ODDC Critical QA

Quality Assurance Checklist

February 2026 — Confidential

Critical Q&A; ODDC Framework — Tough Questions Answered This document addresses the hardest technical, regulatory, and business objections to runtime enforcement and conformance determination for autonomous systems.

Q1: Isn't ODDC just adding cost and complexity to systems that are already safe? "Safe" is not a binary condition—it is a claim. Today, that claim is largely unverifiable at runtime.

ODDC does not add complexity arbitrarily; it adds accountability where accountability is currently absent. In safety-critical domains, the marginal cost of enforcement is negligible compared to the cost of a failure that cannot be reconstructed, explained, or adjudicated.

We have seen this pattern repeatedly: airbags added cost to vehicles, triple-redundant flight controls added cost to aircraft, cryptographic controls added overhead to financial systems. Each was initially dismissed as excessive. Each became mandatory once society decided that provable safety mattered more than marginal efficiency.

Q2: Why can't the AI just police itself? Because self-policing systems fail precisely when trust is most needed.

We do not allow pilots to certify their own flights, banks to audit their own books, or software to attest to its own integrity. An AI enforcing its own limits is a single point of technical, ethical, and legal failure.

ODDC requires ENVELO-compliant enforcement—an independent mechanism that acts as a circuit breaker. It does not evaluate intent or intelligence. It evaluates authority.

Q3: Won't the enforcement layer create new risks? Any safety mechanism introduces risk. The question is how it fails, not whether it can.

ENVELO-compliant enforcement is designed to fail closed. If an action cannot be verified as authorized, it is constrained and the system transitions to a predefined minimal-risk behavior.

Q4: What happens when the AI needs to act outside its ODD in an emergency? If the system needs to act outside its declared ODD, it is not ODDC-conformant for that action.

This is not a bug—it is the design. ODDC attests bounded operation. Emergency behavior outside declared bounds is a different risk profile that requires different governance.

Q5: How is ODDC different from existing safety certifications? ODDC is not a safety certification. It is a conformance determination framework focused on runtime enforcement evidence.

Safety certifications (IEC 61508, ISO 26262) evaluate design processes, hazard analyses, and development lifecycle. ODDC evaluates whether runtime enforcement mechanisms exist and function correctly. The two are complementary, not competing.

Q6: Why 72 hours? Isn't that arbitrary? 72 hours is a minimum threshold, not a magic number. It represents the shortest period that can demonstrate sustained operation across multiple operational cycles.

Sentinel Authority may require extended duration (up to 168 hours) based on risk profile. The principle is evidentiary sufficiency, not calendar convenience.

Q7: What's in it for operators? ODDC provides verifiable evidence of bounded operation that can be used in underwriting, regulatory engagement, and incident response.

Operators with ODDC attestation have a standardized way to demonstrate operational discipline. This can translate to insurance premium reductions, regulatory confidence, and defensible positions in the event of incidents.

— End of Document —