Technical Product Requirements

CJADC2 Orchestration Platform

Version: 1.0 **Author:** John Sasser **Status:** Draft for Review

Table of Contents

1. Executive Summary

The CJADC2 (Combined Joint All-Domain Command and Control) Machine-to-Machine Orchestration Platform is an MVP event-driven system designed to accelerate complex mission decision chains. The platform coordinates six autonomous agents through a secure messaging backbone, treating **"Sensor Data as a Product"** while maintaining strict human-in-the-loop approval for all effects.

Mission Chain: Sensor → Classify → Correlate → Plan → Request-Approval → Dispatch

2. Goals and Non-Goals

Goals

PRIORITY	GOAL	SUCCESS CRITERIA
P0	**End-to-End Orchestration**	Demonstrate full event-driven pipeline from sensor detection to effect execution
P0	**Human-in-the-Loop**	Enforce human approval for 100% of proposed actions before execution
P0	**Policy Enforcement**	OPA/Rego evaluation at every pipeline stage with 100% coverage
P1	**Sub-3s Latency**	Detection-to-decision latency < 3 seconds (p95) on commodity hardware
P1	**At-Least-Once Delivery**	Message delivery with idempotent handlers via NATS JetStream
P2	**Full Observability**	Correlation IDs, Prometheus metrics, and distributed tracing end-to-end

Non-Goals

EXCLUDED	RATIONALE
Real-world sensor/targeting integration	MVP uses synthetic data only; no connection to operational systems
Production HA/DR	Focus on functional demonstration, not operational resilience
Multi-tenant RBAC	Single-tenant with HIL approval is sufficient for MVP scope
ML pipelines or streaming analytics	Out of scope for initial platform demonstration

3. Target Users

Mission Operator

Monitors decision chain and approves/denies proposed actions

PRIMARY

NEEDS

- Clear UI for action review and approval workflow
- Real-time situational awareness dashboard
- Audit trail visibility for all decisions

SUCCESS CRITERIA

- All effects blocked without explicit human approval
- Correlation IDs trace any event end-to-end

System Integrator

Deploys, configures, and extends the platform

TECHNICAL

NEEDS

- Comprehensive API documentation
- Extensible agent architecture
- Configuration management via environment variables

SUCCESS CRITERIA

- New agents can be added following BaseAgent pattern
- Prometheus metrics available for all agents

4. Key Performance Indicators

< 1.5s
Detection-to-Decision p50 latency

< 3.0s
Detection-to-Decision p95 latency

≥ 1K
Messages/Minute Throughput target

CATEGORY	METRIC	TARGET	MEASUREMENT
Latency	End-to-End (p95)	< 5.0s	Sensor emission to Effector execution (excluding HIL wait)
Throughput	Concurrent Tracks	≥ 100	Active tracks in correlation window
Throughput	Proposal Queue	≥ 50	Pending HIL approvals
Reliability	Message Delivery	At-least-once	NATS JetStream store-and-forward
Reliability	Handler Idempotency	100%	Duplicate messages produce identical outcomes
Coverage	Policy Evaluation	100%	Every message evaluated against OPA policies

5. System Architecture

Technology Stack

COMPONENT	TECHNOLOGY	PURPOSE
Messaging	NATS JetStream + mTLS	Secure, persistent pub/sub messaging
Policy Engine	OPA/Rego	Declarative policy enforcement
Persistence	PostgreSQL	Event store, track state, audit log
Agents	Go	High-performance event processors
UI	React + WebSocket	Real-time operator dashboard
Observability	Prometheus + OpenTelemetry	Metrics, tracing, alerting

Agent Pipeline

Figure 5.1: Event-driven agent pipeline with Human-in-the-Loop approval gate

AGENT	INPUT	OUTPUT	RESPONSIBILITY
Sensor Sim	Timer/Config	Detection Event	Emit synthetic detections with random tracks and confidence scores
Classifier	Detection	Track Event	Enrich detections with type classification and confidence updates
Correlator	Track Event	Correlated Track	Deduplicate and merge tracks within 10-second windows
Planner	Correlated Track	ActionProposal	Generate proposed responses based on track characteristics
Authorizer	ActionProposal	Approved Action	Present proposals for human approval/denial via UI
Effector	Approved Action	Effect Log	Execute simulated effects and log state transitions

6. Safety & Threat Model

Safety Constraints

Safety Invariants

- **No ActionProposal proceeds to Effector without explicit human approval**
- All effects are simulated and produce only log entries and state transitions
- Correlation IDs trace every event from sensor to effect for auditability
- Policy violations halt processing and generate alerts

CONSTRAINT	IMPLEMENTATION	RATIONALE
Synthetic Data Only	All sensor data is randomly generated	No connection to real-world systems
No Real-World Targeting	Effects are log-only simulations	Platform has no external system integration
Human-in-the-Loop Required	Authorizer blocks until operator approval	No autonomous effect execution permitted
Full Audit Trail	All decisions logged with correlation IDs	Complete traceability for review

Threat Mitigations

THREAT CATEGORY	MITIGATION	MVP STATUS
Message Tampering	mTLS encryption for all NATS communication	⚠️ Deferred (non-goal NG2)
Unauthorized Access	Certificate-based authentication for agents	⚠️ Using HMAC signing instead
Policy Bypass	Mandatory OPA evaluation at each pipeline stage	✅ Implemented
Replay Attacks	Idempotent handlers with deduplication keys	✅ Implemented
Audit Evasion	Immutable PostgreSQL audit log with correlation IDs	✅ Implemented

Note: mTLS and certificate-based authentication are deferred per non-goal NG2 (production-grade HA). The MVP uses HMAC-SHA256 message signing for integrity verification.

7. Success Criteria

MVP Acceptance

STATUS	CRITERION
✅	Full pipeline executes from Sensor Sim to Effector with HIL approval
✅	Detection-to-decision p95 latency < 3 seconds on laptop
✅	Sustained throughput ≥ 1,000 messages/minute
✅	All effects blocked without human approval
✅	Correlation IDs trace end-to-end for any event
✅	Prometheus metrics available for all agents
✅	Policy enforcement demonstrated at each stage

Status: All MVP acceptance criteria have been met. The platform successfully demonstrates end-to-end event-driven orchestration with human-in-the-loop approval.

Beyond MVP: Additional Capabilities

The following capabilities were implemented beyond the original PRD scope:

FEATURE	DESCRIPTION
Sensor Runtime Configuration	HTTP API for adjusting emission rates, track counts, and type distributions at runtime
Proposal De-duplication	Consolidates multiple sensor hits on the same track into single proposals with hit counting
Metrics Dashboard	Real-time pipeline metrics including per-stage latency percentiles and queue depths
Track History API	Historical detection positions for individual tracks
Audit Trail UI	Searchable, filterable audit log with grouping and timeline views
Consumer Resilience	Automatic NATS consumer recreation on failure for improved reliability
Classification Biasing	Special handling for missile tracks with configurable classification weights

A. Appendix: Glossary

CJADC2
Combined Joint All-Domain Command and Control

HIL
Human-in-the-Loop

OPA
Open Policy Agent

mTLS
Mutual Transport Layer Security

Correlation ID
Unique identifier tracing events through the pipeline

ActionProposal
Suggested response awaiting human approval

Effect
Simulated outcome of an approved action

JetStream
NATS persistence layer for at-least-once delivery