SENTINEL AUTHORITY

CAT-72 Procedure

Conformance Assurance Test

February 2026 — Confidential

CAT-72 is the formal evidentiary procedure verifying that an autonomous system's enforcement mechanisms hold within its Operational Design Domain under sustained operation. The test accumulates 72 cumulative hours of system operation under active interlock enforcement. The clock runs only when the system is actively operating within its deployment context. Completion is mandatory for ODDC determination. No waivers are issued.

Field	Details
Document	CAT-72 Procedure v5.0
Classification	Confidential
Effective Date	February 2026
Identifier	SA-CAT-5.0
Supersedes	SA-CAT-4.0
Owner	Sentinel Authority — Conformance Operations
Contact	conformance@sentinelauthority.org

1. Purpose and Scope

CAT-72 serves three functions:

- Evidentiary Demonstration: The system maintains bounded operation across operational regimes for a minimum of 72 cumulative hours of system operation under active interlock enforcement.
- Verification of Enforcement Mechanisms: All three ENVELO enforcement tiers activate correctly — Tier 1 (self-correction on boundary approach), Tier 2 (Minimum Risk Condition on ODD breach), and Tier 3 (hard halt at the ENVELO wall).
- Audit Generation: Cryptographically sealed records suitable for underwriting review, regulatory inspection, and incident reconstruction.

This procedure applies to all applicants seeking initial ODDC determination or renewal. Partial completion does not satisfy requirements. There is no conditional pass, provisional certification, or graded outcome.

2. Certification Paths

2.1 Adaptive Path (Default)

The ENVELO Interlock connects and enters learning mode. During learning, telemetry is collected and operational boundaries are auto-discovered — no enforcement is active. The system operates normally while the Interlock profiles numeric ranges, categorical sets, boolean requirements, rate-of-change limits, geofences, and connectivity heartbeats. A Sentinel Authority Conformance Engineer reviews the auto-generated boundaries, the operator approves them, and the enforcement test period begins. The operator’s proprietary algorithms, source code, and decision logic are never accessed.

2.2 Prescriptive Path

The operator defines ODD boundaries upfront — typically required for regulatory mandates or contractual obligations. A Sentinel Authority Conformance Engineer reviews the submitted boundaries for minimum specificity requirements (at least one quantitative boundary with measurable threshold, defined unit, and enforcement action). Once approved, enforcement begins immediately against the specified boundaries.

In both paths, once boundaries are locked for testing, they cannot be modified during the enforcement test period. This eliminates the possibility of adjusting pass/fail criteria mid-assessment.

3. Test Duration

3.1 Cumulative Hours

Parameter	Standard	Extended
Minimum Duration	72 cumulative hours of system operation	Up to 168 cumulative hours
Clock Behavior	Runs only during active operation. Pauses when system is idle, powered down, parked, or between operational shifts.	Same cumulative model
Applicability	Standard risk profiles	High-risk domains, complex ODDs, regulatory requirements

The 72-hour requirement is cumulative across operational intervals. A system that operates 8 hours per day accumulates 72 hours across 9 operational days. The clock does not reset on shutdown or power cycle — it pauses and resumes when operation resumes. This reflects real-world deployment patterns where systems do not operate continuously.

3.2 Clock Pause Events

The following events pause the cumulative clock without resetting it. The test resumes from the accumulated total when operation resumes:

- System shutdown, power-down, or sleep (planned maintenance, end of shift)
- System idle or parked between operational intervals
- Scheduled maintenance windows
- Environmental conditions outside ODD (e.g., weather) that prevent operation

3.3 Clock Reset Events

The following events reset the cumulative clock to zero. The entire test must be restarted:

- Loss of evidentiary recording for any duration during active operation
- 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 during active operation
- Any modification to system configuration, ODD parameters, or enforcement settings
- Modification of locked tolerances or MRC definitions

IMPORTANT: A Tier 3 hard halt resets the clock because it indicates a fundamental enforcement event that requires investigation before the system can demonstrate sustained conformance. Emergency safety stops initiated by human operators do not reset the clock, as they represent appropriate human oversight rather than system failure.

4. Demonstration Requirements

CAT-72 testing proceeds through three demonstration phases. These phases accumulate sequentially within the cumulative hour total — they are not rigid time blocks. A Sentinel Authority Conformance Engineer determines when sufficient evidence has been gathered in each phase to advance to the next.

4.1 Phase 1 — Continuous Demonstration

The system operates 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

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

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. Pass/Fail Criteria

Conformance determination is binary: conform or does-not-conform. The following conditions must all be satisfied for a CONFORM determination:

Criterion	Requirement
Cumulative Hours	Minimum 72 cumulative hours of system operation completed without clock reset.
Tier 3 Violations	Zero Tier 3 (hard halt) events during the enforcement test period. Any Tier 3 event resets the clock.
Tier 2 Response	Every ODD breach triggered successful Tier 2 MRC response within the enforcement margin.
Audit Chain	Uninterrupted tamper-evident audit chain for the entire test duration. No gaps in evidentiary recording.
Parameter Coverage	All declared ODD parameters reporting throughout the test. No silent parameters.
Boundary Integrity	Locked tolerances and MRC definitions unchanged from pre-test specifications.

Failure on any criterion results in a does-not-conform determination. The applicant's only recourse is to remediate and retest. No individual at Sentinel Authority has the authority to override a does-not-conform determination.

6. 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
Clock Accumulation Log	Start/pause/resume events	Timestamped + signed

7. 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, and MRC definition for each operational context.

For the adaptive path, tolerances are auto-discovered during the learning phase, reviewed by a Sentinel Authority Conformance Engineer, and presented to the operator for approval. The operator may request adjustments before locking, but once locked, tolerances are final for the test period.

IMPORTANT: Tolerances and MRC definitions cannot be modified during the enforcement test period. Any modification resets the clock to zero.

8. Conformance States

During the CAT-72 process, the system transitions through defined conformance states:

State	Description	Trigger
OBSERVE	Interlock connected, learning mode active. Telemetry collected, no enforcement.	Interlock deployment
BOUNDED	Boundaries locked, enforcement active, cumulative clock running.	Boundary approval + lock
CONFORMANT	72 cumulative hours completed, all pass/fail criteria met. Certificate issued.	Successful CAT-72 completion
PAUSED	System not actively operating. Clock paused. Resumes on next active interval.	System idle / powered down

9. Related Documents

Document	Version	Relationship
ODDC Standard Specification	v1.0	Normative requirements that CAT-72 verifies
ENVELO Interlock Requirements	v3.0	Enforcement architecture that CAT-72 tests
ODDC Certification Guide	v5.0	Complete process guide including CAT-72 context
Governance & Independence Statement	v1.0	Independence controls governing CAT-72 execution
ODDC Overview	v4.0	Framework summary referencing CAT-72

— End of Document —