accepts applications, deploys the ENVELO Interlock, conducts CAT-72 testing, issues or denies determinations, and maintains the public registry.	BSI, SGS, or Bureau Veritas (the registrar)

This separation means that if a future body assumes administration of the ODDC standard, the standard itself is not dependent on Sentinel Authority's continued operation. Conversely, Sentinel Authority's conformance determinations are not self-referential—they attest to an independently defined set of requirements.

3. INDEPENDENCE MECHANISMS

3.1 Pre-CAT-72 Controls

Before any system enters the Conformance Authorization Test (CAT-72), the following structural controls are in place:

- **No consulting relationship.** Sentinel Authority does not advise applicants on system design, ODD specification, or ENVELO implementation strategy. Applicants receive the published requirements and nothing more.
- **Blind boundary discovery.** Under the adaptive path (default), the ENVELO Interlock auto-discovers operational boundaries from system telemetry. The applicant does not dictate what boundaries the Interlock should find.
- **Locked tolerance specifications.** Once tolerances are submitted or discovered, they cannot be amended during testing. This eliminates the possibility of adjusting pass/fail criteria mid-assessment.
- **No pre-certification previews.** Applicants do not receive preliminary results, interim scores, or informal guidance on whether they are likely to pass.

3.2 Decision Authority

Conformance determinations are binary: conform or does-not-conform. There is no conditional pass, provisional certification, or graded outcome. The determination is made against the locked tolerances and the minimum 72 cumulative hours of CAT-72 data. No individual at Sentinel Authority has the authority to override a does-not-conform determination. The applicant's only recourse is to remediate and retest.

3.3 Registry Integrity

Every conformance determination—whether issuance, renewal, suspension, or revocation—is published to the Sentinel Authority public registry at sentinelauthority.org/verify. The registry includes:

- Certificate hash (unique, tamper-evident identifier)
- System identification and ODD scope
- Issuance and expiration dates
- Current status (CONFORMANT, SUSPENDED, REVOKED, EXPIRED)

- Full revocation history with reason codes (publicly visible)

The public revocation history tab ensures that no conformance determination can be quietly removed. If a certificate is revoked, the record remains permanently visible with the reason for revocation. This prevents any perception that Sentinel Authority could suppress negative outcomes.

4. MINIMUM ODD SPECIFICITY REQUIREMENTS

ODDC requires that every certified system operate within a defined Operational Design Domain. To prevent vague or meaningless ODD declarations, Sentinel Authority enforces minimum specificity requirements:

Requirement	Description
R-01	Every ODDC-certified system SHALL declare at least one quantitative operational boundary with a measurable threshold and defined unit. An ODD that contains only qualitative descriptions (e.g., "good weather," "normal traffic") is non-conforming.
R-01a	Each declared boundary SHALL specify: (a) the parameter name, (b) the measurement unit, (c) the numerical threshold or range, and (d) the enforcement action triggered upon exceedance. Boundaries lacking any of these four elements are non-conforming.

These requirements ensure that an ODDC certificate is tied to objectively verifiable constraints—not aspirational language. A regulator or insurer referencing an ODDC certificate can confirm exactly what the system was certified to do, under what conditions, and what happens when those conditions are exceeded.

Adaptive Discovery

Under the adaptive path, the ENVELO Interlock observes the system during normal operation and auto-discovers operational boundaries from telemetry data. The operator reviews and approves the discovered boundaries before enforcement begins. This means even operators who cannot articulate their ODD upfront receive a rigorously quantified boundary set—the Interlock defines what the system actually does, not what someone claims it does.

5. CONTINUOUS CONFORMANCE & LIVENESS HEARTBEAT

ODDC is not a point-in-time audit. Conformance is continuously maintained through the ENVELO Interlock, which remains active on the certified system for the duration of the certificate’s validity.

5.1 The ENVELO Interlock

The Interlock is a runtime enforcement mechanism that constrains the autonomous system’s actions to its declared operational boundaries. It implements a three-tier enforcement architecture:

- **Tier 1: Self-Correction:** System detects boundary approach and self-adjusts. Logged but no external intervention required.
- **Tier 2: Controlled Degradation:** System is directed to a Minimum Risk Condition (MRC) when self-correction is insufficient. Graceful reduction in operational scope.
- **Tier 3: Hard Halt:** Immediate cessation of autonomous operation when Tiers 1 and 2 are insufficient or when a critical boundary is breached.

