A³O

ARCHITECTURE BASELINE

A³O Architecture Baseline R1.2

FULL MASTER — JAUS Integrated

Universal Trusted Framework for Heterogeneous Autonomous Ecosystems

DOCUMENT ID	A3O-ARCH-JAUS-1200
VERSION / STATUS	R1.2 · FULL MASTER · CANDIDATE
LANGUAGE	ENGLISH
CLASSIFICATION	INTERNAL / PARTNER REVIEW
RELEASE DATE	17 JUL 2026
SOURCE BASELINE	R0.1 FULL MASTER STAGE 1 · PRESERVED IN FULL

COORDINATE ANY MACHINE. GOVERN EVERY MISSION. PROVE EVERY ACTION.

RELEASE MANAGEMENT

Document Control and Release Governance

Field	Controlled value
Document identity	A3O-ARCH-JAUS-1200
Title	A^{3}O Architecture Baseline R1.2 FULL MASTER — JAUS Integrated
Status	Candidate architecture baseline for controlled technical review
Source preservation	All text and tables from A3O Master Architecture Baseline R0.1 FULL MASTER STAGE 1 are retained in Part II.
Normative precedence	Part I and the R1.2 overlay clauses supersede conflicting R0.1 clauses. Non-conflicting R0.1 clauses remain applicable.
Compatibility claim	JAUS-aligned target architecture and implementation profile; not a claim of SAE certification or endorsement.
Language	English master
Owner	A^{3}O Systems Architecture
Review domains	Architecture, software, safety, security, integration, verification, product and legal/licensing

STANDARDS AND LICENSING BOUNDARY

This baseline uses public SAE scope information to define an architecture. Detailed wire formats, message fields, JSD artifacts, data sets and formal compliance criteria shall be implemented only from appropriately licensed SAE documents and associated data products.

Release objectives

- Preserve the complete R0.1 FULL MASTER architecture baseline rather than replacing it with a summary.
- Introduce JAUS as a native interoperability domain, not as a superficial protocol adapter.
- Define A^{3}O as the upper-level trust, policy, orchestration, state and evidence layer for JAUS and non-JAUS autonomous systems.
- Make message transformation, authority, safety, versioning and evidence behavior explicit and testable.
- Extend the architecture from security-focused deployments to logistics, manufacturing, inspection, medical robotics and multi-domain autonomous operations.
- Provide a traceable path from source sections to new requirements, components, tests and implementation work packages.

NAVIGATION

Controlled Structure

on	Title
T I	R1.2 JAUS-Integrated Architecture Baseline
	Executive Architecture Statement
	A3O-1000 Foundation, Standards Alignment and Governance
	A3O-1200 Semantic and Ontology Architecture
	A3O-1300 Information and Data Contract Architecture
	A3O-1400 Capability and Industry Profile Architecture
	A3O-2000 Reference Architecture and JAUS Interoperability Domain
	A3O-2100 Runtime and Edge Architecture
	A3O-2200 Policy, Delegation and Human Authority

on	Title
	A3O-2300 AI and Cognitive Services
	A3O-2400 Swarm and Distributed Coordination
	A3O-2500 Safety, Resilience and Assurance
	A3O-3000 System and Component Architecture
	A3O-4000 Cross-Industry Solution Blueprints
	A3O-5000 Conformance, Certification Readiness and Metrics
	A3O-6000 Governed Learning and Adaptation
	A3O-7000 Federated Autonomous Ecosystems
	A3O-8000 Extreme, Contested and Strategic Operations
	A3O-9000 Schemas, SDKs, Annexes and Test Assets
	Implementation Roadmap and Release Gates
	Change and Traceability Matrix
T II	Preserved R0.1 FULL MASTER Baseline with R1.2 JAUS Overlays
EX A	Normative Requirement Catalogue
EX B	Standards Baseline and Bibliography

NORMATIVE MODERNIZATION

Part I — R1.2 JAUS-Integrated Architecture Baseline

A3O-0000

1. Executive Architecture Statement

A^{3}O is defined as a universal trusted framework for the management, coordination, safety and evidence-based operation of heterogeneous autonomous systems. The framework is deliberately independent of any single vehicle type, robot vendor, communication medium or mission domain. Its governing operating model is Observe → Understand → Coordinate → Decide → Authorize → Execute → Verify → Learn.

R1.2 introduces JAUS as a native interoperability domain. JAUS supplies formally defined service interfaces, component discovery, message interaction patterns, lifecycle management and control ownership. A^{3}O remains the upper-level authority for identity binding, mission context, policy enforcement, human authorization, multi-platform coordination, shared world state, digital-twin projection and operational evidence.

The architecture therefore separates connectivity from trust. A JAUS component can be discovered and decoded without being accepted as trusted, safe, authorized or mission-eligible. Operational admission requires an A^{3}O identity, an approved service/version profile, a valid security and safety posture, an assigned ecosystem, and an authority context appropriate to the requested action.

PRIMARY TECHNOLOGY THESIS

A^{3}O is the next-generation JAUS-compatible software core for trusted multi-vendor autonomy. It extends JAUS interoperability with policy-controlled autonomy, ecosystem-scale orchestration, human authority and evidence by design.

1.1 Architectural division of responsibility

Layer	Responsibility
JAUS standards and JSDs	Define service interfaces, message protocols, addressing, discovery, access control, management and domain capabilities.
A^{3}O JAUS Interoperability Domain	Implements transport, schema registry, discovery bridge, authority broker, event bridge and semantic transformation while preserving JAUS semantics.
A^{3}O Trust and Identity Plane	Binds protocol addresses to persistent global identities, ownership, attestation, ecosystem and mission context.
A^{3}O Mission, Policy and Safety Planes	Determine whether a capability may be used, who may control it, under which constraints, for how long and with what evidence.
A^{3}O State, Knowledge and Evidence Planes	Build shared operational state, retain provenance, correlate decisions and actions, and support replay and assurance.
Industry profiles	Add domain-specific semantics, workflows, risk controls, compliance overlays and conformance tests without altering the universal core.

1.2 Platform-independence rule

Mission logic, user experience and assurance logic shall depend on canonical capabilities and state objects, not directly on vendor-specific APIs or transport endpoints. Vendor or JAUS-specific details terminate at the interoperability boundary. Where a standard JAUS service exactly represents the required capability, the applicable standard service shall be preferred. Where no applicable service exists, the implementation shall use a clearly namespaced A^{3}O extension or a non-JAUS adapter and shall never present the extension as an SAE-standard interface.

1.3 Compatibility and certification language

Until implementation and test evidence exist, the permitted language is “JAUS-aligned architecture”, “JAUS compatibility target” or “designed for JAUS integration”. “Certified”, “approved by SAE”, “SAE-compliant” or equivalent language shall not be used unless the precise claim, test scope, evidence and issuing body are identified. Industry regulatory authorization remains separate from JAUS interoperability.

2. A3O-1000 — Foundation, Standards Alignment and Interoperability Governance

A3O-1000 establishes the architectural rules by which JAUS becomes a controlled interoperability domain inside the wider A³O ecosystem. The domain is not allowed to redefine the mission model, bypass local safety mechanisms, or create authority merely because a message can be transported and decoded.

2.1 Standards baseline

Reference	Public title	Public status as verified 17 Jul 2026	DOI
AIR5665C	Architecture Framework for Unmanned Systems	Stabilized May 2024	10.4271/AIR5665C
AS5669A	JAUS / SDP Transport Specification	Reaffirmed April 2019	10.4271/AS5669A
AS5684B	JAUS Service Interface Definition Language	Reaffirmed April 2025	10.4271/AS5684B
AS5710A	JAUS Core Service Set	Reaffirmed April 2015	10.4271/AS5710A
AS6009A	JAUS Mobility Service Set	Revised October 2023	10.4271/AS6009A
AS6057A	JAUS Manipulator Service Set	Reaffirmed April 2025	10.4271/AS6057A
AS6060A	JAUS Environment Sensing Service Set	Reaffirmed May 2026	10.4271/AS6060A
AS6062A	JAUS Mission Spooling Service Set	Reaffirmed March 2024	10.4271/AS6062A
AS6091	JAUS Unmanned Ground Vehicle Service Set	Reaffirmed April 2025	10.4271/AS6091
AS6111	JAUS Unmanned Maritime Vehicle Service Set	Issued September 2023	10.4271/AS6111
AS8024	JAUS Autonomous Capabilities Service Set	Reaffirmed April 2025	10.4271/AS8024
ARP6227	JAUS Messaging over OMG DDS	Reaffirmed March 2024	10.4271/ARP6227

CRITICAL CORRECTION

AS-4JAUS is the SAE committee designation, not a single standard. AS5684B defines JSIDL. AS5710A defines the Core Service Set. AS5669A defines the JAUS/SDP transport specification.

2.2 Governing principles

	Principle	Normative interpretation
001	Preservation of semantics	A³O shall preserve the source service, message identity, source and destination address, applicable version and interaction semantics.
002	Discovery is not trust	A discovered entity is a candidate capability until identity, profile, safety and ownership che are complete.
003	Authority does not expand through translation	An adapter may reduce authority or reject a request; it shall not grant authority unavailable the source or target.
004	Local safety precedence	Physical interlocks and certified local safety functions retain precedence over remote missio optimization.
005	Evidence at runtime	Raw messages, decoding versions, semantic transformations, policy decisions, outgoing commands and outcomes shall be correlated at runtime.
006	Explicit extensions	A³O-specific services use controlled namespaces and are distinguishable from standard JAU services.
007	Fail closed on ambiguity	Unknown or ambiguous service versions, coordinate frames, units, authority or state shall n produce control actions.
008	Multi-protocol parity	JAUS, DDS, ROS, OPC UA, MQTT, REST and vendor interfaces are normalized into the same p and evidence model.

2.3 Identity and address model

JAUS addressing is treated as a protocol-local routing identity. A³O introduces a persistent global identity that remains stable when the address, network, controller or vendor implementation changes. The binding record includes ecosystem, organization, physical asset, subsystem/node/component address, service inventory, certificate or attestation reference, trust state, lifecycle state and revocation status.

2.4 JSIDL and service-definition governance

- The controlled JSIDL Registry is the source of truth for imported service definitions, dependencies, namespaces, versions and generated bindings.
- Only licensed and provenance-recorded service artifacts may be promoted to an operational registry.
- Every decoder and encoder build shall identify the exact service-definition package and generation toolchain used.
- A change of JSD version, generated codec, transformation rule or unit/frame mapping is an architecture-controlled change and requires regression evidence.
- Custom A³O services shall use an A³O namespace, a documented compatibility policy and a distinct conformance profile.

2.5 Architecture decision and traceability rule

Every JAUS integration decision shall be traceable through Requirement → Capability → Standard or Extension → Service Definition → Runtime Component → Test Case → Evidence → Release. When an A³O capability can be satisfied by more than one JAUS service or version, an Architecture Decision Record shall document the selection, exclusions, semantic mapping and transition strategy.

A3O-1200

3. A3O-1200 — Semantic and Ontology Architecture

The semantic architecture prevents protocol terminology from leaking into mission logic. A³O represents what an entity is, what it can do, what state it reports and what authority is required. JAUS terminology is retained for protocol fidelity and mapped to canonical A³O concepts for cross-protocol reasoning.

JAUS concept	A³O canonical concept	Interpretation
JAUS Subsystem	Managed Autonomous Platform	Robot, UxV, production cell, medical robot or autonomous machine.
JAUS Node	Edge Compute Node	Onboard computer, controller, server or certified compute partition.
JAUS Component	Capability Endpoint	Addressable software entity providing one or more services.
JAUS Service	Capability Contract	Formal interface, message set and interaction protocol.
JSD / JSIDL	Service Schema Artifact	Machine-readable service definition and version.
JAUS Address	External Protocol Identity	Local routing identity scoped by ecosystem and platform.
Command	Governed Action Request	State-changing request subject to policy, safety and authority.
Query	State Information Request	One-shot information retrieval with correlation and timeout.
Report	Observation Event / State Delta	Validated response or state update.
Event	Live State Subscription	Asynchronous update stream with lifecycle and rate controls.
Access Control	Authority Lease	Preemptable control ownership represented in A³O policy and evidence.
Management	Lifecycle Transition	Controlled component-state transition.

3.1 Semantic mapping record

Each mapping is a versioned architectural artifact. It identifies source service and version, source field path, unit, coordinate frame, validity conditions, canonical target field, uncertainty transformation, loss-of-information declaration, and reverse-encoding constraints. A mapping is not considered safe merely because all fields can be parsed.

3.2 Coordinate, unit and time semantics

- Coordinate frames shall be explicitly identified and transformed through a registered frame graph. Missing or ambiguous frames fail closed for control use.
- Units shall be normalized into a declared canonical system while retaining the source value and unit in evidence.
- Source time, receive time, transformation time and trusted-time status shall be recorded separately.
- Uncertainty, validity, quality and staleness are first-class fields; they shall not be silently discarded.
- Live, simulated, forecast, training and replay data shall remain distinguishable in identity and state semantics.

3.3 Ontology extension policy

Industry profiles may extend the universal ontology with domain objects such as cargo custody, production recipe, patient-independent payload status, environmental sample, perimeter sector or mission task. Extensions shall declare ownership, privacy classification, safety relevance and mapping to shared concepts such as Entity, Capability, State, Mission, Action, Evidence and Authority.

A3O-1300

4. A3O-1300 — Information and Data Contract Architecture

A3O-1300 defines how source protocol messages become trustworthy operational information. The canonical data fabric never replaces the source message. It carries a decoded representation and state delta while retaining a cryptographic reference to the raw input and the exact decoding and mapping artifacts.

