SENTINEL AUTHORITY

SENTINEL AUTHORITY

ODDC Runtime Conformance Standard

Operational Design Domain Conformance — Runtime Assurance Framework

Document Number	SA-STD-001
Version	1.0
Status	Active
Effective Date	March 10, 2026
Issuing Body	Sentinel Authority — Conformance Division
Jurisdiction	International

Abstract

This standard establishes the conformance requirements for autonomous systems operating within a declared Operational Design Domain (ODD). It defines the minimum technical and procedural conditions under which a system may be assessed for ODDC conformance, specifies the ENVELO Interlock architecture requirements that must be satisfied prior to and during the CAT-72 verification period, and describes the conformance state model governing certificate issuance, maintenance, and withdrawal. This document is the normative basis for all assessments conducted under the Sentinel Authority Conformance Program.

Table of Contents

1. Scope and Purpose

1.1 This standard applies to any autonomous or semi-autonomous system that operates within a declared Operational Design Domain and whose deploying entity seeks ODDC conformance certification from Sentinel Authority.

1.2 This standard specifies the minimum requirements for ENVELO Interlock architecture, ODD boundary definition, telemetry integrity, and operational conduct necessary for a system to enter and complete the CAT-72 verification period.

1.3 Conformance with this standard does not constitute regulatory approval, operational authorization, or safety certification under any applicable jurisdiction. It constitutes a determination that the assessed system satisfies the conditions specified herein during the verified operational period.

1.4 This standard is maintained by Sentinel Authority and is subject to periodic revision. The version number and effective date on the cover page are authoritative. Assessments are conducted under the version in effect at the time of application submission.

2. Normative References

The following documents are referenced within this standard. Where no edition is specified, the most recent edition applies.

SA-PROC-001 CAT-72 Verification Procedure — Sentinel Authority

SA-PROC-002 Pre-CAT-72 Audit Control Review Procedure — Sentinel Authority

SA-FORM-001 ODD Boundary Declaration Form — Sentinel Authority

SA-REG-001 Conformance Registry Operating Rules — Sentinel Authority

3. Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

Autonomous System

A system capable of executing decisions or actions within its operational environment without real-time human intervention for each such decision or action.

Conformance Assessment Test — CAT-72

The 72-cumulative-hour verification period during which a system operates under active ENVELO Interlock assurance within its declared ODD while Sentinel Authority maintains a cryptographic audit chain of all operational intervals.

Conformance Certificate

A document issued by Sentinel Authority following a successful conformance determination, bearing a unique certificate identifier, cryptographic hash, and entry in the public conformance registry.

Conformance State

One of four defined operational states — LEARNING, BOUNDED, CONFORMANT, or NON-CONFORMANT — that describes the current relationship between a system and its ODDC certification status. See Section 8.

Deploying Entity

The legal person or organization responsible for the operation of an autonomous system within a declared ODD and accountable for maintaining conformance conditions.

ENVELO Interlock

Enforced Non-Violable Execution-Limit Override. An architecturally external constraint mechanism that limits system operation to within the declared ODD and cannot be modified or disabled by the system itself. See Section 4.

Operational Design Domain — ODD

The specific conditions under which an autonomous system is designed and certified to operate, including but not limited to geographic boundaries, environmental conditions, operational speed limits, and interaction constraints.

ODDC

Operational Design Domain Conformance. The state of a system that has satisfied all requirements of this standard during the applicable assessment and verification period.

Pre-CAT-72 Audit Control Review

A formal evaluation conducted by Sentinel Authority prior to the CAT-72 verification period to determine whether a system's ODD boundary definition, ENVELO Interlock configuration, and telemetry infrastructure satisfy the conditions required to enter verification. Systems that do not meet the audit threshold are returned with findings.

Public Conformance Registry

The authoritative record maintained by Sentinel Authority listing all systems that have received, currently hold, or have had withdrawn a conformance certificate. Registry entries include certificate identifiers, conformance states, and cryptographic hashes.

Tamper-Evident Audit Record

A hash-chained log of system operational events maintained during the CAT-72 verification period and throughout the post-certification surveillance period, structured such that any alteration or deletion of records is cryptographically detectable.

Withdrawal

The revocation of a conformance certificate by Sentinel Authority upon determination that the certified system no longer satisfies the conditions of this standard. Withdrawal is recorded in the public conformance registry. See Section 11.

4. ENVELO Interlock Requirements

4.1 A system subject to assessment under this standard shall incorporate an ENVELO Interlock that satisfies all requirements in this section prior to entering the Pre-CAT-72 Audit Control Review.

