SENTINEL AUTHORITY

CAT-72 Procedure

Conformance Assessment Test

February 2026 — Confidential

CAT-72 Procedure Conformance Assessment Test CAT-72 is the formal evidentiary procedure establishing that an autonomous system operates within its Operational Design Domain with ENVELO-compliant three-tier enforcement. CAT-72 supports both prescriptive boundaries (operator-specified) and adaptive boundaries (auto-discovered through the ENVELO Interlock's learning mode). Completion is mandatory for ODDC determination. No waivers are issued.

1. Purpose and Scope

CAT-72 serves three functions:

- Evidentiary Demonstration: System maintains bounded operation across operational regimes
- Enforcement Verification: All three ENVELO enforcement tiers activate correctly
- Audit Generation: Cryptographically sealed records suitable for underwriting and incident reconstruction This procedure applies to all applicants seeking initial ODDC determination or renewal. Partial completion does not satisfy requirements.

2. Certification Paths

Adaptive Path (Default) The ENVELO Interlock connects and enters learning mode. During learning, telemetry is collected and profiled — no enforcement is active. The system operates normally while the Interlock auto-discovers operational boundaries (numeric ranges, categorical sets, boolean requirements, rate-of-change limits, geofences, and connectivity heartbeats). The operator reviews the auto-generated boundaries, approves them, and the 72-hour enforcement window begins. The operator's proprietary algorithms, source code, and decision logic are never accessed.

Prescriptive Path The operator defines ODD boundaries upfront — typically required for regulatory mandates or contractual obligations. Enforcement begins immediately against the specified boundaries.

3. Test Duration

Parameter Standard Extended Minimum Duration 72 hours (4,320 minutes) Up to 168 hours Continuity Cumulative (active intervals)

Cumulative (active intervals) Applicability Standard risk profiles High-risk domains, complex ODDs

3.1 Interruption Events

Any of the following events constitute an interruption requiring test restart:

- System shutdown, restart, or power cycle (planned or unplanned)
- Loss of evidentiary recording for any duration
- Manual override or intervention (except emergency safety stops)
- Tier 3 ENVELO enforcement activation resulting in system halt
- Loss of communication with Sentinel Authority witness infrastructure
- Any modification to system configuration, ODD parameters, or enforcement settings

4. Demonstration Requirements

4.1 Phase 1 — Continuous Demo (Hours 0–24)

The system operates for 24 continuous hours under normal conditions within its ODD. The system's own internal safeguards handle any approach to the ODD boundary. ENVELO monitors without intervention.

Convergence Criteria:

- Mean operating point stability within tolerance bands
- Variance bounded within limits for all critical state variables
- No excursions beyond ODD boundaries
- Tier 1 self-correction events observed and logged
- Continuous hash chain integrity maintained

4.2 Phase 2 — Stress Testing (Hours 24–48)

Edge conditions are introduced to force the system toward and across ODD boundaries. This phase verifies that ENVELO's Tier 2 enforcement correctly intervenes when the system breaches the ODD, decelerating it to a Minimum Risk Condition before reaching the ENVELO wall.

Success Criteria:

- Boundary approach scenarios show correct Tier 1 self-correction
- All ODD breaches trigger Tier 2 (MRC) response
- MRC achieved within enforcement margin for all events
- System recovers from MRC to normal operation
- All enforcement events logged with full context

4.3 Phase 3 — Enforcement Proof (Hours 48–72)

This phase verifies the complete enforcement chain including hard halt. Conditions are created where MRC is insufficient to verify Tier 3 behavior.

Success Criteria:

- Tier 3 hard halt activates when MRC is insufficient
- Halt is instantaneous and non-bypassable
- System requires full restart after halt
- Negative testing confirms no bypass pathways exist
- ENVELO correctly defaults to halt on uncertainty
- Complete audit trail covers all three tiers

5. Evidence Requirements

Artifact Format Integrity Telemetry Log Time-series state data Cryptographically signed State Recordings Snapshot sequence Hash-chain linked Tier Transition Events Tier level + context + action Timestamped + signed MRC Records Defined vs. achieved MRC state Timestamped + signed Convergence Metrics Statistical summary Boundary proximity calc

6. Tolerance Declaration

For the prescriptive path, operators specify operational tolerances and MRC definitions prior to CAT-72 based on:

- Equipment manufacturer specifications
- Applicable regulatory requirements
- Risk profile and consequence severity
- Industry standards and best practices
- MRC definition for each operational context For the adaptive path, tolerances are auto-discovered during the learning phase and presented to the operator for review and approval. In both cases, tolerances and MRC definitions cannot be modified during the enforcement test period.

IMPORTANT: Tolerances and MRC definitions cannot be modified during the test period.

— End of Document —