4.1 JAUS-aware message pipeline

1. Transport reception and immutable raw capture
2. JAUS frame identification and source/destination address resolution
3. Service and message lookup in the controlled JSIDL Registry
4. Decode, structural validation and declared-version validation
5. Discovery/capability correlation and A^3O identity binding
6. Trust, classification, privacy and mission-context enrichment
7. Access Control, authority and lifecycle-state evaluation
8. Unit, coordinate-frame and semantic normalization
9. Canonical envelope and state-delta creation
10. Routing to state, event, mission, UI, twin and evidence consumers
11. Governed command generation, JAUS encoding and transport transmission
12. Feedback correlation, outcome assessment and evidence finalization

4.2 Canonical JAUS envelope

ILLUSTRATIVE INTERNAL A³O REPRESENTATION


```
{
 "envelope_version": "a3o.jaus.v1",
 "message_id": "018f2aa0-42c7-7c63-a10e-82b104b5f120",
 "protocol": {
  "family": "JAUS",
  "transport_profile": "SAE-AS5669A",
  "service_definition_language": "SAE-AS5684B"
 },
 "source": {
  "jaus_address": {"subsystem": 42, "node": 3, "component": 17},
  "a3o_node_id": "node:logistics-hub:amr-042",
  "trust_status": "VERIFIED"
 },
 "destination": {
  "jaus_address": {"subsystem": 1, "node": 1, "component": 10},
  "a3o_service_id": "service:mission-orchestrator"
 },
 "service": {
  "jsidl_reference": "registered-service-definition",
  "service_version": "declared-by-provider",
  "message_name": "JSD_DEFINED_MESSAGE",
  "interaction": "REPORT"
 },
 "context": {
  "ecosystem_id": "ecosystem:hub-bratislava-01",
  "mission_id": "mission:cargo-transfer-1187",
  "authority_lease_id": null,
  "policy_decision_id": "policy:decision:74921"
 },
 "time": {
  "source_timestamp": "2026-07-17T09:40:31.184Z",
  "received_timestamp": "2026-07-17T09:40:31.207Z",
  "trusted_time_status": "SYNCHRONIZED"
 },
 "payload": {
  "raw_message_retained": true,
  "decoded_fields": {},
  "canonical_state_delta": {}
 },
 "evidence": {
  "raw_hash": "sha256:...",
  "adapter_version": "a3o-jaus-gateway-1.0.0",
  "mapping_profile": "A3O-JAUS-MOBILITY-1.0"
 }
}
```


NON-NORMATIVE EXAMPLE

The JSON envelope is an internal A³O data contract. It is not the JAUS wire format and does not reproduce proprietary SAE message definitions.

4.3 Interaction mapping

JAUS interaction	A³O object	Operational rule
Command	GovernedActionRequest	Requires mission, policy, safety, human/delegated authority and JAUS Access Control validation.
Query	InformationRequest	Carries correlation, deadline, target service/version and expected response semantics.
Report	ObservationEvent / EntityStateDelta	Updates state only after schema, identity, freshness, frame and quality validation.
Event subscription	LiveStateSubscription	Maintains subscription lifecycle, rate, change conditions, loss detection and backpressure.
Discovery report	CapabilityRegistrationCandidate	Creates a candidate record; operational admission is a separate governance decision.
Management transition	LifecycleTransition	Evaluated against allowed source/target states, readiness, ownership and safety impact.
Access Control	AuthorityLease	Records controller, priority, acquisition, preemption, expiry, release and related mission.

JAUS interaction	A³O object	Operational rule
Liveness	HealthSignal	Contributes to health state but does not by itself prove safety or correctness.
Time	TrustedTimeContext	Records clock status and timestamp confidence.

4.4 Data retention and evidence

- Raw inbound and outbound control-relevant messages shall be retained or content-addressably archived according to the evidence policy.
- The service definition, generated codec, adapter version, mapping profile, policy decision and authority lease shall be referenced by immutable identifiers.
- A state update shall identify whether it resulted from a direct report, subscribed event, fused estimate, operator input, simulation or prediction.
- An outgoing command shall be correlated to the originating mission intent and to the resulting platform reports or timeout/failure state.
- Evidence storage may be partitioned for privacy or classification, but correlation identifiers and integrity proofs shall remain available to authorized assurance processes.

A3O-1400

5. A3O-1400 — Capability and Industry Profile Architecture

Capabilities are the stable contract between mission intent and implementation. A capability may be realized by a standard JAUS service, a combination of JAUS services, an A³O extension, a non-JAUS adapter, or a human procedure. The realization remains replaceable provided that the declared behavior, safety constraints, state semantics and conformance tests are satisfied.

Profile	Scope
A3O-JAUS-CORE	Transport, Events, Access Control, Management, Time, Liveness, Discovery and List Manager integration.
A3O-JAUS-MOBILITY	Pose, velocity, acceleration, drivers, waypoint/path capabilities and mobility constraints.
A3O-JAUS-SENSING	Range, visual, video, still image, audio, force/torque and resource-discovery capabilities as applicable.
A3O-JAUS-MANIPULATION	Manipulator sensing, control and motion capabilities for production and field robotics.
A3O-JAUS-MISSION	Mission Spooler integration beneath A³O ecosystem-level mission orchestration.
A3O-JAUS-AUTONOMY	Communications-loss, path reporting, cost-map and other autonomous capabilities.
A3O-JAUS-UGV	Ground-vehicle-specific capabilities augmenting platform-independent mobility.
A3O-JAUS-UMV	Maritime vehicle capabilities augmenting the common mobility model.
A3O-JAUS-INDUSTRIAL	Manipulator, AMR, production cell and industrial safety mappings.
A3O-JAUS-MEDICAL-ROBOTICS	Controlled mobility and payload workflows with separate medical safety/regulatory controls.
A3O-JAUS-SWARM	A³O extension profile for peer trust, collective state, distributed task allocation and partition handling.

5.1 Capability realization decision

13. Prefer an applicable standard service when the semantics and control model match the required capability.
14. Compose multiple services only when the resulting behavior and authority boundaries are explicit and testable.
15. Use an A³O extension when a cross-domain capability is required but no suitable JAUS service exists.
16. Use a non-JAUS adapter when the endpoint cannot expose JAUS; normalize it into the same A³O capability contract.
17. Document loss, approximation or constraints introduced by every mapping.

6. A3O-2000 — Reference Architecture and JAUS Interoperability Domain

The JAUS Interoperability Domain is a bounded architecture layer between external autonomous-system networks and the A³O canonical fabric. It is composed of independent services so that transport, schema, discovery, authority, lifecycle, events and semantic transformation can evolve and be tested separately.

Architecture layer	Primary responsibility
Experience and Integration Plane	Command UI, APIs, SDKs, digital twin, partner systems and operational exports.
Mission, Policy and Cognitive Plane	Mission orchestration, human authority, policy, safety, optimization and AI decision support.
State, Knowledge and Evidence Plane	Shared world state, provenance, replay, evidence graph and assurance packages.
Canonical Event and Data Fabric	Protocol-neutral envelopes, ontology, state deltas, command intents and event routing.
JAUS Interoperability Domain	Transport gateway, JSIDL Registry, Discovery Bridge, Access Control Broker, Management Bridge, Event Bridge and adapters.
Autonomous Systems and Other Endpoints	JAUS Subsystems/Nodes/Components plus DDS, ROS, OPC UA, MQTT, REST and vendor-specific systems.

6.1 Trust boundaries

Boundary	Rule
External network → Transport Gateway	Untrusted until transport, source, rate and policy checks complete.
Transport Gateway → JSIDL Registry	Only a validated service definition and compatible version may decode the payload.
Decoded message → Canonical Fabric	Identity, freshness, frame, unit, quality and semantic mapping must be established.
Canonical state → Policy / Mission	State may inform planning; it does not itself grant control authority.
Policy / Mission → Command Encoder	No direct UI or AI bypass; all required safety and authority evidence must exist.
Evidence Recorder → Evidence Store	Append-only or equivalent integrity protection with controlled retention and access.

6.2 Deployment patterns

Pattern	Intent
Embedded	Gateway and selected runtime services execute on the platform or its edge computer.
Site edge	A site server integrates multiple local robots and continues operation during cloud disconnection.
Federated edge	Multiple sites exchange approved state, mission and evidence without sharing all raw data.
Cloud-assisted	Central services provide fleet analytics, registry replication and governance while control remains bounded at the edge.
Partition-tolerant	Time-bounded delegated authority and local safety permit defined operation during communication loss.
High-assurance enclave	Control and evidence services execute in a restricted security domain with mediated external integration.

A3O-2100

7. A3O-2100 — Runtime and Edge Architecture

The runtime architecture is event-driven, distributed and partition-aware. It allows a local ecosystem to continue safe operation when cloud or peer connectivity is degraded, but it prevents a communication failure from silently expanding authority.

7.1 Core runtime services

Runtime service	Responsibility
Transport Gateway	Receives/transmits JAUS/SDP traffic, performs routing and retains raw transport evidence.
JSIDL Registry Runtime	Resolves service/version definitions and supplies generated decoders/encoders.
Discovery Bridge	Maintains JAUS hierarchy and candidate capability inventory.
Identity Binder	Maps JAUS addresses to A^{3}O identities and trust records.
Access Control Broker	Coordinates JAUS ownership with A^{3}O authority leases and policy.
Management Bridge	Maps component lifecycle to A^{3}O operational readiness.
Event Bridge	Creates and manages subscriptions, rate limits, loss detection and canonical events.
Telemetry Normalizer	Validates reports/events and produces state deltas.
Command Encoder	Encodes only authorized action intents into applicable service messages.
Evidence Correlator	Links raw messages, transformations, decisions, actions and outcomes.

7.2 Partition behavior

- Delegated authority shall have an explicit scope, duration, renewal condition and revocation path.
- Loss of the controller, policy service or trusted time shall transition the affected capability to a declared degraded mode; it shall not default to unrestricted autonomy.
- Local state changes and actions produced during partition shall be recorded and reconciled when connectivity returns.
- Conflicting state or mission updates shall be retained, compared and resolved through a deterministic reconciliation policy.
- The edge runtime shall expose health, queue, subscription, timing and evidence-backlog metrics.

7.3 Performance budgets

Each profile shall define latency, jitter, throughput, event-rate, command deadline, subscription capacity, queue depth, state freshness and recovery budgets. A transformation that exceeds its deadline shall not be treated as a valid control input merely because it eventually completes. Performance evidence is part of conformance, not a separate operational concern.

A3O-2200

8. A3O-2200 — Policy, Delegation and Human Authority

A^{3}O separates control ownership, authorization and execution. JAUS Access Control answers who currently owns preemptable control of a component. A^{3}O policy determines whether a proposed action is permitted in the mission, safety, organizational and legal context. Human or delegated authority determines who may approve or delegate that action.

8.1 Control precedence

18. Physical emergency protection and certified safety interlocks
19. Local platform safety kernel and hard operating limits
20. JAUS Access Control ownership and preemption rules
21. A^{3}O mission policy, security policy and safety envelope
22. Human operator or formally delegated authority
23. Mission orchestration and resource optimization
24. AI recommendations and optimization proposals

NO AUTHORITY BYPASS
A³O shall not bypass JAUS Access Control or local safety mechanisms. AI, UI and workflow components submit action intent; they do not directly transmit control messages.

8.2 Authority lease

An A³O AuthorityLease records subject, target capability, permitted actions, mission, policy basis, priority, start, expiry, renewal rule, geographic/operational scope, required approvals, revocation conditions and the related JAUS Access Control state. A lease may be narrower than JAUS control ownership and cannot be broader.

8.3 Human authorization levels

Level	Meaning
L0 Manual	Human directly commands each action; automation supplies state only.
L1 Assisted	Automation proposes or stabilizes actions; human remains continuously responsible.
L2 Supervised	Automation executes bounded tasks under active human supervision.
L3 Delegated	Human delegates a time- and scope-bounded mission segment.
L4 Coordinated Autonomous	Multiple platforms coordinate within an approved policy and safety envelope.
L5 Certified Autonomous Domain	Operation is permitted within a formally approved operational domain and assurance case.

A3O-2300

9. A3O-2300 — AI and Cognitive Services

AI services interpret information, estimate state, classify conditions, propose plans and optimize resources. They do not own transport identities, JAUS Access Control, safety interlocks or policy authority. The architecture treats an AI output as a proposal with provenance and confidence, not as an executable command.

9.1 Permitted cognitive outputs

- Observation interpretation and anomaly assessment
- Entity classification and state estimation
- Route, task, schedule and resource-allocation proposal
- Risk estimate and policy-relevant explanation
- Recommended event subscriptions and data-quality actions
- Predicted outcome and confidence interval

9.2 Mandatory barriers

Boundary	Rule
AI → JAUS Transport	Prohibited direct path.
AI → Policy	Proposal with model identity, version, input provenance, confidence and explanation.
Policy → Command	Requires authority, safety, lifecycle and Access Control checks.
Model update → Authority	Model update shall not expand permitted actions or autonomy level.
Training data → Live state	Training, simulation and replay data shall not be accepted as live observations.

9.3 Governed learning

JAUS reports and events may contribute to learning datasets only under an approved data-governance policy. The raw protocol source, mapping version, data quality, privacy class and mission context shall be retained. A learned model shall be validated against the applicable capability profile and shall not alter JSD-defined service contracts.