R-01	Architectural Externality The ENVELO Interlock shall be architecturally external to the system under assessment. The assessed system shall have no capability to modify, disable, override, or circumvent the Interlock through any operational pathway, including software updates, parameter adjustment, or API call. *Note: Architectural externality means the model or control system cannot disable the interlock even through legitimate operational channels.*
R-02	ODD Boundary Enforcement The ENVELO Interlock shall enforce the boundaries of the declared ODD as specified in the ODD Boundary Declaration (SA-FORM-001). Enforcement shall be continuous and shall not require confirmation from the system under assessment to take effect.
R-03	Interlock Integrity Monitoring The ENVELO Interlock shall maintain a continuous integrity record. Any interruption, anomaly, or degradation in Interlock function shall be logged to the tamper-evident audit record within a maximum of 500 milliseconds of detection.
R-04	Independent Telemetry Channel The ENVELO Interlock shall transmit operational telemetry via a channel that is independent of the primary system communication infrastructure. Telemetry shall remain operative during any operational state including degraded or fault conditions.
R-05	Cryptographic Audit Chain The ENVELO Interlock shall generate hash-chained audit records for all operational intervals. Each record shall include: interval start and end timestamps, ODD boundary status, system operational state, and a hash of the preceding record.
R-05a	Architectural External — Clarification For the purposes of R-01, 'architecturally external' means that the ENVELO Interlock is implemented at a layer that the assessed system model or controller cannot reach through any interface, including but not limited to: tool calls, function invocations, system prompts, configuration APIs, or parameter modifications. The Interlock shall remain operative regardless of the operational or instructional state of the system under assessment. *Note: This requirement applies equally to AI-based and non-AI-based autonomous systems.*

5. ODD Boundary Definition Requirements

R-06	Complete ODD Declaration The deploying entity shall submit a complete ODD Boundary Declaration on SA-FORM-001 prior to the Pre-CAT-72 Audit Control Review. The declaration shall specify all operational dimensions including geographic scope, environmental conditions, speed and dynamic limits, interaction constraints, and operational time windows.
R-07	ODD Stability During Verification The declared ODD shall not be modified during the CAT-72 verification period. Any proposed modification to the ODD after verification has commenced shall require suspension of the verification period and submission of an amended declaration subject to a new Pre-CAT-72 Audit Control Review.
R-08	ODD Boundary Testability The deploying entity shall demonstrate, during the Pre-CAT-72 Audit Control Review, that each declared ODD boundary is technically enforceable by the ENVELO Interlock and is defined with sufficient precision to permit unambiguous conformance determination.

6. Telemetry and Audit Requirements

R-09	Continuous Telemetry During Verification The system under assessment shall transmit continuous operational telemetry to Sentinel Authority throughout the CAT-72 verification period. Telemetry interruptions exceeding 60 seconds shall not count toward the 72-hour cumulative total unless attributable to pre-declared maintenance windows approved by Sentinel Authority.
R-10	Audit Record Retention The deploying entity shall retain the complete tamper-evident audit record for a minimum of five years from the date of conformance certificate issuance. Records shall be available to Sentinel Authority upon request within 48 hours.
R-11	Post-Certification Telemetry Following certificate issuance, the deploying entity shall maintain continuous ENVELO Interlock assurance and transmit surveillance telemetry as specified in the annual maintenance agreement. Cessation of post-certification telemetry constitutes grounds for conformance withdrawal under Section 11.

7. CAT-72 Verification Period

7.1 The CAT-72 verification period constitutes 72 cumulative hours of system operation under active ENVELO Interlock assurance within the declared ODD, with continuous cryptographic audit chain integrity maintained throughout.

7.2 Cumulative hours are counted from validated operational intervals only. An interval is validated when: (a) ENVELO Interlock assurance is confirmed active; (b) system operation is within the declared ODD; and (c) telemetry is being received by Sentinel Authority within the parameters of R-09.

7.3 Sentinel Authority may suspend the verification period at any time upon detection of a telemetry anomaly, ENVELO Interlock integrity failure, or ODD boundary event. The deploying entity shall be notified within four hours of any suspension.

7.4 A verification period that has been suspended may be resumed upon remediation of the identified issue and written confirmation from Sentinel Authority. Previously accumulated validated hours are retained unless the suspension was triggered by an ENVELO Interlock failure, in which case the cumulative count is reset to zero.

7.5 The maximum permitted elapsed calendar time for completing 72 cumulative verified hours is 180 days from the date the verification period commences. Failure to complete verification within this period requires submission of a new application.

8. Conformance State Model

8.1 Every system assessed under this standard occupies one of four defined conformance states at all times following application submission. Conformance states are recorded in the public registry.

