ODDC Critical Q&A;

Answers to Stakeholder Questions

Version 1.0 · February 2026 · Public Document

Document Purpose

This document addresses the most common and critical questions stakeholders raise about the ODDC framework. It is intended for regulators, insurers, enterprise partners, legal counsel, and technology evaluators.

Q1: Is ODDC a safety certification?

No. ODDC does not attest that a system is safe. It attests that a system operates within its declared Operational Design Domain. Safety is a property of the boundaries themselves—which are defined by the operator and evaluated by domain-specific regulators. ODDC verifies enforcement; domain experts verify adequacy.

Q2: How is ODDC different from ISO 42001, NIST AI RMF, or SOC 2?

Those frameworks verify that organizations have the right processes, policies, and governance structures in place. They are process attestation frameworks. ODDC verifies that deployed systems actually behave within declared constraints—behavioral attestation. They are complementary, not competing. An organization can be fully ISO 42001 certified and still deploy a system that exceeds its operational design domain, because no mechanism in ISO 42001 enforces boundaries at runtime.

Q3: What does ‘conformance’ mean in this context?

Conformance means the system operates within 100% of its declared boundary parameters for at least 95% of operational time, with all boundary exceedances handled by the three-tier enforcement cascade (self-correction, minimum risk condition, hard halt). It is a quantitative determination, not a subjective judgment.

Q4: Who defines the boundaries?

The operator defines the boundaries. Sentinel Authority does not tell operators what their boundaries should be. Operators define the conditions under which their system is designed to operate; Sentinel Authority independently verifies that the system actually stays within those conditions.

Q5: Can the operator game the boundaries?

An operator can set artificially wide boundaries, but this creates its own problems: regulators, insurers, and customers can evaluate the declared boundaries and determine whether they are appropriate for the use case. ODDC provides transparency—the boundaries are documented, the conformance is verified, and the evidence is

independently reviewable. Gaming the boundaries is visible.

Q6: What if a system fails CAT-72?

The operator receives a detailed findings report identifying specific enforcement failures. They may remediate the identified issues and re-test. Each re-test is a separate engagement. There is no partial certification or conditional pass—the system is either CONFORMANT or NON-CONFORMANT.

Q7: Does ODDC require changes to the autonomous system itself?

ODDC does not require changes to the autonomous system's core software, algorithms, or architecture. The ENVELO Interlock operates alongside the system, observing telemetry and enforcing boundaries externally. It does require that the system expose operational telemetry that the Interlock can ingest.

Q8: How does this help insurers?

ODDC provides independent, quantitative conformance data that insurers can use for risk differentiation. Instead of relying on operator self-attestation, underwriters have verifiable evidence of whether a system operates within declared boundaries. This enables risk-differentiated pricing: conformant systems present lower risk than non-conformant ones.

Q9: How does this help regulators?

ODDC gives regulators an independent evidentiary basis for oversight. Instead of relying on manufacturer claims, regulators can reference conformance records that document the scope, evidence, and verification of operational boundary enforcement. It also provides a ready-to-reference conformity assessment methodology for frameworks like the EU AI Act that mandate assessment but lack implementation mechanisms.

Q10: Is the ENVELO Interlock itself certified?

The Interlock is validated through the same CAT-72 process. Its enforcement behavior, telemetry integrity, and security properties are tested as part of every certification engagement. The Interlock's code is not open-source, but its requirements are public and its behavior is independently verifiable through the cryptographic evidence chain.

Q11: What happens if a certified system causes harm?

ODDC certification provides objective evidence about whether the system was operating within its declared boundaries at the time of the incident. If it was, the ODDC record supports the operator's position that the system was conformant. If it was not, the ODDC record provides evidence of the boundary exceedance. Either way, it replaces competing claims with verifiable evidence.

Q12: What does ODDC cost?

Initial certification: $12,000. Annual renewal: $12,000. Re-test after failure: $12,000. There are no per-unit, per-vehicle, or per-deployment licensing fees. Pricing is per-system.