A3O-2400

10. A3O-2400 — Swarm and Distributed Coordination

JAUS provides standardized interaction with components and platforms. A³O extends this foundation for collective autonomy: peer trust, capability advertisement, shared state, distributed task allocation, topology management, partition behavior and evidence merging. Swarm membership does not imply unrestricted peer control.

Component	Function
Peer Identity Manager	Authenticates peers and binds local JAUS identities to swarm identities.
Capability Advertisement Service	Publishes bounded capabilities, constraints and current availability.
Mesh State Exchange	Exchanges signed state deltas with freshness and conflict metadata.
Distributed Task Allocator	Allocates tasks according to capability, policy, energy, risk and connectivity.
Local Safety Kernel	Rejects unsafe tasks and retains platform-local safety precedence.
Partition Manager	Applies delegated authority, degraded mission rules and reconciliation.
Evidence Merger	Combines per-node evidence without hiding conflicts or missing segments.

10.1 Swarm invariants

- Every participating node has a verifiable identity and declared trust status.
- Every peer message identifies mission, policy, schema and time context.
- Loss of a leader or peer does not expand authority.
- Local safety overrides mission optimization.
- Task reassignment preserves intent, ownership and evidence lineage.
- Partitioned operation uses time-bounded delegated authority.
- Conflicts are retained and reconciled; they are not silently overwritten.
- Collective AI outputs remain traceable to contributing nodes and evidence.
- A compromised node can be isolated without invalidating the identity of the remaining swarm.
- Swarm reconfiguration is auditable and testable.

A3O-2500

11. A3O-2500 — Safety, Resilience and Assurance

Interoperability is not equivalent to safety. A correctly decoded command can still be unsafe, unauthorized, late, inconsistent with local state or incompatible with the operational design domain. A3O-2500 therefore applies safety and assurance controls around the JAUS interaction path.

11.1 Safety envelope

- Declared operational domain and environmental limits
- Platform capability, configuration and health constraints
- Geographic, temporal, energy and payload constraints
- Permitted action classes and forbidden transitions
- Minimum state quality, freshness and trusted-time conditions
- Required human approval, redundancy or confirmation
- Fallback, abort, safe-stop and communications-loss behavior

11.2 Outcome verification

Command acceptance is not treated as successful completion. The runtime correlates the command with status reports, resulting state, sensor evidence, timeout behavior and the mission acceptance criterion. The result is an OutcomeAssessment with status, confidence, deviations, unresolved risks and evidence references.

11.3 Assurance case

Each deployment profile shall maintain an assurance case linking hazards, mitigations, architecture requirements, implementation controls, tests, operational procedures and evidence. JAUS compatibility is one evidence category within the assurance case; it does not replace industry safety certification or authorization.

12. A3O-3000 — System and Component Architecture

A software module becomes a JAUS-addressable component when it provides an independently discoverable capability, has a meaningful lifecycle, receives queries or commands, publishes reports or events, requires distinct control ownership, or can be replaced by another implementation. Internal microservices need not be exposed as JAUS components.

Component	Domain	Responsibility	Hard boundary
A3O.JAUS.TransportGateway	Transport	AS5669A transport handling, routing, connection state, rate controls and raw packet retention.	No semantic transformation.
A3O.JAUS.JSIDLRegistry	Schema	Licensed JSD import, dependency/version validation, codec generation and compatibility analysis.	No operational authority.
A3O.JAUS.DiscoveryBridge	Discovery	Hierarchy discovery, service inventory and candidate capability registration.	Discovery does not grant trust.
A3O.JAUS.IdentityBinder	Trust	Binds protocol addresses to persistent A³O identities, owners and attestation.	Cannot accept unknown ownership silently.
A3O.JAUS.AccessControlBroker	Authority	Coordinates JAUS control acquisition/release/preemption with A³O authority leases.	Cannot override local safety.
A3O.JAUS.ManagementBridge	Lifecycle	Maps component lifecycle, readiness, standby, shutdown and faults.	Cannot force invalid transitions.
A3O.JAUS.EventBridge	Events	Creates subscriptions, applies rates and conditions, detects loss and maps canonical events.	Cannot create unlimited subscriptions.
A3O.TelemetryNormalizationComponent	Data	Decodes Reports/Events, normalizes units/frames and updates state with provenance.	Does not issue commands.
A3O.RadarTrackFusionComponent	Sensing	Fuses radar, LiDAR, RF, optical and other observations into operational entities.	Uses a distinct A³O extension where no standard service applies.
A3O.MissionOrchestratorBridge	Mission	Maps ecosystem mission plans to platform-local task lists and execution state.	Does not bypass task or control ownership.
A3O.CommandEncoder	Execution	Encodes authorized action intents using the resolved service and version.	Rejects ambiguity and missing authority.
A3O.EvidenceRecorder	Assurance	Correlates raw messages, transformations, decisions, commands and outcomes.	Evidence cannot be post-hoc reconstructed as equivalent to runtime capture.

12.1 Radar and track fusion service boundary

The RadarTrackFusionComponent consumes standard sensing services where their semantics apply and also consumes non-JAUS radar, RF, optical, acoustic and other adapters. A fused track is a derived operational entity and shall not be represented as a standard SAE message unless an applicable standard service explicitly defines that semantic object.

```
ILLUSTRATIVE A³O EXTENSION NAMESPACE
urn:a3o:jaus:service:track-fusion:1.0
  QueryTrackList
  ReportTrackList
  QueryTrackDetail
  ReportTrackDetail
  CreateTrackEvent
  CancelTrackEvent
  ReportTrackLifecycle
```

12.2 Mission orchestration boundary

```
MISSION LAYERING
A³O Strategic Mission
  ├─ objectives and policy
  ├─ multi-platform coordination
  ├─ resource and risk optimization
  └─ JAUS Mission Spool
     ├─ Task 1
     ├─ Task 2
     └─ Task 3
```

A³O owns ecosystem objectives, dependencies, multi-platform allocation, policy, human authorization, replanning and evidence. The JAUS Mission Spooler is used as a platform-local mechanism for storing, managing and executing task lists and reporting execution state.

A3O-4000

13. A3O-4000 — Cross-Industry Solution Blueprints

Industry blueprints apply the same universal trust, state, authority and evidence architecture to different domains. The JAUS layer is used where suitable; proprietary industrial, medical or transport protocols remain supported through governed adapters. Each blueprint adds domain hazards, workflows, privacy and compliance requirements.

Profile	Systems	A³O focus
Logistics and transport	AMRs, autonomous trucks, loading robots, warehouse systems, ports and delivery vehicles.	Handoff, route, energy, geofencing, cargo identity, chain of custody and fleet deadlock.
Manufacturing	Manipulators, cobots, AGV/AMR, vision, conveyors, production cells and process systems.	Safe coordination, recipe/version integrity, tool state, interlocks, production provenance and changeover.
Inspection and information collection	UAS, UGV, USV, UUV, fixed sensors and mapping systems.	Coverage, provenance, coordinate integrity, sample identity, data quality and communication loss.
Medical and care robotics	Delivery, telepresence, assistive, evacuation and response robots.	Identity, privacy, payload custody, prioritization, human escalation and separate medical authorization.
Security and defence	Sensors, effectors, UxV, launchers, C2 systems and contested-edge nodes.	Mission identity, positive control, policy, spoofing resistance, partition behavior and immutable evidence.

13.1 DroneDefender relationship

DroneDefender is retained as the first Security and Defence mission profile and reference implementation. It demonstrates the governed loop for sensing, fusion, authorization, action and evidence, but it no longer defines the A³O platform category. Universal A³O components and JAUS profiles shall remain reusable outside the security domain.

13.2 Medical and regulated-domain disclaimer

JAUS compatibility provides interoperability. It does not establish medical-device compliance, functional safety, machinery conformity, aviation approval, maritime classification or defence authorization. Each deployment shall apply the appropriate domain assurance and legal framework independently.

A3O-5000

14. A3O-5000 — Conformance, Certification Readiness and Metrics

	Name	Exit criterion
	JAUS-Aware	Recognizes entities, addresses, services and messages; no operational control claim
	Core Compatible	Passes the defined A³O integration suite for applicable AS5710A core services and transport.
	Service-Set Compatible	Passes selected application service-set profile tests.
	Governed A³O Integration	Identity, policy, safety, authority, state, evidence and degraded-mode controls pass.
	A³O Certified Profile	An A³O partner profile passes the controlled profile suite; external certification is st separately.

14.1 Test families

	Test family	Coverage
	Discovery and hierarchy	Entity discovery, service inventory, disappearance, reappearance and address collision.

	Test family	Coverage
	Schema and version	JSD import, dependency resolution, codec round-trip, unknown and incompatible versi
	Query / Report	Correlation, timeout, stale state, invalid payload and quality handling.
	Events	Create, confirm, update, cancel, rate, change conditions, loss and exhaustion.
	Access Control	Acquire, release, contention, preemption, expiry, stale ownership and policy conflict.
	Management	Lifecycle transitions, invalid transitions, readiness, fault and recovery.
	Transport resilience	Loss, delay, duplication, reordering, fragmentation and reconnection.
	Security	Spoofing, replay, downgrade, flooding, malicious discovery and quarantine.
	Evidence	Raw-to-outcome completeness, integrity, timing and traceability.
	Industry scenario	Mission execution in the approved operational profile and safety envelope.

14.2 Required metrics

- Discovery completion and convergence time
- Decode/encode latency by service and message class
- Transformation latency and failure rate
- State freshness and uncertainty distribution
- Event subscription success, loss, rate and backpressure
- Access Control acquisition, contention, preemption and expiry events
- Command authorization and rejection reasons
- Outcome verification completion and unresolved outcomes
- Evidence completeness and storage backlog
- Unknown service, version, mapping and identity incidents

A3O-6000

15. A3O-6000 — Governed Learning and Adaptation

Learning and adaptation are governed architecture changes. A model or rule may improve classification, planning or optimization, but it cannot silently change a service contract, semantic mapping, authority level, safety envelope or conformance profile.

- Training datasets retain source protocol, service/version, mapping, mission, quality and privacy metadata.
- A proposed model is evaluated against approved scenarios, edge cases and safety constraints before deployment.
- Runtime monitoring detects data drift, concept drift, performance regression and policy-relevant anomalies.
- Rollback is available and evidence identifies the model version used for each recommendation or decision support output.
- Federated or distributed learning does not bypass data-governance, trust or export restrictions.

A3O-7000

16. A3O-7000 — Federated Autonomous Ecosystems

JAUS addresses are local protocol identities and may collide across organizations or ecosystems. Federation scopes every address under a persistent A^{3}O ecosystem and organization identity, allowing multiple independent JAUS domains to exchange approved capabilities and state without requiring a single global address space.

16.1 Federation contract

- Federated participants exchange signed capability, trust, policy and schema metadata before operational data.
- Raw data sharing is optional and governed separately from state or evidence summaries.
- Authority remains explicit and is not inherited from a partner network connection.
- Schema and mapping versions are negotiated and recorded.
- Conflicts, partial evidence and revoked identities remain visible to authorized assurance processes.
- Federated missions define ownership, escalation, liability-relevant records and termination behavior.

A3O-8000

17. A3O-8000 — Extreme, Contested and Strategic Operations

Contested and degraded environments require the same architecture principles under reduced trust, intermittent communications, manipulated time and hostile inputs. The goal is not uninterrupted maximum autonomy; it is controlled degradation without hidden authority expansion.

Threat	Scenario	Primary controls
Spoofed JAUS component	A hostile entity claims an expected address or service identity.	Identity binding, allowlists, attestation and quarantine.
Malicious discovery	Flooded or deceptive capability advertisements alter the inventory.	Rate limits, hierarchy validation and trust gating.
False capability advertisement	A node overstates services, limits or readiness.	Profile tests, runtime verification and bounded admission.
Version downgrade	An older or weaker service/mapping is selected.	Pinned compatibility ranges and downgrade policy.
Access Control abuse	Illicit preemption or stale ownership enables control.	Priority policy, expiry, alerts and evidence.
Replay / duplicate	Old command or report is accepted as current.	Trusted time, sequence/correlation checks and deduplication.
Event exhaustion	Subscriptions consume component or network capacity.	Quotas, rate control and circuit breakers.
Mapping poisoning	A valid message is transformed into incorrect operational meaning.	Signed mappings, review, regression and separation of duties.
Evidence withholding	A node omits or alters records after an action.	Hashing, append-only storage, replication and gap detection.
Topology manipulation	Peer links or swarm leadership are falsified.	Authenticated membership and audited reconfiguration.

17.1 Degraded-mode rule

Every profile shall define the behavior for loss of communications, loss of trusted time, loss of identity validation, stale state, incomplete evidence, conflicting commands and partial subsystem failure. A degraded mode shall be bounded, observable, reversible and testable.

A3O-9000

18. A3O-9000 — Schemas, SDKs, Annexes and Test Assets

Repository asset	Purpose
/a3o-jaus-sdk	Client and component integration libraries with policy-aware APIs.
/jsidl-importer	Controlled import, validation and dependency analysis.
/service-registry	Versioned service and compatibility records.
/generated-codecs	Generated encoders/decoders linked to source artifacts and toolchain.
/transport-adapters	JAUS/SDP, DDS and other bounded transport integrations.
/discovery-simulator	Entity hierarchy, appearance/disappearance and fault scenarios.
/access-control-test-harness	Ownership, priority, preemption, expiry and conflict tests.
/reference-components	Known-good and negative-test components.
/industry-profiles	Logistics, manufacturing, inspection, medical and security profiles.
/conformance-tests	Automated profile suites and evidence outputs.

