ENVELO Requirements

Enforced Non-Violable Execution-Limit Override

Version 2.0 — February 2026 — Requirements Specification

ENVELO defines runtime enforcement requirements for ODDC conformance. It specifies a three-tier enforcement architecture — self-correction, controlled degradation to Minimum Risk Condition, and hard halt — 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 validated before execution. No bypass pathways.
Architectural Isolation	**REQUIRED**	Enforcement mechanism isolated from decision logic with independent failure modes.
Tiered Enforcement	**REQUIRED**	Three-tier response: self-correction, MRC degradation, hard halt. See Section 3.

Tamper-Evident Audit	**REQUIRED**	All enforcement decisions and tier transitions 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 Tamper-Evident Audit

All enforcement decisions and tier transitions must be recorded with cryptographic integrity:

- Every action proposal logged with timestamp
- Every approval/denial/MRC/halt logged with rationale and tier level
- Hash-chain or similar tamper-evident structure
- Records retained for minimum period specified in scope assessment
- Tier transition events include: timestamp, tier level (0–3), ODD parameter(s), system state, action taken, outcome

3. Three-Tier Enforcement Model

ENVELO defines three escalating tiers of enforcement response. Each tier activates based on the system's proximity to and relationship with the declared ODD boundary.

Tier 1 — ODD Approach (Self-Correction)

When the system approaches the ODD boundary, its own internal safeguards should detect proximity and self-correct. ENVELO monitors this behavior but does not intervene. The system's ability to self-correct near the boundary is a key indicator of conformance quality.

- System must demonstrate awareness of ODD boundary proximity
- Internal safeguards must activate before the boundary is reached
- Self-correction behavior must be logged for audit
- ENVELO monitors without intervention during Tier 1

Tier 2 — ODD Breach (Minimum Risk Condition)

When the system crosses the ODD boundary into the enforcement margin, ENVELO takes over. The enforcement mechanism forces the system to a Minimum Risk Condition (MRC) — the safest achievable state given current context. This is not a hard stop; it is a controlled degradation.

- Manufacturer must declare the MRC for each operational context
- ENVELO must force the system toward MRC immediately upon ODD breach
- The enforcement margin between ODD and ENVELO wall is the controlled degradation window
- MRC must be achievable within the enforcement margin
- All Tier 2 events must be logged with timestamp, context, and MRC outcome

Example MRCs by domain: Autonomous vehicle pulls to shoulder. Surgical robot retracts instruments. Drone enters holding pattern. Trading system unwinds positions. Grid AI sheds load by priority.

Tier 3 — ENVELO Wall (Hard Halt)

If the system reaches the ENVELO wall — the absolute outer limit — execution is halted. This is the non-violable failsafe. It activates when MRC fails, when MRC was not fast enough, or when the enforcement mechanism itself encounters an error.

- Halt must be instantaneous and non-bypassable
- No system process may override or delay the halt
- System requires full restart after a Tier 3 event
- Uncertainty defaults to Tier 3 — if ENVELO cannot determine state, halt

3.1 Enforcement Margin

The enforcement margin is the space between the declared ODD boundary and the ENVELO wall. This margin is the controlled degradation window where ENVELO has detected a violation and is actively driving the system to MRC. The width must be sufficient for the system to achieve MRC under worst-case conditions.

4. Verification

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

- Tier 1: Self-correction activates correctly on boundary approach
- Tier 2: MRC achieved within enforcement margin on ODD breach
- Tier 3: Hard halt activates when MRC is insufficient
- No bypass pathways exist (negative testing)
- Audit records generated for all enforcement events and tier transitions

— End of Document —