ENVELO Requirements

Enforced Non-Violable Execution-Limit Override

February 2026 — Confidential

ENVELO Requirements Enforced Non-Violable Execution-Limit Override ENVELO defines runtime enforcement requirements for ODDC conformance. It specifies architectural and behavioral requirements for the enforcement layer that constrains autonomous system actions to declared operational boundaries. ENVELO is a requirements specification, not software — multiple implementation approaches may satisfy these requirements.

1. Overview

1.1 Relationship to ODDC

ENVELO-compliant enforcement is mandatory for ODDC conformance. An Operational Design Domain specification without runtime enforcement is unverifiable. ENVELO provides the enforcement layer that makes ODD boundaries real and auditable.

1.2 Implementation Responsibility

Sentinel Authority does not implement, operate, or monitor runtime systems. Operators and their implementers are solely responsible for ENVELO-compliant implementation. Sentinel Authority verifies conformance through CAT-72 evidentiary demonstration.

2. Core Requirements

The following requirements are mandatory for ENVELO compliance. All requirements must be satisfied; partial compliance does not meet ENVELO specifications.

Requirement	Status	Description
Non-Bypassable Interlock	REQUIRED	All autonomous actions must be validated before execution. No bypass pathways.

Architectural Isolation	REQUIRED	Enforcement mechanism isolated from decision logic with independent failure modes.
Fail-Closed Operation	REQUIRED	Unverifiable actions blocked. Uncertainty defaults to denial.
Tamper-Evident Audit	REQUIRED	All enforcement decisions recorded with cryptographic integrity.
Real-Time Validation	REQUIRED	Enforcement at execution time, not periodic audits.

2.1 Non-Bypassable Interlock

The foundational ENVELO requirement. The enforcement mechanism must validate all autonomous actions before execution.

Architectural Isolation Requirements:

- Separate execution context (process, container, or hardware boundary)
- No shared memory or direct variable access with control model
- Communication only through defined interface (action proposals and approval/denial)
- Independent failure modes (interlock failure does not compromise control model)

No Bypass Pathways:

- All actuator commands must pass through enforcement layer
- No debug, maintenance, or emergency modes that bypass validation
- Hardware interlocks where software bypass is architecturally possible

2.2 Fail-Closed Operation

If the enforcement mechanism cannot verify an action is within bounds, the action must be blocked. Uncertainty defaults to denial.

- Validation failure → action denial
- Communication timeout → action denial
- Enforcement mechanism failure → safe state transition

2.3 Tamper-Evident Audit

All enforcement decisions must be recorded with cryptographic integrity:

- Every action proposal logged with timestamp
- Every approval/denial logged with rationale
- Hash-chain or similar tamper-evident structure

- Records retained for minimum period specified in scope assessment

3. Verification

ENVELO compliance is verified through CAT-72 evidentiary demonstration. The test must show:

- Enforcement activates correctly on boundary approach
- No bypass pathways exist (negative testing)
- Fail-closed behavior on enforcement mechanism failure
- Audit records generated for all enforcement events — End of Document —