Repository asset	Purpose
/example-messages	Licensed or synthetic examples with explicit provenance and restrictions.
/mapping-registry	Versioned semantic, unit, frame and state mappings.

18.1 Release artifact requirements

- Machine-readable version and dependency manifest
- Software bill of materials and license inventory
- Service-definition provenance and permitted-use record
- Generated-code toolchain identity and reproducibility record
- Supported standards/profile/version matrix
- Threat model and known limitations
- Conformance results and evidence package
- Migration and rollback guidance

DELIVERY

19. Implementation Roadmap and Release Gates

Phase	Workstream	Indicative duration	Exit condition
Phase 0	Standards baseline	4–6 weeks	Acquire licensed documents/data, confirm applicability, define claims and conformance scope.
Phase 1	Core interoperability runtime	8–12 weeks	Transport, JSIDL Registry, Discovery, Events, Management, Time, Liveness and Access Control integration.
Phase 2	Canonical bridge and evidence	8–10 weeks	Identity binding, semantic mapping, state updates, UI projection, authority and evidence correlation.
Phase 3	Application service sets	12–16 weeks	Mobility, sensing, manipulation, mission and autonomous capabilities profiles.
Phase 4	Industry pilots	12–20 weeks	At least one non-security pilot plus the DroneDefender reference profile.
Phase 5	Conformance laboratory	Continuous	Simulator, reference components, negative tests, compatibility matrix and partner acceptance.

19.1 Release gates

Gate	Required evidence
G0 — Standards and licensing	Applicable standards and data products acquired; use rights and citations recorded.
G1 — Architecture	R1.2 requirements, components, trust boundaries and profiles approved.
G2 — Core runtime	J1 conformance target and negative tests pass.
G3 — Application profile	Selected J2 service-set profile passes.
G4 — Governance and assurance	J3 identity, authority, safety, evidence and degraded-mode tests pass.
G5 — Partner profile	J4 profile accepted and published with explicit claim scope.

CONTROLLED CHANGE

20. Change and Traceability Matrix

The matrix below identifies how the preserved R0.1 architecture series is extended by R1.2. It does not replace the detailed requirements and overlays embedded in Part II.

Source series	Preserved R0.1 intent	R1.2 JAUS integration	Requirement range
A3O-1000	Foundation, vocabulary, lifecycle, traceability	JAUS standards governance, claim language,	JGP-001…008; JAU-1001…1015

Source series	Preserved R0.1 intent	R1.2 JAUS integration	Requirement range
		address/identity binding, JSIDL provenance	
A3O-1200	Canonical semantics and ontology	JAUS-to-A³O concept mapping; units, frames, time, uncertainty and extension policy	JAU-1201…1210
A3O-1300	Information architecture	Raw retention, canonical envelope, transformation and evidence correlation	JAU-1301…1314
A3O-1400	Capability architecture	Service realization decisions and compatibility profiles	JAU-1401…1410
A3O-2000	Reference architecture	Dedicated JAUS Interoperability Domain and trust boundaries	JAU-2001…2012
A3O-2100	Runtime architecture	Gateway, registry, discovery, authority, lifecycle, events and partition behavior	JAU-2101…2115
A3O-2300	AI architecture	AI advisory barrier; no direct command path or authority expansion	JAU-2301…2308
A3O-3000	System architecture	JAUS component criteria, component contracts and hard boundaries	JAU-3001…3020
A3O-4000	Solution architecture	Cross-industry profiles and DroneDefender as first reference profile	JAU-4001…4012
A3O-5000	Compliance framework	J0–J4 levels, test families, metrics and claim controls	JAU-5001…5015
A3O-6000	Autonomous governance	Governed learning and model-change controls	JAU-6001…6008
A3O-7000	Global ecosystem	Federated identity, address scoping and partner contracts	JAU-7001…7009
A3O-8000	Strategic/extreme systems	Contested JAUS threats and controlled degradation	JAU-8001…8012
A3O-9000	Annexes	SDK, schemas, registry, test assets and reproducible releases	JAU-9001…9010

SOURCE PRESERVATION

Part II contains the complete source baseline text and tables. R1.2 overlays are inserted after source artifact headings so reviewers can evaluate the new JAUS implications in context.

SOURCE BASELINE

Part II — Preserved R0.1 FULL MASTER Baseline with R1.2 JAUS Overlays

The following content preserves the source A3O Master Architecture Baseline R0.1 FULL MASTER STAGE 1. R1.2 overlay clauses are inserted immediately after source artifact headings. Source text and tables remain present for audit and comparison.

PRECEDENCE
Where an R1.2 overlay conflicts with preserved R0.1 language, the R1.2 overlay and Part I requirements govern. Otherwise the R0.1 clause remains applicable.

A3O Master Architecture Baseline R0.1 (Merged)

This document consolidates A3O-1000 to A3O-5000 architecture layers into a unified baseline.

A3O-1000_Foundation_Extension_PartA_R0.1.docx

FOUNDATION OVERLAY
This A3O-1000 Foundation Extension PartA R0.1 source artifact remains applicable. R1.2 adds the requirement that JAUS standards, service definitions, address bindings and compatibility claims are governed architecture artifacts with persistent identity, lifecycle, provenance and approval. Any use of a JAUS service shall trace to the applicable standard or explicitly named A^{3}O extension and to the release in which the mapping was verified.

A3O-1000 Foundation Extension
Part A — Architecture Meta Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Extends the A3O Meta Model with normative definitions governing architectural ownership, abstraction, dependency management and semantic consistency.

2. Canonical Metamodel Layers

3. Canonical Meta Rules

4. Architecture Ownership Matrix

Enterprise owns governance.
Mission owns operational intent.
Capability owns reusable abilities.
Runtime owns execution.
AI owns reasoning services.
Implementation owns realization but never architectural semantics.

5. Traceability Constraints

Every object SHALL trace to its governing domain.

Every implementation SHALL trace to a Capability.

Every Runtime Event SHALL trace to a Mission.

Every Decision SHALL reference supporting Evidence.

6. Conformance

A conforming A3O specification SHALL satisfy all Meta Model ownership, dependency, identity and traceability constraints defined in this extension.

A3O-1000_Foundation_Extension_PartB_R0.1.docx

FOUNDATION OVERLAY

This A3O-1000 Foundation Extension PartB R0.1 source artifact remains applicable. R1.2 adds the requirement that JAUS standards, service definitions, address bindings and compatibility claims are governed architecture artifacts with persistent identity, lifecycle, provenance and approval. Any use of a JAUS service shall trace to the applicable standard or explicitly named A^{3}O extension and to the release in which the mapping was verified.

A3O-1000 Foundation Extension
Part B — Canonical Vocabulary and Identity

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Extends the Foundation by defining canonical vocabulary governance, identity rules and naming conventions for all A3O architecture artifacts.

2. Vocabulary Governance

3. Identity Model

IDM-001 Every canonical object SHALL have a globally unique persistent identifier.

IDM-002 Identifiers SHALL remain stable throughout the object lifecycle.

IDM-003 Human-readable names MAY change without affecting identifiers.

IDM-004 Relationships SHALL reference identifiers rather than names.

IDM-005 Retired identifiers SHALL never be reused.

4. Naming Conventions

Prefix conventions:
A3O-xxxx – Specifications
MMR – Meta Model Rules
VOC – Vocabulary
ADR – Architecture Decision Record
REG – Registry
MET – Metric
ANX – Annex

5. Traceability

Vocabulary entries SHALL trace to domain owners, change history, governing ADRs and baseline releases.

6. Conformance

Conforming specifications SHALL exclusively use canonical vocabulary and identity rules defined by the Foundation.

A3O-1000_Foundation_Extension_PartC_R0.1.docx

FOUNDATION OVERLAY

This A3O-1000 Foundation Extension PartC R0.1 source artifact remains applicable. R1.2 adds the requirement that JAUS standards, service definitions, address bindings and compatibility claims are governed architecture artifacts with persistent identity, lifecycle, provenance and approval. Any use of a JAUS service shall trace to the applicable standard or explicitly named A^{3}O extension and to the release in which the mapping was verified.

A3O-1000 Foundation Extension
Part C — Canonical Lifecycle and Dependency Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical lifecycle, dependency constraints and evolution rules governing all A3O architectural artifacts.

2. Canonical Lifecycle

3. Lifecycle Rules

LCR-001 Every canonical object SHALL be in exactly one lifecycle state.

LCR-002 State transitions SHALL be authorized by governance.

LCR-003 Operational objects SHALL continuously produce evidence.

LCR-004 Retired artifacts SHALL remain reproducible.

LCR-005 Lifecycle history SHALL be immutable.

4. Dependency Model

5. Architecture Evolution

Architecture evolves through Proposal → ADR → Review → Approval → Baseline Publication → Adoption → Continuous Assessment.

6. Conformance

Conforming A3O artifacts SHALL implement the canonical lifecycle and dependency model without introducing unmanaged states or dependencies.

A3O-1000_Foundation_Extension_PartD_R0.1.docx

FOUNDATION OVERLAY

This A3O-1000 Foundation Extension PartD R0.1 source artifact remains applicable. R1.2 adds the requirement that JAUS standards, service definitions, address bindings and compatibility claims are governed architecture artifacts with persistent identity, lifecycle, provenance and approval. Any use of a JAUS service shall trace to the applicable standard or explicitly named A^{3}O extension and to the release in which the mapping was verified.

A3O-1000 Foundation Extension
Part D — Canonical Traceability Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical end-to-end traceability model ensuring every architectural artifact can be related to its governing concepts, decisions, evidence and implementations.

2. Traceability Chain

3. Traceability Constraints

TCR-001 Every normative requirement SHALL participate in at least one traceability chain.

TCR-002 Every implementation SHALL reference its governing Capability.

TCR-003 Every Runtime Event SHALL reference Mission, Capability and Runtime identifiers.

TCR-004 Evidence SHALL reference originating Runtime Events.

TCR-005 Decisions SHALL reference supporting Evidence and applicable ADRs.

TCR-006 Traceability records SHALL be immutable.

TCR-007 Missing traceability SHALL constitute architecture non-conformance.

TCR-008 Traceability SHALL remain technology independent.

4. Traceability Matrix

Mandatory matrix dimensions:
Requirement → Capability
Capability → Service
Service → Runtime
Runtime → Evidence
Evidence → Decision
Decision → Baseline

5. Conformance

A conforming A3O implementation SHALL maintain complete, auditable and end-to-end traceability across the entire architectural lifecycle.

A3O-1200_Semantic_Architecture_PartA_R0.1.docx

SEMANTIC OVERLAY

This A3O-1200 Semantic Architecture PartA R0.1 source artifact is extended by the JAUS-to-A^{3}O semantic mapping model. Protocol terms, units, coordinate frames, timestamps, validity and uncertainty shall be transformed through versioned mappings. Standard JAUS semantics are preserved; A^{3}O extensions are separately namespaced and never represented as SAE-defined services.

A3O-1200 Semantic Architecture
Part A — Canonical Semantic Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical semantic model that provides a shared meaning for all architectural objects, information structures and runtime interactions.

2. Semantic Principles

3. Canonical Semantic Objects

4. Semantic Constraints

SMC-001 Every Information Object SHALL reference canonical semantic objects.

SMC-002 Semantic relationships SHALL be explicitly defined.

SMC-003 Ambiguous terminology SHALL NOT appear in normative specifications.

SMC-004 Semantic ownership SHALL be unique.

SMC-005 Semantic changes SHALL be governed through ADRs.

5. Conformance

A conforming A3O specification SHALL exclusively use canonical semantic definitions and preserve semantic consistency across all architecture domains.

A3O-1200_Semantic_Architecture_PartB_R0.1.docx

SEMANTIC OVERLAY

This A3O-1200 Semantic Architecture PartB R0.1 source artifact is extended by the JAUS-to-A^{3}O semantic mapping model. Protocol terms, units, coordinate frames, timestamps, validity and uncertainty shall be transformed through versioned mappings. Standard JAUS semantics are preserved; A^{3}O extensions are separately namespaced and never represented as SAE-defined services.

A3O-1200 Semantic Architecture
Part B — Canonical Ontology and Semantic Relationships

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical ontology and semantic relationship model that governs how architectural concepts are related throughout the A3O framework.

2. Ontology Principles

3. Canonical Semantic Relationships

4. Semantic Constraints

SRC-001 Every semantic relationship SHALL have one authoritative definition.

SRC-002 Circular semantic ownership SHALL NOT exist.

SRC-003 Relationship semantics SHALL remain technology independent.

SRC-004 Every relationship SHALL be traceable.

SRC-005 Semantic extensions SHALL preserve canonical meanings.

5. Conformance

Conforming A3O specifications SHALL use only canonical semantic relationships or approved governed extensions.

A3O-1200_Semantic_Architecture_PartC_R0.1.docx

SEMANTIC OVERLAY

This A3O-1200 Semantic Architecture PartC R0.1 source artifact is extended by the JAUS-to-A^{3}O semantic mapping model. Protocol terms, units, coordinate frames, timestamps, validity and uncertainty shall be transformed through versioned mappings. Standard JAUS semantics are preserved; A^{3}O extensions are separately namespaced and never represented as SAE-defined services.

A3O-1200 Semantic Architecture
Part C — Canonical Type System

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical semantic type system used to classify all A3O architectural objects, assertions, information structures and runtime entities.

2. Type System Principles

3. Canonical Type Catalog

4. Type Constraints

TYC-001 Every Information Object SHALL reference canonical semantic types.

