ODDC SCENARIOS

Industry Applications — Sentinel Authority

v1.1

1. Overview

1.1 Purpose

This document presents representative scenarios illustrating how ODDC with ENVELO-compliant enforcement applies across industries. These scenarios demonstrate the range of operational domains, enforcement mechanisms, and evidentiary outputs that characterize ODDC conformance.

1.2 Non-Normative Status

These examples are illustrative and non-normative. They do not define requirements; they illustrate how requirements might be applied. Actual conformance requirements are determined through scope assessment with Sentinel Authority based on specific system characteristics.

1.3 Scenario Structure

Each scenario describes:

- Operational context and autonomous system functions
- Representative ODD boundaries and tolerances
- ENVELO enforcement mechanisms (modeled)
- Evidence outputs for CAT-72 demonstration

2. Data Centers & Hyperscale Computing

2.1 Operational Context

Hyperscale data center environments increasingly rely on autonomous systems to allocate power, optimize cooling, place workloads, and orchestrate AI-on-AI stacks. These systems make real-time decisions affecting facility safety, equipment longevity, and operational continuity.

Autonomous control in data centers presents unique risks: thermal runaway, power cascade failures, and uncontrolled AI recursion. ODDC provides bounded operation assurance for these critical infrastructure systems.

2.2 Representative ODD Boundaries

- Power draw: Per-rack limits (e.g., 20kW), row limits, facility aggregate limits
- Thermal envelope: Inlet temperature ranges, delta-T limits, humidity bounds
- Workload density: Compute density per zone, memory utilization ceilings
- AI recursion: Maximum depth for AI systems managing other AI systems
- Response latency: Maximum decision-to-action time for thermal events

2.3 Representative Interlock Behavior

- Hard-cap interlocks on CPU throttling to prevent TDP overruns during load spikes. Enforcement layer monitors aggregate power draw and blocks workload placement that would exceed rack or row power limits.
- Automatic workload shedding to non-critical queues as facility power approaches envelope limits. Enforcement

layer maintains priority queue and initiates graceful degradation before hard limits.

- Maximum recursion depth for AI managing AI without human checkpoint. Enforcement layer tracks decision provenance and requires human confirmation for decisions exceeding recursion threshold.
- Thermal interlock preventing workload placement when cooling capacity is insufficient. Enforcement layer maintains thermal model and blocks placement in zones approaching thermal limits.

2.4 Evidence Outputs

- Continuous power monitoring telemetry (per-rack, per-row, facility aggregate) at 1 Hz minimum
- Thermal state recording (inlet, outlet, ambient) at 1 Hz minimum
- Workload placement decisions with enforcement evaluation results
- Interlock activation events with full context
- Append-only audit logs with hash-chain integrity

3. Autonomous Vehicles

3.1 Operational Context

Autonomous vehicles operate in dynamic, safety-critical environments where control system failures can result in injury or death. ODDC provides assurance that vehicle behavior remains within mathematically specified authorization parameters regardless of AI model behavior.

ODDC for autonomous vehicles complements (but does not replace) functional safety certification. ODDC addresses bounded operation; functional safety addresses safe operation.

3.2 Representative ODD Boundaries

- Speed limits: Zone-specific ceilings, school zone restrictions, weather-adjusted limits
- Confidence thresholds: Minimum perception confidence for continued autonomous operation
- Weather degradation: Speed and capability restrictions based on visibility, precipitation, road conditions
- Geofencing: Permitted operational zones, restricted areas, mandatory human control zones
- Following distance: Minimum separation based on speed and conditions

3.3 Representative Interlock Behavior

- Non-bypassable speed interlock tied to zone authorization parameters. Enforcement layer receives zone data from mapping system and physically limits motor controller output to zone-permitted speeds.
- Mandatory stop or slowdown when detection confidence falls below envelope threshold. Enforcement layer monitors perception system confidence scores and initiates controlled stop when thresholds are breached.
- Weather-tier degradation limits on velocity and acceleration. Enforcement layer receives weather classification and applies corresponding operational restrictions automatically.
- Geofence enforcement requiring human takeover in restricted zones. Enforcement layer monitors position and initiates handoff procedure when approaching restricted zone boundaries.

3.4 Evidence Outputs

- Vehicle state telemetry (position, velocity, acceleration) at 10 Hz minimum
- Perception system confidence scores at 10 Hz minimum
- Zone authorization state and transitions
- All enforcement activations with triggering conditions
- Cryptographic attestation suitable for accident reconstruction

4. Healthcare & Medical AI

4.1 Operational Context

Medical AI systems operate in life-critical environments where errors can cause patient harm or death. These systems increasingly provide diagnostic recommendations, treatment suggestions, and direct clinical interventions. ODDC provides assurance that AI recommendations and actions remain within clinically appropriate boundaries.

ODDC for medical AI does not replace regulatory approval (FDA clearance, CE marking). It provides an additional layer of runtime assurance for bounded operation.