5.2 Liveness Heartbeat

The certificate verification endpoint at sentinelauthority.org/verify performs a continuous liveness check. When a certificate is queried, the system confirms not only that the certificate was issued, but that the ENVELO Interlock is currently active and reporting. This means:

- A certificate that shows CONFORMANT status confirms the Interlock is live and enforcement is active right now.
- If the Interlock stops reporting, the certificate status transitions to SUSPENDED automatically—no human intervention required.
- Regulators and insurers can verify conformance status in real time, not based on a historical snapshot.

5.3 Post-Certification Compliance

Conformance is maintained through ongoing Interlock operation. If a system's compliance rate falls below 95% of in-bounds operation over any rolling 30-day window, the certificate is automatically suspended. The operator has a 30-day correction window to remediate. If the compliance rate is not restored within 30 days, the certificate is revoked and the revocation is published to the registry with a reason code.

6. EXPLICIT EXCLUSIONS

ODDC conformance is deliberately narrow in scope. The following are explicitly outside the scope of what an ODDC certificate attests to:

Exclusion	Explanation
Functional safety	ODDC does not assess whether the system is safe by design. It attests that the system operates within declared boundaries. Functional safety assessment (e.g., ISO 26262, IEC 61508) remains the responsibility of the system developer.
Regulatory or legal compliance	ODDC conformance does not constitute compliance with any federal, state, or international regulation. Operators remain responsible for all applicable legal requirements.
Cybersecurity posture	ODDC does not assess the system's resilience to cyber attack, penetration, or exploitation. Cybersecurity certification (e.g., SOC 2, ISO 27001) is a separate concern.
AI model correctness	ODDC does not evaluate the training data, algorithmic fairness, accuracy, or decision quality of the underlying AI model. It attests only that the system's operational outputs remain within declared boundaries.
System performance	ODDC does not certify that a system performs well, only that it performs within bounds. A system may be ODDC-conformant and still perform poorly within its declared domain.
Insurance or warranty	An ODDC certificate is not an insurance policy, product warranty, or guarantee of any kind. It is an independent attestation of boundary conformance.

These exclusions are not limitations—they are deliberate scoping decisions. ODDC is designed to do one thing with institutional rigor: verify that an autonomous system operates within its declared boundaries, enforced at runtime, verified continuously. By explicitly excluding adjacent concerns, ODDC avoids scope creep that would dilute the precision of the conformance determination.

7. CONTACT & REGULATORY INTEGRATION

7.1 For Regulators

Sentinel Authority welcomes engagement with federal, state, and international regulatory bodies evaluating autonomous systems oversight frameworks. ODDC is designed to be complementary to existing regulatory structures—not a replacement. Regulators may reference ODDC conformance as one input among many in their oversight decisions.

Sentinel Authority can provide regulators with:

- Technical briefings on the ODDC framework, ENVELO enforcement architecture, and CAT-72 test methodology
- Access to anonymized conformance data and enforcement statistics
- Formal letters of explanation for procurement or policy development processes
- Registry API access for automated conformance status verification

7.2 For Insurance Underwriters

ODDC conformance provides underwriters with a verified, continuously monitored signal that an autonomous system operates within declared boundaries. This does not replace actuarial assessment, but it provides an objective data point for risk evaluation—one that is independently verified, runtime-enforced, and publicly auditable.

7.3 For Government Procurement

Procurement officers evaluating autonomous systems may reference ODDC conformance as evidence that a system has been independently verified to operate within declared operational constraints. The public registry provides real-time status verification. The certificate hash provides tamper-evident proof of issuance.

7.4 Contact

Channel	Details
Website	sentinelauthority.org
Registry / Verify	sentinelauthority.org/verify
General Inquiries	info@sentinelauthority.org
Conformance Inquiries	conformance@sentinelauthority.org

— End of Document —