TYC-002 Type ambiguity SHALL NOT exist.

TYC-003 Objects MAY implement multiple interfaces but SHALL have one primary semantic type.

TYC-004 Type evolution SHALL preserve compatibility.

TYC-005 Type mappings SHALL remain traceable.

5. Conformance

Conforming A3O specifications SHALL classify all canonical objects using the canonical type system.

A3O-1200_Semantic_Architecture_PartD_R0.1.docx

SEMANTIC OVERLAY

This A3O-1200 Semantic Architecture PartD R0.1 source artifact is extended by the JAUS-to-A^{3}O semantic mapping model. Protocol terms, units, coordinate frames, timestamps, validity and uncertainty shall be transformed through versioned mappings. Standard JAUS semantics are preserved; A^{3}O extensions are separately namespaced and never represented as SAE-defined services.

A3O-1200 Semantic Architecture
Part D — Context, Assertions and Evidence Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical semantic model for Context, Assertions and Evidence, enabling consistent interpretation, validation and traceability of architectural knowledge.

2. Context Model

3. Assertion Model

AST-001 Every Assertion SHALL have a unique identifier.

AST-002 Assertions SHALL declare applicable Context.

AST-003 Assertions SHALL be supported or refuted by Evidence.

AST-004 Assertions SHALL preserve semantic version history.

AST-005 Assertion ownership SHALL be explicit.

4. Evidence Model

5. Semantic Constraints

SEC-001 Every Assertion SHALL reference at least one Evidence object.

SEC-002 Evidence SHALL retain provenance.

SEC-003 Context SHALL determine assertion validity.

SEC-004 Evidence SHALL remain immutable.

SEC-005 Semantic validation SHALL be reproducible.

6. Conformance

Conforming A3O implementations SHALL manage Context, Assertions and Evidence according to this canonical semantic model.

A3O-1200_Semantic_Architecture_PartE_R0.1.docx

SEMANTIC OVERLAY

This A3O-1200 Semantic Architecture PartE R0.1 source artifact is extended by the JAUS-to-A^{3}O semantic mapping model. Protocol terms, units, coordinate frames, timestamps, validity and uncertainty shall be transformed through versioned mappings. Standard JAUS semantics are preserved; A^{3}O extensions are separately namespaced and never represented as SAE-defined services.

A3O-1200 Semantic Architecture
Part E — Semantic Versioning and Evolution

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical model for semantic versioning, compatibility management and controlled evolution of semantic assets within the A3O framework.

2. Semantic Versioning Model

3. Evolution Rules

SER-001 Canonical meanings SHALL NOT change without governance approval.
SER-002 Every semantic change SHALL reference one or more ADRs.
SER-003 Semantic evolution SHALL preserve identifier stability.
SER-004 Superseded concepts SHALL remain available for audit.
SER-005 Compatibility analysis SHALL accompany every major semantic revision.
SER-006 Semantic migrations SHALL be documented.
SER-007 Version history SHALL be immutable.
SER-008 Semantic releases SHALL be reproducible.

4. Compatibility Matrix

Major → compatibility review required
Minor → backward compatible
Revision → no semantic impact
Deprecated → supported until governed retirement

5. Conformance

Conforming A3O semantic specifications SHALL implement canonical semantic versioning, preserve backward traceability and manage evolution through governed changes.

A3O-1300_Information_Architecture_PartA_R0.1.docx

INFORMATION OVERLAY
This A3O-1300 Information Architecture PartA R0.1 source artifact is extended by immutable raw-message retention, exact JSD/version references, canonical envelopes, state-delta provenance and evidence correlation. A decoded payload alone is insufficient: the architecture retains how, when and under which mapping and trust context the information became operational state.

A3O-1300 Information Architecture
Part A — Canonical Information Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical information model governing information objects, metadata, ownership and lifecycle across the A3O architecture.

2. Information Principles

3. Canonical Information Objects

4. Information Constraints

INC-001 Every Information Object SHALL reference canonical semantic definitions.
INC-002 Metadata SHALL accompany every managed information object.
INC-003 Information ownership SHALL be explicit.
INC-004 Information integrity SHALL be verifiable.
INC-005 Information lineage SHALL be preserved.

5. Conformance

Conforming A3O implementations SHALL manage information according to the canonical information model, ownership and lifecycle rules.

A3O-1300_Information_Architecture_PartB_R0.1.docx

INFORMATION OVERLAY
This A3O-1300 Information Architecture PartB R0.1 source artifact is extended by immutable raw-message retention, exact JSD/version references, canonical envelopes, state-delta provenance and evidence correlation. A decoded payload alone is insufficient: the architecture retains how, when and under which mapping and trust context the information became operational state.

A3O-1300 Information Architecture
Part B — Metadata, Information Contracts and Lineage

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical metadata model, information contracts and lineage mechanisms required for governed information exchange throughout the A3O architecture.

2. Metadata Model

3. Information Contracts

ICR-001 Every information exchange SHALL be governed by a canonical Information Contract.

ICR-002 Contracts SHALL define producer, consumer and semantic scope.

ICR-003 Contracts SHALL specify mandatory metadata.

ICR-004 Contract versions SHALL be traceable.

ICR-005 Contract changes SHALL be governed through ADRs.

4. Information Lineage

Mandatory lineage chain:
Source → Acquisition → Transformation → Validation → Distribution → Consumption → Archive

5. Lineage Constraints

LNG-001 Every transformation SHALL preserve provenance.

LNG-002 Lineage SHALL remain complete and immutable.

LNG-003 Consumers SHALL be able to reconstruct information origin.

LNG-004 Missing lineage SHALL constitute non-conformance.

LNG-005 Lineage SHALL support audit and certification.

6. Conformance

Conforming A3O implementations SHALL maintain canonical metadata, governed information contracts and complete lineage for all managed information assets.

A3O-1300_Information_Architecture_PartC_R0.1.docx

INFORMATION OVERLAY

This A3O-1300 Information Architecture PartC R0.1 source artifact is extended by immutable raw-message retention, exact JSD/version references, canonical envelopes, state-delta provenance and evidence correlation. A decoded payload alone is insufficient: the architecture retains how, when and under which mapping and trust context the information became operational state.

A3O-1300 Information Architecture
Part C — Information Flows and Exchange Patterns

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines canonical information flow models and exchange patterns ensuring reliable, traceable and semantically consistent movement of information across A3O domains.

2. Information Flow Principles

3. Canonical Exchange Patterns

4. Information Flow Constraints

IFC-001 Every exchange SHALL identify producer and consumer.

IFC-002 Information SHALL retain provenance throughout the flow.

IFC-003 Transformations SHALL be explicitly documented.

IFC-004 Exchange failures SHALL be auditable.

IFC-005 Cross-domain exchanges SHALL enforce governing policies.

5. Conformance

Conforming A3O implementations SHALL implement canonical exchange patterns and maintain complete traceability for all governed information flows.

A3O-1300_Information_Architecture_PartD_R0.1.docx

INFORMATION OVERLAY

This A3O-1300 Information Architecture PartD R0.1 source artifact is extended by immutable raw-message retention, exact JSD/version references, canonical envelopes, state-delta provenance and evidence correlation. A decoded payload alone is insufficient: the architecture retains how, when and under which mapping and trust context the information became operational state.

A3O-1300 Information Architecture
Part D — Information Quality, Integrity and Validation

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical quality, integrity and validation model for information assets managed within the A3O Architecture.

2. Information Quality Dimensions

3. Integrity Model

IIN-001 Every managed information object SHALL support integrity verification.

IIN-002 Integrity mechanisms SHALL detect unauthorized modification.

IIN-003 Information packages SHALL preserve internal consistency.

IIN-004 Integrity evidence SHALL be retained for audit.

IIN-005 Integrity validation SHALL be repeatable.

4. Validation Model

5. Normative Constraints

IVC-001 Validation SHALL precede publication of governed information.

IVC-002 Failed validation SHALL generate a governed finding.

IVC-003 Quality metrics SHALL be measurable and traceable.

IVC-004 Validation evidence SHALL reference canonical identifiers.

IVC-005 Information quality SHALL be continuously monitored.

6. Conformance

Conforming A3O implementations SHALL continuously assess information quality, preserve integrity and maintain objective validation evidence for governed information assets.

A3O-1300_Information_Architecture_PartE_R0.1.docx

INFORMATION OVERLAY

This A3O-1300 Information Architecture PartE R0.1 source artifact is extended by immutable raw-message retention, exact JSD/version references, canonical envelopes, state-delta provenance and evidence correlation. A decoded payload alone is insufficient: the architecture retains how, when and under which mapping and trust context the information became operational state.

A3O-1300 Information Architecture
Part E — Information Governance, Retention and Federation

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical governance, retention and federation model for information assets across enterprise, mission and federated A3O environments.

2. Information Governance Model

3. Retention Model

RET-001 Every managed information object SHALL declare a retention policy.

RET-002 Retention periods SHALL be governed.

RET-003 Archived information SHALL preserve provenance and integrity.

RET-004 Disposal SHALL require explicit authorization.

RET-005 Retention decisions SHALL remain auditable.

4. Federation Model

5. Normative Constraints

FGC-001 Federated exchanges SHALL preserve ownership boundaries.

FGC-002 Information governance SHALL remain policy driven.

FGC-003 Retention SHALL comply with governing regulations.

FGC-004 Federated information SHALL preserve semantic consistency.

FGC-005 Governance evidence SHALL be maintained for audit.

6. Conformance

Conforming A3O implementations SHALL implement canonical information governance, retention and federation models for all managed information assets.

A3O-1400_Capability_Architecture_PartA_R0.1.docx

CAPABILITY OVERLAY

This A3O-1400 Capability Architecture PartA R0.1 source artifact is extended by JAUS capability realization profiles. A capability may map to a standard JAUS service, a service composition, an A^{3}O extension or a non-JAUS adapter. The choice shall preserve behavior, authority, safety constraints, state semantics and conformance evidence.

A3O-1400 Capability Architecture
Part A — Canonical Capability Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical capability model used to identify, specify, govern and realize capabilities throughout the A3O architecture.

2. Capability Principles

3. Canonical Capability Elements

4. Capability Constraints

CPC-001 Every Capability SHALL trace to one or more Mission objectives.

CPC-002 Every Capability SHALL expose measurable outcomes.

CPC-003 Capability dependencies SHALL be explicitly declared.

CPC-004 Capability realization SHALL preserve semantic intent.

CPC-005 Capability changes SHALL be governed through ADRs.

5. Conformance

Conforming A3O implementations SHALL define, govern and realize capabilities using the canonical capability model.

A3O-1400_Capability_Architecture_PartB_R0.1.docx

CAPABILITY OVERLAY

This A3O-1400 Capability Architecture PartB R0.1 source artifact is extended by JAUS capability realization profiles. A capability may map to a standard JAUS service, a service composition, an A^{3}O extension or a non-JAUS adapter. The choice shall preserve behavior, authority, safety constraints, state semantics and conformance evidence.

A3O-1400 Capability Architecture
Part B — Capability Composition and Dependency Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical model for composing, decomposing and governing dependencies between capabilities within the A3O Architecture.

2. Composition Principles

3. Dependency Types

4. Composition Constraints

CCD-001 Circular capability dependencies SHALL NOT exist.

CCD-002 Composite capabilities SHALL expose measurable outcomes.

CCD-003 Dependency changes SHALL be governed through ADRs.

CCD-004 Every dependency SHALL be traceable.

CCD-005 Capability composition SHALL preserve compatibility.

5. Conformance

Conforming A3O implementations SHALL model capability composition and dependencies using the canonical capability relationship model.

A3O-1400_Capability_Architecture_PartC_R0.1.docx

CAPABILITY OVERLAY

This A3O-1400 Capability Architecture PartC R0.1 source artifact is extended by JAUS capability realization profiles. A capability may map to a standard JAUS service, a service composition, an A³O extension or a non-JAUS adapter. The choice shall preserve behavior, authority, safety constraints, state semantics and conformance evidence.

A3O-1400 Capability Architecture
Part C — Capability Lifecycle and Maturity Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical lifecycle and maturity model governing the evolution, assessment and operational readiness of A3O capabilities.

2. Capability Lifecycle

3. Capability Maturity Levels

4. Lifecycle Constraints

CLC-001 Every Capability SHALL be in exactly one lifecycle state.

CLC-002 Lifecycle transitions SHALL require governance approval where applicable.

CLC-003 Capability maturity SHALL be evidence-based.

CLC-004 Operational Capabilities SHALL publish measurable outcomes.

CLC-005 Capability retirement SHALL preserve traceability and historical evidence.

5. Conformance

Conforming A3O implementations SHALL manage capability lifecycle states, maturity assessments and evolution according to this specification.

A3O-1400_Capability_Architecture_PartD_R0.1.docx

CAPABILITY OVERLAY

This A3O-1400 Capability Architecture PartD R0.1 source artifact is extended by JAUS capability realization profiles. A capability may map to a standard JAUS service, a service composition, an A³O extension or a non-JAUS adapter. The choice shall preserve behavior, authority, safety constraints, state semantics and conformance evidence.

A3O-1400 Capability Architecture
Part D — Capability Federation and Governance

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical federation and governance model for capabilities operating across organizational, mission and runtime boundaries.

2. Federation Principles

3. Federation Roles

4. Governance Constraints

CFG-001 Federated capabilities SHALL be registered in the Canonical Registry.

CFG-002 Federation agreements SHALL reference canonical contracts.

CFG-003 Cross-domain execution SHALL generate traceable Runtime Evidence.