4.2 Representative ODD Boundaries

- Diagnostic confidence: Minimum confidence thresholds for autonomous recommendations
- Intervention staging: Human confirmation requirements based on intervention severity
- Dosage limits: Maximum medication dosages, rate limits for infusions
- Vital sign boundaries: Alert and intervention thresholds for monitored parameters
- Procedure envelopes: Physical boundaries for robotic surgical assistance

4.3 Representative Interlock Behavior

- Mandatory confirmation interlock for Stage 3+ interventions. Enforcement layer classifies intervention severity and requires documented clinician confirmation before AI-recommended high-impact actions.
- Hard deviation thresholds on surgical trajectories. Robotic systems include enforcement layer that halts motion when trajectory deviates from planned path beyond tolerance.
- Automatic escalation on anomalous vital signs beyond envelope thresholds. Monitoring systems trigger immediate clinician alert and optionally suspend autonomous interventions when patient state approaches boundaries.
- Dosage ceiling enforcement preventing medication delivery beyond protocol limits regardless of AI recommendation.

4.4 Evidence Outputs

- All AI recommendations with confidence scores and supporting data
- Clinician confirmation records for staged interventions
- Continuous vital sign monitoring with boundary proximity
- Procedure telemetry for robotic assistance

- Append-only clinical decision trace with timestamps

5. Financial Services & Trading

5.1 Operational Context

Automated trading systems can execute thousands of transactions per second with minimal human oversight. Uncontrolled algorithmic trading has caused flash crashes and cascading market failures. ODDC provides assurance that trading systems operate within quantifiable risk envelopes.

5.2 Representative ODD Boundaries

- Position limits: Maximum position sizes per instrument, sector, and portfolio
- Concentration thresholds: Maximum percentage of portfolio in correlated positions
- Volatility triggers: VIX-based operational restrictions
- Drawdown caps: Maximum permitted loss before automatic halt
- Order rate limits: Maximum orders per second, maximum notional per time window

5.3 Representative Interlock Behavior

- Volatility-triggered circuit breaker disconnecting order submission channels. Enforcement layer monitors market volatility indicators and physically disconnects trading connectivity when thresholds breach.
- Real-time enforcement of position limits and concentration thresholds. Enforcement layer maintains position state and blocks orders that would exceed limits before submission to exchange.
- Mandatory review triggers on envelope-defined drawdown events. System requires human authorization to resume trading after significant losses.
- Order rate limiting at enforcement layer preventing excessive market impact regardless of algorithm behavior.

5.4 Evidence Outputs

- Complete order flow with enforcement evaluation for each order
- Position state at enforcement layer (independent of trading system)
- All circuit breaker activations with triggering conditions
- Cryptographic attestation suitable for regulatory examination

6. Industrial Manufacturing

6.1 Operational Context

Autonomous robotics and AI-driven production systems operate alongside humans in hazardous environments. Industrial automation presents risks including crushing injuries, chemical exposure, and equipment damage. ODDC provides assurance that robotic systems operate within safety envelopes.

6.2 Representative ODD Boundaries

- Force output: Maximum force and torque for each actuator

- Speed zones: Reduced speed when humans present in workspace
- Proximity thresholds: Minimum distance from detected humans
- Workspace boundaries: Physical limits of permitted robot motion
- Payload limits: Maximum weight and center-of-gravity constraints

6.3 Representative Interlock Behavior

- Proximity-triggered force limiters and full-stop thresholds. Safety-rated sensors detect human presence; enforcement layer reduces force limits or halts motion based on proximity.
- Non-bypassable caps on actuator torque or force output. Enforcement layer physically limits motor current regardless of control system commands.
- Speed reduction zones with enforcement independent of control system. Enforcement layer monitors workspace occupancy and applies speed restrictions automatically.
- Emergency stop integration with tamper-evident logging of all stop events.

6.4 Evidence Outputs

- Continuous robot state telemetry (position, velocity, force) at 10 Hz minimum
- Proximity sensor data and human detection events
- All enforcement activations including force limiting and stops
- Safety zone state and transitions
- Audit log suitable for incident investigation

7. Aerospace & Defense

7.1 Operational Context

Autonomous aircraft and mission systems require strict operational certainty due to consequences of uncontrolled behavior. These systems operate in environments where recovery from errors may be impossible. ODDC provides assurance that autonomous aerospace systems maintain bounded operation.

7.2 Representative ODD Boundaries

- Geofencing: Permitted flight zones, restricted airspace, international boundaries
- Altitude limits: Ceiling and floor constraints, terrain clearance
- Communication requirements: Maximum permitted comm-loss duration
- Payload authorization: Multi-party release requirements
- Fuel reserves: Minimum fuel state for continued autonomous operation

7.3 Representative Interlock Behavior

- Geofence-triggered return-to-base initiation. Enforcement layer monitors position against permitted zones and initiates automatic RTB when approaching boundaries.
- Mandatory RTB after defined comm-loss duration. Enforcement layer maintains independent timer and initiates

return procedure when communication timeout exceeds threshold.

- Multi-party cryptographic release for payload authorization. Enforcement layer requires valid cryptographic credentials from multiple authorized parties before permitting payload deployment.
- Fuel reserve enforcement preventing mission continuation below minimum fuel state.

7.4 Evidence Outputs

- Complete flight telemetry with position, altitude, and system state
- Communication state log with all timeout events
- Geofence evaluation for entire flight path
- Authorization records for all payload events
- Cryptographically signed compliance logs for post-mission audit