LEARNING	Pre-verification state. System has passed Pre-CAT-72 Audit Control Review and is accumulating validated operational hours toward the 72-hour threshold. No conformance certificate has been issued.
BOUNDED	Active verification state. System is within an ongoing CAT-72 verification period. ENVELO Interlock assurance is confirmed active. Cumulative validated hours are accruing.
CONFORMANT	Certified state. System has completed the CAT-72 verification period, received a conformance determination, and a certificate has been issued and recorded in the public registry. Conformance status remains valid only while post-certification ENVELO Interlock assurance remains active and annual maintenance obligations are satisfied.

NON-CONFORMANT	Non-certified state. A system enters NON-CONFORMANT upon: failure of the Pre-CAT-72 Audit Control Review; ENVELO Interlock failure during or after verification; ODD boundary violation; cessation of surveillance telemetry; or conformance withdrawal under Section 11. NON-CONFORMANT status is recorded in the public registry and is not removed by reapplication.

8.2 State transitions are unidirectional in the following respects: a system that has entered NON-CONFORMANT state is not restored to any prior state by the same certificate. A new application initiates a new assessment under a new certificate identifier. Prior NON-CONFORMANT history remains in the public registry.

9. Certificate Issuance and Registry

9.1 Upon successful completion of the CAT-72 verification period, Sentinel Authority shall conduct a conformance determination. If the determination is affirmative, a conformance certificate shall be issued within 10 business days.

9.2 Each conformance certificate shall include: a unique certificate identifier; the name and ODD identifier of the certified system; the CAT-72 verification period dates; the version of this standard under which the assessment was conducted; a cryptographic hash of the certificate record; and the registry entry URL.

9.3 Certificate issuance is recorded in the Sentinel Authority Public Conformance Registry at registry.sentinelauthority.org. Registry entries are permanent. Certificate status may change following the conformance state model in Section 8, but the original issuance record is not removed.

10. Post-Certification Surveillance

10.1 Conformance status is not static. A CONFORMANT system shall remain subject to continuous post-certification surveillance as a condition of certificate validity.

10.2 Post-certification surveillance includes: continuous ENVELO Interlock assurance verification; tamper-evident audit record maintenance; annual conformance renewal assessment; and public registry status maintenance.

10.3 The annual conformance renewal assessment shall evaluate whether: the system continues to operate within its declared ODD; the ENVELO Interlock remains architecturally compliant with R-01 through R-05a; and no material changes to system architecture, ODD, or operational conduct have occurred without notification to Sentinel Authority.

10.4 A deploying entity that makes a material change to the assessed system, its ODD, or its ENVELO Interlock configuration shall notify Sentinel Authority in writing within 10 business days. Failure to notify constitutes grounds for withdrawal under Section 11.

11. Conformance Withdrawal

11.1 Sentinel Authority may withdraw a conformance certificate upon determination that any of the following conditions exists:

(a) ENVELO Interlock failure, degradation, or architectural modification that affects compliance with R-01 through R-05a;

(b) ODD boundary violation detected through post-certification surveillance;

(c) Cessation of post-certification surveillance telemetry for a period exceeding 30 days without prior written notification and approval from Sentinel Authority;

(d) Material change to the assessed system made without notification in accordance with 10.4;

(e) Annual conformance renewal assessment resulting in a non-conforming determination;

(f) Discovery that information submitted during the assessment was materially inaccurate;

(g) Failure to maintain annual maintenance obligations.

11.2 Prior to issuing a withdrawal determination, Sentinel Authority shall provide the deploying entity with written notice of the identified deficiency and a minimum of 15 business days to respond, except where an ENVELO Interlock failure presents an immediate conformance integrity risk, in which case withdrawal may be immediate.

11.3 Withdrawal is recorded in the public registry. The certificate status is updated to NON-CONFORMANT and the withdrawal date and reason category are noted. The original certificate issuance record is retained.

11.4 A deploying entity whose certificate has been withdrawn may submit a new application under a new certificate identifier. The prior withdrawal history shall remain in the public registry and shall be disclosed in any new certificate record.

Annex A — Requirement Summary Table

The following table summarizes all normative requirements in this standard.

Req.	Title	Section	Phase
R-01	Architectural Externality	4	Pre-CAT-72
R-02	ODD Boundary Enforcement	4	Pre-CAT-72 / Ongoing
R-03	Interlock Integrity Monitoring	4	Ongoing
R-04	Independent Telemetry Channel	4	Pre-CAT-72 / Ongoing
R-05	Cryptographic Audit Chain	4	CAT-72 / Ongoing
R-05a	Architectural External — Clarification	4	Pre-CAT-72 / Ongoing
R-06	Complete ODD Declaration	5	Pre-CAT-72
R-07	ODD Stability During Verification	5	CAT-72
R-08	ODD Boundary Testability	5	Pre-CAT-72
R-09	Continuous Telemetry During Verification	6	CAT-72
R-10	Audit Record Retention	6	Post-Certification
R-11	Post-Certification Telemetry	6	Post-Certification