CFG-004 Governance decisions SHALL be documented by ADRs.

CFG-005 Federation policies SHALL be enforced consistently across participating domains.

5. Conformance

Conforming A3O implementations SHALL support governed capability federation, preserve ownership boundaries and maintain complete traceability.

A3O-1400_Capability_Architecture_PartE_R0.1.docx

CAPABILITY OVERLAY

This A3O-1400 Capability Architecture PartE R0.1 source artifact is extended by JAUS capability realization profiles. A capability may map to a standard JAUS service, a service composition, an A³O extension or a non-JAUS adapter. The choice shall preserve behavior, authority, safety constraints, state semantics and conformance evidence.

A3O-1400 Capability Architecture
Part E — Capability Evolution, Optimization and Continuous Improvement

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical model for capability evolution, optimization and continuous improvement while preserving architectural integrity and backward traceability.

2. Evolution Principles

3. Continuous Improvement Cycle

4. Evolution Constraints

CEC-001 Every capability change SHALL reference one or more ADRs.

CEC-002 Capability identifiers SHALL remain stable across compatible revisions.

CEC-003 Optimization SHALL be supported by measurable evidence.

CEC-004 Deprecated capabilities SHALL remain traceable until retirement.

CEC-005 Continuous improvement SHALL preserve interoperability.

5. Conformance

Conforming A3O implementations SHALL manage capability evolution through governed, evidence-based and traceable continuous improvement processes.

A3O-2000_Reference_Architecture_PartA_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartA R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part A — Canonical Reference Architecture Framework

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical framework for developing, governing and reusing Reference Architectures across all A3O domains.

2. Reference Architecture Principles

RAF-001 Reference Architectures SHALL be implementation independent.
RAF-002 Reference Architectures SHALL reuse canonical semantic, information and capability models.
RAF-003 Every Reference Architecture SHALL define mandatory and optional elements.
RAF-004 Every Reference Architecture SHALL declare conformance criteria.
RAF-005 Reference Architectures SHALL be versioned and governed.

3. Canonical Elements

- Scope
- Stakeholders
- Context
- Architecture Building Blocks
- Interfaces
- Contracts

- Policies
- Constraints
- Quality Attributes
- Conformance Rules

4. Layer Mapping

Foundation → Semantic → Information → Capability → Reference → Runtime → System → Deployment → Implementation

5. Governance Constraints

RFG-001 Every Reference Architecture SHALL reference an approved Baseline.
RFG-002 Changes SHALL be approved through ADRs.
RFG-003 Building Blocks SHALL have canonical identifiers.
RFG-004 Dependencies SHALL remain traceable.
RFG-005 Reference Architectures SHALL support federation.

6. Conformance

Conforming A3O implementations SHALL realize approved Reference Architectures without violating mandatory architectural constraints.

A3O-2000_Reference_Architecture_PartB_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartB R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part B — Canonical Architecture Building Blocks

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Architecture Building Blocks (ABBs) used to compose every A3O Reference Architecture in a consistent, reusable and governed manner.

2. Building Block Principles

ABB-001 Every Building Block SHALL have a globally unique identifier.
ABB-002 Building Blocks SHALL encapsulate a single architectural responsibility.
ABB-003 Building Blocks SHALL expose only governed interfaces.
ABB-004 Building Blocks SHALL be reusable across Reference Architectures.
ABB-005 Building Blocks SHALL remain implementation independent.

3. Canonical Building Block Catalog

4. Composition Constraints

ABC-001 Every Reference Architecture SHALL declare the Building Blocks it contains.
ABC-002 Building Block dependencies SHALL be acyclic.
ABC-003 Every interface SHALL reference a canonical contract.
ABC-004 Building Block composition SHALL preserve traceability.
ABC-005 Building Blocks SHALL support substitution only through governed compatibility.

5. Conformance

Conforming A3O Reference Architectures SHALL be composed exclusively from approved canonical Architecture Building Blocks or governed extensions.

A3O-2000_Reference_Architecture_PartC_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartC R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part C — Canonical Architecture Patterns

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical architecture patterns that may be reused to construct A3O Reference Architectures while preserving interoperability, governance and traceability.

2. Pattern Principles

PAT-001 Patterns SHALL be implementation independent.

PAT-002 Patterns SHALL be reusable across domains.

PAT-003 Patterns SHALL define mandatory and optional elements.

PAT-004 Patterns SHALL reference canonical Architecture Building Blocks.

PAT-005 Pattern evolution SHALL be governed through ADRs.

3. Canonical Pattern Catalog

4. Pattern Constraints

PTC-001 Every deployed pattern SHALL identify participating ABBs.

PTC-002 Patterns SHALL preserve semantic consistency.

PTC-003 Pattern composition SHALL remain traceable.

PTC-004 Pattern substitution SHALL require compatibility assessment.

PTC-005 Cross-pattern interactions SHALL use canonical contracts.

5. Conformance

Conforming A3O Reference Architectures SHALL employ approved canonical patterns or governed extensions compatible with the Architecture Baseline.

A3O-2000_Reference_Architecture_PartD_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartD R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part D — Enterprise Reference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Enterprise Reference Architecture governing enterprise strategy, governance, organizational capabilities and business services.

2. Enterprise Architecture Principles

ERP-001 Enterprise Architecture SHALL align strategy, governance and execution.

ERP-002 Enterprise services SHALL reuse canonical capabilities.

ERP-003 Enterprise decisions SHALL be evidence-based.

ERP-004 Enterprise architecture SHALL support federation.

ERP-005 Enterprise architecture SHALL remain technology independent.

3. Enterprise Architecture Domains

4. Governance Constraints

ERG-001 Enterprise domains SHALL reference canonical capabilities.

ERG-002 Enterprise services SHALL publish governed interfaces.

ERG-003 Cross-domain interactions SHALL use canonical contracts.

ERG-004 Enterprise architecture changes SHALL be approved through ADRs.

ERG-005 Enterprise architecture SHALL preserve end-to-end traceability.

5. Conformance

Conforming Enterprise Architectures SHALL implement the canonical enterprise model and satisfy all mandatory governance constraints.

A3O-2000_Reference_Architecture_PartE_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartE R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part E — Mission Reference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Mission Reference Architecture governing mission planning, execution, coordination and assessment across the A3O ecosystem.

2. Mission Principles

MRP-001 Missions SHALL be driven by explicit objectives.

MRP-002 Missions SHALL be realized through governed capabilities.

MRP-003 Mission execution SHALL be evidence-based.

MRP-004 Mission coordination SHALL preserve end-to-end traceability.

MRP-005 Mission Architecture SHALL remain implementation independent.

3. Mission Architecture Domains

4. Governance Constraints

MRG-001 Every Mission SHALL reference approved Capabilities.

MRG-002 Mission objectives SHALL be measurable.

MRG-003 Mission events SHALL generate Runtime Evidence.

MRG-004 Mission changes SHALL be governed through ADRs.

MRG-005 Mission Architecture SHALL support federation and interoperability.

5. Conformance

Conforming Mission Architectures SHALL implement the canonical mission model, maintain objective evidence and satisfy all mandatory governance constraints.

A3O-2000_Reference_Architecture_PartF_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartF R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part F — Knowledge Reference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Knowledge Reference Architecture governing knowledge acquisition, semantic integration, reasoning, evidence management and decision support across A3O.

2. Knowledge Principles

KRP-001 Knowledge SHALL be derived from governed information and evidence.

KRP-002 Knowledge SHALL use canonical semantic definitions and ontologies.

KRP-003 Knowledge assets SHALL be versioned and traceable.

KRP-004 Knowledge SHALL support human and AI reasoning.

KRP-005 Knowledge Architecture SHALL remain implementation independent.

3. Knowledge Domains

4. Governance Constraints

KRG-001 Every Knowledge Asset SHALL reference canonical semantic concepts.

KRG-002 Knowledge assertions SHALL be supported by Evidence.

KRG-003 Knowledge lineage SHALL remain traceable.

KRG-004 Knowledge changes SHALL be approved through ADRs where normative.

KRG-005 Knowledge Architecture SHALL support federation and interoperability.

5. Conformance

Conforming Knowledge Architectures SHALL preserve semantic consistency, evidence traceability and governed lifecycle management for all knowledge assets.

A3O-2000_Reference_Architecture_PartG_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartG R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part G — Runtime Reference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Runtime Reference Architecture governing execution environments, orchestration, runtime services, observability and operational resilience.

2. Runtime Principles

RRP-001 Runtime SHALL execute governed Capabilities.

RRP-002 Runtime SHALL preserve semantic consistency.

RRP-003 Runtime SHALL generate objective Runtime Evidence.

RRP-004 Runtime SHALL be observable, resilient and scalable.

RRP-005 Runtime SHALL remain implementation independent.

3. Runtime Domains

4. Governance Constraints

RRG-001 Every runtime service SHALL reference approved Capabilities.

RRG-002 Runtime interactions SHALL use canonical contracts.

RRG-003 Runtime events SHALL be immutable and traceable.

RRG-004 Runtime policy changes SHALL be governed through ADRs.

RRG-005 Runtime Architecture SHALL support federation and interoperability.

5. Conformance

Conforming Runtime Architectures SHALL implement governed execution, complete observability and end-to-end traceability for all runtime operations.

A3O-2000_Reference_Architecture_PartH_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartH R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part H — Security Reference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Security Reference Architecture governing trust, identity, protection, resilience, privacy and assurance across all A3O domains.

2. Security Principles

SRP-001 Security SHALL be integrated into every architecture layer by design.

SRP-002 Identity SHALL be the foundation of trust.

SRP-003 Every access decision SHALL be policy governed.

SRP-004 Security SHALL generate objective audit evidence.

SRP-005 Security Architecture SHALL remain technology independent.

3. Security Domains

4. Governance Constraints

SRG-001 Every protected asset SHALL have an assigned security classification.

SRG-002 Security policies SHALL reference canonical identities and contracts.

SRG-003 Security events SHALL produce immutable audit evidence.

SRG-004 Security architecture changes SHALL be approved through ADRs.

SRG-005 Security controls SHALL support federation and interoperability.

5. Conformance

Conforming Security Architectures SHALL implement canonical identity, policy, protection and audit mechanisms while maintaining end-to-end traceability.

A3O-2000_Reference_Architecture_PartI_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartI R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part I — Integration Reference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Integration Reference Architecture governing interoperability, service interaction, messaging, APIs, event exchange and federation across A3O.

2. Integration Principles

IRP-001 Integration SHALL use canonical contracts.

IRP-002 Interfaces SHALL be technology independent.

IRP-003 Interactions SHALL preserve semantic consistency.

IRP-004 Integration SHALL support synchronous and asynchronous communication.

IRP-005 Integration SHALL produce complete operational traceability.

3. Integration Domains

4. Governance Constraints

IRG-001 Every integration SHALL reference a canonical Information Contract.

IRG-002 Every interface SHALL have a stable canonical identifier.

IRG-003 Integration events SHALL generate Runtime Evidence.

IRG-004 Integration changes SHALL be governed through ADRs.

IRG-005 Federated integrations SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming Integration Architectures SHALL implement canonical contracts, governed interfaces, interoperable messaging and end-to-end traceability.

A3O-2000_Reference_Architecture_PartJ_R0.1.docx

REFERENCE ARCHITECTURE OVERLAY

This A3O-2000 Reference Architecture PartJ R0.1 source artifact now includes the bounded JAUS Interoperability Domain. Transport, JSIDL resolution, discovery, identity binding, Access Control, lifecycle, events, transformation and evidence are separate runtime responsibilities. Discovery and message decoding do not create trust or authority.

A3O-2000 Reference Architecture
Part J — Reference Architecture Evolution and Baselines

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical model for evolution, baseline management, compatibility and release governance of A3O Reference Architectures.

2. Evolution Principles

REV-001 Every Reference Architecture SHALL belong to an approved Baseline.
REV-002 Architectural evolution SHALL be governed through ADRs.
REV-003 Compatible evolution SHALL preserve canonical identifiers.
REV-004 Baseline releases SHALL be reproducible and auditable.
REV-005 Evolution SHALL preserve traceability across releases.

3. Baseline Model

4. Governance Constraints

RBG-001 Every Baseline SHALL be approved by the Architecture Governance Authority.
RBG-002 Baseline changes SHALL reference one or more ADRs.
RBG-003 Compatibility profiles SHALL be published with every release.
RBG-004 Deprecated elements SHALL remain traceable until retirement.
RBG-005 Every Baseline SHALL support objective conformance assessment.

5. Conformance

Conforming A3O implementations SHALL reference an approved Architecture Baseline, preserve compatibility where required and maintain complete architectural traceability across releases.

A3O-2100_Runtime_Architecture_PartA_R0.1.docx

RUNTIME OVERLAY

This A3O-2100 Runtime Architecture PartA R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part A — Runtime Execution Model

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Runtime Execution Model governing execution semantics, workload lifecycle, orchestration and runtime state management for the A3O platform.

2. Runtime Execution Principles

REM-001 Runtime execution SHALL realize approved Capabilities only.
REM-002 Execution SHALL preserve canonical semantic consistency.
REM-003 Runtime execution SHALL be deterministic where required by policy.
REM-004 Every execution SHALL generate objective Runtime Evidence.
REM-005 Runtime execution SHALL remain technology independent.

3. Runtime Execution Components

4. Governance Constraints

REG-001 Every runtime execution SHALL reference an approved Capability.
REG-002 Every execution instance SHALL have a globally unique identifier.
REG-003 Runtime state transitions SHALL be traceable.
REG-004 Runtime policy violations SHALL generate governed findings.
REG-005 Runtime execution SHALL support federation and interoperability.

