SENTINEL AUTHORITY

Conformance Determination for Autonomous Systems

ENVELO Requirements

Enforcer for Non-Violable Execution & Limit Oversight

Version 1.0 · January 2026 · Public Summary

Document Purpose

This document specifies the high-level requirements for ENVELO-compliant enforcement mechanisms. ENVELO defines *what* runtime enforcement must accomplish—not *how* implementations must be constructed. Requirements are stated in normative language to support conformance assessment.

> *ENVELO is a requirements specification, not software. Sentinel Authority defines enforcement requirements; operators design and implement compliant systems. Implementation details, architectures, and technology choices are at the operator's discretion provided requirements are satisfied.*

Terminology

The following terms carry specific meaning in this specification:

- **SHALL** — Requirement is mandatory for conformance.
- **SHOULD** — Requirement is recommended; deviation requires documented justification.
- **MAY** — Requirement is optional.
- **Envelope** — The formally specified boundary of permitted autonomous action.
- **Enforcement Layer** — The runtime mechanism that evaluates and controls autonomous actions.
- **Violation** — Any attempted action outside the declared envelope boundary.

1. Core Enforcement Requirements

1.1 Non-Bypassability

- The enforcement layer SHALL interpose on all autonomous decision-to-action pathways.
- No autonomous action SHALL reach actuation without enforcement layer evaluation.
- The enforcement layer SHALL NOT be disabled, circumvented, or bypassed by autonomous system logic.
- Enforcement layer availability SHALL be a precondition for autonomous operation.

1.2 Boundary Enforcement

- The enforcement layer SHALL evaluate each proposed action against the declared envelope.
- Actions within envelope bounds SHALL be permitted to proceed.
- Actions outside envelope bounds SHALL be blocked, denied, or overridden.
- Boundary evaluation SHALL occur prior to actuation, not post-hoc.

1.3 Fail-Closed Behavior

- Upon detecting an envelope violation, the system SHALL transition to a safe state.
- Safe states MAY include: halt, default denial, human handoff, or pre-defined fallback.
- The system SHALL NOT continue autonomous operation following unresolved violations.
- Enforcement layer failure SHALL trigger fail-closed behavior, not fail-open.

2. Envelope Specification Requirements

2.1 Formal Declaration

- The Operational Design Domain SHALL be formally specified prior to deployment.
- Envelope boundaries SHALL be expressed in machine-readable format.
- Envelope specifications SHALL include conditions, constraints, and permitted action space.
- Ambiguous or underspecified boundaries SHALL NOT satisfy conformance requirements.

2.2 Constraint Types

Envelope specifications SHOULD address applicable constraints including:

- Physical limits (velocity, force, temperature, spatial boundaries)
- Temporal constraints (rate limits, duration limits, sequencing requirements)
- Environmental conditions (operational context, preconditions)
- Resource constraints (capacity limits, availability requirements)

- Invariants (conditions that must remain true throughout operation)

3. Audit and Evidence Requirements

3.1 Logging

- All enforcement decisions SHALL be logged with sufficient detail for audit reconstruction.
- Logs SHALL include: timestamp, proposed action, envelope evaluation result, and outcome.
- Logs SHALL capture both permitted actions and blocked violations.
- Log integrity SHALL be protected against tampering or retroactive modification.

3.2 Evidence Generation

- The enforcement layer SHALL generate audit evidence suitable for third-party review.
- Evidence SHOULD support cryptographic verification of integrity and authenticity.
- Evidence SHALL be retained for the duration required by applicable policy or regulation.
- Evidence format SHOULD support automated verification and analysis.

4. Operational Requirements

4.1 Continuous Enforcement

- Enforcement SHALL be continuous throughout autonomous operation.
- Enforcement SHALL NOT be suspended, paused, or deferred during operation.
- Real-time enforcement latency SHALL NOT create unsafe gaps in boundary checking.

4.2 State Management

- The system SHALL maintain awareness of current operational state relative to envelope boundaries.
- State drift toward envelope boundaries SHOULD trigger graduated responses.
- State transitions SHALL be logged and available for audit.

5. Conformance Assessment

Conformance to ENVELO requirements is assessed through Sentinel Authority procedures including CAT-72 (Convergence Authorization Test). Assessment evaluates:

- Correct implementation of non-bypassable enforcement
- Proper fail-closed behavior under violation conditions

- Audit log completeness and integrity
- Sustained operation within declared boundaries under test conditions

This document specifies requirements. Detailed assessment procedures and test specifications are published separately.