5. Conformance

Conforming Runtime Architectures SHALL implement the canonical Runtime Execution Model, preserve execution traceability and maintain objective runtime evidence.

A3O-2100_Runtime_Architecture_PartB_R0.1.docx

RUNTIME OVERLAY

This A3O-2100 Runtime Architecture PartB R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part B — Runtime Services

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Runtime Services model governing reusable execution services supporting workloads, orchestration, security and operational management.

2. Runtime Service Principles

RSP-001 Runtime Services SHALL expose canonical service contracts.

RSP-002 Services SHALL be stateless unless governed state is required.

RSP-003 Services SHALL emit observable runtime events.

RSP-004 Services SHALL enforce security and policy controls.

RSP-005 Services SHALL remain implementation independent.

3. Canonical Runtime Services

4. Governance Constraints

RSG-001 Every Runtime Service SHALL have a canonical identifier.

RSG-002 Service interfaces SHALL use approved contracts.

RSG-003 Service failures SHALL generate Runtime Evidence.

RSG-004 Service changes SHALL be governed through ADRs.

RSG-005 Runtime Services SHALL support federation and interoperability.

5. Conformance

Conforming Runtime Architectures SHALL implement approved Runtime Services using canonical interfaces, policies and traceability mechanisms.

A3O-2100_Runtime_Architecture_PartC_R0.1.docx

RUNTIME OVERLAY

This A3O-2100 Runtime Architecture PartC R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part C — Workflow and Orchestration

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Workflow and Orchestration model governing execution sequencing, coordination, distributed processes and mission workflow management across the A3O Runtime.

2. Workflow Principles

RWF-001 Workflows SHALL orchestrate approved Capabilities only.

RWF-002 Workflow definitions SHALL be declarative and technology independent.

RWF-003 Orchestration SHALL preserve semantic consistency and traceability.

RWF-004 Long-running workflows SHALL support checkpointing and recovery.

RWF-005 Workflow execution SHALL generate objective Runtime Evidence.

3. Canonical Workflow Components

4. Governance Constraints

RWG-001 Every workflow SHALL have a canonical identifier.

RWG-002 Workflow versions SHALL be governed and traceable.

RWG-003 Orchestration decisions SHALL comply with runtime policies.

RWG-004 Workflow failures SHALL produce Runtime Evidence and Findings.

RWG-005 Federated workflows SHALL use canonical contracts and identities.

5. Conformance

Conforming Runtime Architectures SHALL implement governed workflow orchestration, preserve execution traceability and support interoperable distributed process execution.

A3O-2100_Runtime_Architecture_PartD_R0.1.docx

RUNTIME OVERLAY

This A3O-2100 Runtime Architecture PartD R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part D — Runtime State Management

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Runtime State Management model governing lifecycle state, consistency, persistence, recovery and synchronization of runtime execution across the A3O platform.

2. State Management Principles

RSM-001 Runtime state SHALL have a canonical lifecycle.

RSM-002 State transitions SHALL be deterministic where required by policy.

RSM-003 Runtime state SHALL remain traceable and auditable.

RSM-004 Persistent state SHALL preserve integrity and provenance.

RSM-005 State management SHALL be implementation independent.

3. Canonical Runtime States

4. Governance Constraints

RST-001 Every runtime instance SHALL have exactly one active lifecycle state.

RST-002 Every state transition SHALL generate Runtime Evidence.

RST-003 Illegal state transitions SHALL generate governed Findings.

RST-004 State recovery SHALL preserve execution consistency.

RST-005 Runtime state SHALL support federation and distributed synchronization.

5. Conformance

Conforming Runtime Architectures SHALL implement canonical runtime state management, preserve lifecycle integrity and maintain complete state transition traceability.

A3O-2100_Runtime_Architecture_PartE_R0.1.docx

RUNTIME OVERLAY

This A3O-2100 Runtime Architecture PartE R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part E — Event Processing and Event Management

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Event Processing model governing event generation, routing, correlation, persistence, stream processing and Runtime Evidence creation within the A3O platform.

2. Event Processing Principles

EVP-001 Every significant runtime occurrence SHALL generate a canonical Runtime Event.

EVP-002 Events SHALL be immutable after publication.
EVP-003 Event processing SHALL preserve ordering where required by policy.
EVP-004 Events SHALL support distributed and federated processing.
EVP-005 Event processing SHALL remain technology independent.

3. Canonical Event Components

4. Governance Constraints

EVG-001 Every Runtime Event SHALL have a globally unique identifier.
EVG-002 Event schemas SHALL reference canonical semantic definitions.
EVG-003 Event loss SHALL be detectable and auditable.
EVG-004 Event processing policy changes SHALL be governed through ADRs.
EVG-005 Federated event exchanges SHALL preserve identity, ordering and traceability.

5. Conformance

Conforming Runtime Architectures SHALL implement canonical event generation, processing, persistence and evidence creation while maintaining complete end-to-end traceability.

A3O-2100_Runtime_Architecture_PartF_R0.1.docx

RUNTIME OVERLAY
This A3O-2100 Runtime Architecture PartF R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part F — Digital Twin Runtime

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Digital Twin Runtime model governing lifecycle, synchronization, simulation, state management and interaction between physical and digital entities within the A3O platform.

2. Digital Twin Principles

DTR-001 Every Digital Twin SHALL represent one governed physical or logical entity.
DTR-002 Twin synchronization SHALL preserve semantic consistency.
DTR-003 Twin state SHALL be traceable throughout its lifecycle.
DTR-004 Simulation and operational modes SHALL be explicitly distinguished.
DTR-005 Digital Twin Runtime SHALL remain implementation independent.

3. Canonical Digital Twin Components

4. Governance Constraints

DTG-001 Every Digital Twin SHALL have a globally unique canonical identifier.
DTG-002 Twin synchronization SHALL generate Runtime Evidence.
DTG-003 Twin lifecycle transitions SHALL be auditable and traceable.
DTG-004 Simulation results SHALL be distinguishable from operational evidence.
DTG-005 Federated Digital Twins SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming Runtime Architectures SHALL implement governed Digital Twin lifecycle management, synchronization, simulation and evidence generation while maintaining end-to-end traceability.

A3O-2100_Runtime_Architecture_PartG_R0.1.docx

RUNTIME OVERLAY
This A3O-2100 Runtime Architecture PartG R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part G — Agent Runtime

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Agent Runtime model governing autonomous and collaborative software agents, their lifecycle, reasoning, communication and coordination within the A3O Runtime.

2. Agent Runtime Principles

AGR-001 Every Agent SHALL execute within a governed Runtime context.

AGR-002 Agents SHALL operate only within approved policies and capabilities.

AGR-003 Agent decisions SHALL be observable and traceable.

AGR-004 Agent collaboration SHALL use canonical contracts and identities.

AGR-005 Agent Runtime SHALL remain implementation independent.

3. Canonical Agent Components

4. Governance Constraints

AGG-001 Every Agent SHALL have a globally unique canonical identifier.

AGG-002 Agent decisions SHALL generate Runtime Evidence.

AGG-003 Agent-to-Agent communication SHALL use governed contracts.

AGG-004 Agent policy violations SHALL generate governed Findings.

AGG-005 Federated agents SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming Runtime Architectures SHALL implement governed agent lifecycle management, secure collaboration, observable reasoning and complete decision traceability.

A3O-2100_Runtime_Architecture_PartH_R0.1.docx

RUNTIME OVERLAY

This A3O-2100 Runtime Architecture PartH R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part H — AI Runtime Integration

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical AI Runtime Integration model governing execution of AI capabilities, LLMs, ML models, reasoning engines, tools and retrieval services within the A3O Runtime.

2. AI Runtime Principles

AIR-001 AI Runtime SHALL execute only approved AI capabilities and models.

AIR-002 AI decisions SHALL be explainable where required by policy.

AIR-003 AI execution SHALL preserve semantic consistency and evidence traceability.

AIR-004 AI components SHALL interact through canonical contracts and identities.

AIR-005 AI Runtime SHALL remain implementation independent.

3. Canonical AI Runtime Components

4. Governance Constraints

AIG-001 Every AI model SHALL have a canonical identifier and version.

AIG-002 AI prompts, inputs and outputs SHALL be traceable where permitted by policy.

AIG-003 AI execution SHALL generate Runtime Evidence.

AIG-004 AI policy violations SHALL create governed Findings.

AIG-005 Federated AI Runtime SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming Runtime Architectures SHALL integrate AI services through governed execution, canonical interfaces, evidence generation and complete end-to-end traceability.

A3O-2100_Runtime_Architecture_PartI_R0.1.docx

RUNTIME OVERLAY
This A3O-2100 Runtime Architecture PartI R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part I — Runtime Observability and Telemetry

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Runtime Observability and Telemetry model governing collection, correlation, analysis and retention of operational telemetry, logs, metrics, traces and Runtime Evidence.

2. Observability Principles

OBS-001 Every significant runtime activity SHALL be observable.

OBS-002 Metrics, logs and traces SHALL use canonical identifiers.

OBS-003 Telemetry SHALL support real-time and historical analysis.

OBS-004 Observability SHALL preserve evidence integrity and provenance.

OBS-005 Observability SHALL remain implementation independent.

3. Canonical Observability Components

4. Governance Constraints

OBG-001 Every telemetry record SHALL reference a canonical execution identifier.

OBG-002 Runtime Evidence SHALL be immutable and auditable.

OBG-003 Observability policies SHALL govern telemetry retention.

OBG-004 Alert generation SHALL be policy driven and traceable.

OBG-005 Federated observability SHALL preserve semantic consistency and identity.

5. Conformance

Conforming Runtime Architectures SHALL implement canonical observability, telemetry collection, analytics and evidence management with complete end-to-end traceability.

A3O-2100_Runtime_Architecture_PartJ_R0.1.docx

RUNTIME OVERLAY
This A3O-2100 Runtime Architecture PartJ R0.1 source artifact is extended by partition-aware JAUS runtime behavior. Authority is time- and scope-bounded; loss of connectivity shall not expand autonomy. Local actions, state changes, conflicts and evidence gaps are retained for deterministic reconciliation after recovery.

A3O-2100 Runtime Architecture
Part J — Runtime Resilience, Recovery and Evolution

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical model for runtime resilience, fault tolerance, recovery, scaling, upgrade management and continuous evolution of the A3O Runtime Platform.

2. Runtime Resilience Principles

RRP-001 Runtime SHALL tolerate component failures without unacceptable mission impact.

RRP-002 Recovery SHALL preserve execution consistency and evidence integrity.

RRP-003 Runtime evolution SHALL be governed and reversible where required.

RRP-004 Scaling SHALL preserve interoperability and policy compliance.

RRP-005 Runtime resilience SHALL remain implementation independent.

3. Canonical Resilience Components

4. Governance Constraints

RRG-001 Every recovery action SHALL generate immutable Runtime Evidence.

RRG-002 Runtime upgrades SHALL reference approved ADRs and Baselines.

RRG-003 Compatibility SHALL be validated before activation of runtime changes.

RRG-004 Runtime rollback SHALL preserve state integrity and traceability.

RRG-005 Federated runtime environments SHALL evolve without violating canonical contracts or policies.

5. Conformance

Conforming Runtime Architectures SHALL implement governed resilience, recovery, compatibility validation, controlled evolution and complete operational traceability.

A3O-2300_AI_Architecture_PartA_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartA R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part A — Canonical AI Architecture Framework

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical framework for Artificial Intelligence within A3O, governing AI capabilities, reasoning, learning, decision support, explainability and lifecycle management.

2. AI Architecture Principles

CAF-001 AI capabilities SHALL operate under explicit governance policies.

CAF-002 AI SHALL preserve semantic consistency with canonical knowledge models.

CAF-003 AI decisions SHALL be explainable where required by policy.

CAF-004 AI SHALL produce objective evidence for significant decisions.

CAF-005 AI Architecture SHALL remain implementation independent.

3. Canonical AI Building Blocks

4. Governance Constraints

CAG-001 Every AI capability SHALL have a canonical identifier.

CAG-002 Every deployed model SHALL reference an approved baseline.

CAG-003 AI decisions SHALL be traceable to evidence where applicable.

CAG-004 AI changes SHALL be governed through ADRs.

CAG-005 Federated AI SHALL preserve identity, policy and semantic consistency.

5. Conformance

Conforming AI Architectures SHALL implement the canonical AI framework, governed lifecycle, explainability and end-to-end traceability.

A3O-2300_AI_Architecture_PartB_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartB R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part B — AI Models and Inference Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical architecture for AI models, inference execution, model lifecycle and governed deployment within the A3O platform.

2. AI Model Principles

AIM-001 Every AI model SHALL have a canonical identifier and version.

AIM-002 Inference SHALL execute only approved models.

AIM-003 Model execution SHALL produce traceable evidence.

AIM-004 Model interfaces SHALL use canonical contracts.

AIM-005 AI model architecture SHALL remain implementation independent.

3. Canonical AI Components

4. Governance Constraints

AMG-001 Every inference request SHALL reference an approved model version.

AMG-002 Model provenance SHALL remain traceable.

AMG-003 Evaluation results SHALL be retained as objective evidence.

AMG-004 Model deployment SHALL require governance approval.

AMG-005 Federated inference SHALL preserve identity, policy and semantic consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed model lifecycle management, controlled inference, objective evaluation and complete traceability.

A3O-2300_AI_Architecture_PartC_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartC R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part C — Knowledge Graph, Semantic Memory and RAG

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical architecture for Knowledge Graphs, Semantic Memory, vector knowledge stores and Retrieval-Augmented Generation (RAG) supporting governed AI reasoning within the A3O platform.

2. Knowledge and RAG Principles

KRG-001 AI knowledge SHALL originate from governed information assets.

KRG-002 Semantic Memory SHALL preserve canonical ontology and identity.

KRG-003 Retrieval SHALL be policy-governed and traceable.

KRG-004 Generated responses SHALL reference supporting evidence where required.

KRG-005 Knowledge services SHALL remain implementation independent.

3. Canonical Knowledge Components

4. Governance Constraints

KMG-001 Every knowledge asset SHALL have a canonical identifier.

KMG-002 Knowledge lineage SHALL remain completely traceable.

KMG-003 Retrieval operations SHALL generate Runtime Evidence.

KMG-004 Semantic changes SHALL be approved through governance.

KMG-005 Federated knowledge exchange SHALL preserve ontology, identity and policy consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed knowledge graphs, semantic memory, RAG workflows and evidence-backed retrieval while maintaining end-to-end traceability.

A3O-2300_AI_Architecture_PartD_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartD R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part D — Cognitive Reasoning Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Cognitive Reasoning Architecture governing symbolic reasoning, probabilistic inference, planning, decision support and hybrid reasoning across the A3O platform.

2. Cognitive Reasoning Principles

CRP-001 Reasoning SHALL operate on governed knowledge.

CRP-002 Reasoning SHALL preserve semantic consistency.

CRP-003 Reasoning outcomes SHALL be explainable where required.

CRP-004 Reasoning SHALL generate objective evidence and provenance.

CRP-005 Cognitive reasoning SHALL remain implementation independent.

3. Canonical Cognitive Components

4. Governance Constraints

CRG-001 Every reasoning asset SHALL have a canonical identifier.

CRG-002 Reasoning chains SHALL be fully traceable.

CRG-003 Reasoning decisions SHALL reference supporting evidence where required.

CRG-004 Changes to reasoning rules SHALL be governed through ADRs.

CRG-005 Federated reasoning SHALL preserve ontology, policy and identity consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed cognitive reasoning, hybrid inference, explainability and complete decision traceability.

A3O-2300_AI_Architecture_PartE_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartE R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part E — Multi-Agent Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Multi-Agent Architecture governing cooperation, coordination, negotiation, delegation and federation of autonomous AI agents within the A3O platform.

2. Multi-Agent Principles

MAP-001 Multi-Agent systems SHALL operate using governed capabilities and policies.

MAP-002 Agent collaboration SHALL preserve semantic consistency.

MAP-003 Coordination SHALL be observable and fully traceable.

MAP-004 Agent autonomy SHALL remain bounded by governance policies.

MAP-005 Multi-Agent Architecture SHALL remain implementation independent.

3. Canonical Multi-Agent Components

4. Governance Constraints

MAG-001 Every agent SHALL possess a globally unique canonical identifier.

MAG-002 Inter-agent communications SHALL use governed canonical contracts.

MAG-003 Collective decisions SHALL generate traceable evidence.

MAG-004 Agent federation SHALL preserve policy, identity and semantic consistency.

MAG-005 Multi-Agent topology changes SHALL be approved through governance where required.

5. Conformance

Conforming AI Architectures SHALL implement governed multi-agent collaboration, coordination, federation and complete end-to-end decision traceability.

A3O-2300_AI_Architecture_PartF_R0.1.docx

AI OVERLAY
This A3O-2300 AI Architecture PartF R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part F — AI Planning and Decision Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical AI Planning and Decision Architecture governing goal decomposition, planning, optimization, decision making, execution control and policy-driven autonomous behavior within the A3O platform.

2. Planning and Decision Principles

ADP-001 Planning SHALL operate on approved goals, policies and knowledge.

ADP-002 Decision making SHALL be evidence-based where applicable.

ADP-003 Planning SHALL preserve semantic consistency and traceability.

ADP-004 Autonomous decisions SHALL remain bounded by governance constraints.

ADP-005 Planning Architecture SHALL remain implementation independent.

3. Canonical Planning Components

4. Governance Constraints

APG-001 Every decision SHALL reference one or more approved goals.

APG-002 Planning artifacts SHALL have canonical identifiers and versions.

APG-003 Autonomous decisions SHALL generate objective Runtime Evidence.

APG-004 Planning policy changes SHALL be governed through ADRs.

APG-005 Federated planning SHALL preserve policy, semantic and identity consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed planning, evidence-based decision making, optimization and complete end-to-end traceability for autonomous and assisted decisions.

A3O-2300_AI_Architecture_PartG_R0.1.docx

AI OVERLAY
This A3O-2300 AI Architecture PartG R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part G — AI Governance and Explainability

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical governance and explainability architecture for AI capabilities, ensuring accountable operation, transparency, auditability and regulatory compliance across the A3O platform.

2. Governance Principles

AGP-001 Every AI capability SHALL operate under explicit governance policies.

AGP-002 Significant AI decisions SHALL be explainable where required.

AGP-003 AI governance SHALL preserve complete traceability.

AGP-004 Governance SHALL be evidence-based and auditable.

AGP-005 Governance architecture SHALL remain implementation independent.

3. Canonical Governance Components

4. Governance Constraints

AXG-001 Every governed AI decision SHALL reference applicable policies.

AXG-002 Explainability artifacts SHALL be versioned and traceable.

AXG-003 Audit records SHALL be immutable.

AXG-004 Governance exceptions SHALL require formal approval and evidence.

AXG-005 Federated AI governance SHALL preserve policy and semantic consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed AI oversight, explainability, auditability and policy enforcement with complete end-to-end traceability.

A3O-2300_AI_Architecture_PartH_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartH R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part H — AI Safety and Trust

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical AI Safety and Trust Architecture governing safe operation, trustworthiness, robustness, risk mitigation and assurance for AI capabilities across the A3O platform.

2. AI Safety Principles

AST-001 AI SHALL operate within approved safety boundaries.

AST-002 Trust SHALL be established through verifiable evidence and governance.

AST-003 Safety controls SHALL be continuously monitored.

AST-004 Unsafe AI behavior SHALL be detected and mitigated.

AST-005 Safety Architecture SHALL remain implementation independent.

3. Canonical Safety Components

4. Governance Constraints

ASG-001 Every AI deployment SHALL reference an approved safety profile.

ASG-002 Safety incidents SHALL generate immutable evidence.

ASG-003 Safety exceptions SHALL require explicit governance approval.

ASG-004 Trust assessments SHALL be versioned and auditable.

ASG-005 Federated AI SHALL preserve common safety and trust policies.

5. Conformance

Conforming AI Architectures SHALL implement governed AI safety, trust management, continuous risk monitoring and complete evidence-backed traceability.

A3O-2300_AI_Architecture_PartI_R0.1.docx

AI OVERLAY

This A3O-2300 AI Architecture PartI R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part I — AI Learning and Adaptation

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical AI Learning and Adaptation Architecture governing continuous learning, model adaptation, feedback processing, performance improvement and controlled knowledge evolution across the A3O platform.

2. Learning Principles

ALP-001 Learning SHALL use governed and trusted datasets.

ALP-002 Adaptation SHALL preserve semantic consistency and policy compliance.
ALP-003 Learning outcomes SHALL be measurable and reproducible.
ALP-004 Adaptation SHALL generate objective evidence and provenance.
ALP-005 Learning Architecture SHALL remain implementation independent.

3. Canonical Learning Components

4. Governance Constraints

ALG-001 Every learning cycle SHALL reference approved datasets and policies.
ALG-002 Adapted models SHALL receive new governed versions.
ALG-003 Learning evidence SHALL remain immutable and auditable.
ALG-004 Performance regression SHALL trigger governance review.
ALG-005 Federated learning SHALL preserve identity, policy and semantic consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed learning, controlled adaptation, continuous evaluation and complete evidence-backed traceability.

A3O-2300_AI_Architecture_PartJ_R0.1.docx

AI OVERLAY
This A3O-2300 AI Architecture PartJ R0.1 source artifact is extended by a strict AI-to-command barrier. Cognitive services produce observations, estimates, recommendations or action proposals with model/version provenance. They do not own JAUS transport, Access Control, local safety or policy authority and cannot directly transmit control messages.

A3O-2300 AI Architecture
Part J — AI Evolution and Continuous Improvement

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical architecture for governed evolution, continuous improvement, lifecycle optimization, capability maturity and long-term sustainability of AI capabilities within the A3O platform.

2. Evolution Principles

AEP-001 AI evolution SHALL be governed through approved architecture baselines.
AEP-002 Continuous improvement SHALL be evidence-driven.
AEP-003 Evolution SHALL preserve compatibility and semantic consistency.
AEP-004 Every AI release SHALL remain fully traceable.
AEP-005 AI evolution SHALL remain implementation independent.

3. Canonical Evolution Components

4. Governance Constraints

AEG-001 Every AI release SHALL reference an approved baseline.
AEG-002 Architectural evolution SHALL be approved through ADRs.
AEG-003 Improvement decisions SHALL be supported by objective evidence.
AEG-004 Deprecated AI capabilities SHALL remain traceable until retirement.
AEG-005 Federated AI evolution SHALL preserve policy, semantic and identity consistency.

5. Conformance

Conforming AI Architectures SHALL implement governed AI evolution, continuous improvement, compatibility management and complete lifecycle traceability.

A3O-3000_System_Architecture_PartA_R0.1.docx

COMPONENT OVERLAY
This A3O-3000 System Architecture PartA R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part A — Canonical System Architecture Framework

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical System Architecture Framework governing composition, structure, interfaces, lifecycle and operational behavior of complete A3O systems.

2. System Architecture Principles

SAF-001 Every system SHALL be composed from governed architectural building blocks.

SAF-002 System architecture SHALL preserve semantic consistency across all layers.

SAF-003 System behavior SHALL be observable and traceable.

SAF-004 System evolution SHALL follow approved governance baselines.

SAF-005 System Architecture SHALL remain implementation independent.

3. Canonical System Building Blocks

4. Governance Constraints

SFG-001 Every system SHALL reference an approved architecture baseline.

SFG-002 Every system component SHALL have a canonical identifier.

SFG-003 Cross-layer dependencies SHALL remain traceable.

SFG-004 Architectural changes SHALL be governed through ADRs.

SFG-005 Federated systems SHALL preserve semantic, policy and identity consistency.

5. Conformance

Conforming System Architectures SHALL implement the canonical system framework, governed composition, lifecycle management and complete architectural traceability.

A3O-3000_System_Architecture_PartB_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartB R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part B — System Composition

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical System Composition Architecture governing decomposition, composition, modularity, dependency management and assembly of A3O systems from governed architectural elements.

2. System Composition Principles

SCP-001 Every system SHALL be assembled from approved Architecture Building Blocks (ABBs).

SCP-002 System composition SHALL preserve semantic consistency across all modules.

SCP-003 Dependencies SHALL be explicit, governed and traceable.

SCP-004 Components SHALL support independent evolution where feasible.

SCP-005 System Composition SHALL remain implementation independent.

3. Canonical Composition Components

4. Governance Constraints

SCG-001 Every composition artifact SHALL have a canonical identifier and version.

SCG-002 Every module dependency SHALL be explicitly declared.

SCG-003 Composition validation SHALL precede deployment.

SCG-004 Structural changes SHALL be governed through ADRs.

SCG-005 Federated systems SHALL preserve composition compatibility and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed system composition, validated modular assembly, dependency management and complete architectural traceability.

A3O-3000_System_Architecture_PartC_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartC R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part C — Service Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Service Architecture governing service definition, lifecycle, contracts, composition, discovery and governance across A3O systems.

2. Service Architecture Principles

SVP-001 Every service SHALL implement an approved Capability.

SVP-002 Every service SHALL expose canonical contracts.

SVP-003 Services SHALL be independently deployable where feasible.

SVP-004 Service interactions SHALL be observable and traceable.

SVP-005 Service Architecture SHALL remain implementation independent.

3. Canonical Service Components

4. Governance Constraints

SVG-001 Every service SHALL have a canonical identifier and version.

SVG-002 Every service contract SHALL be approved before publication.

SVG-003 Breaking interface changes SHALL require compatibility assessment.

SVG-004 Service lifecycle changes SHALL be governed through ADRs.

SVG-005 Federated services SHALL preserve identity, policy and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed services, canonical contracts, lifecycle management and complete service traceability.

A3O-3000_System_Architecture_PartD_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartD R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part D — Data & Information Flow

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Data and Information Flow Architecture governing creation, movement, transformation, synchronization, lineage, quality and governance of information across A3O systems.

2. Data & Information Flow Principles

DIF-001 Every information flow SHALL use canonical information models.

DIF-002 Data transformations SHALL preserve semantic consistency.

DIF-003 Information lineage SHALL be complete and auditable.

DIF-004 Information exchange SHALL comply with governance and security policies.

DIF-005 Data Flow Architecture SHALL remain implementation independent.

3. Canonical Flow Components

4. Governance Constraints

DIG-001 Every information flow SHALL have a canonical identifier.

DIG-002 Every transformation SHALL be traceable from source to destination.

DIG-003 Information quality rules SHALL be governed and versioned.

DIG-004 Cross-domain information exchange SHALL enforce approved policies.

DIG-005 Federated information flows SHALL preserve semantic consistency and identity.

5. Conformance

Conforming System Architectures SHALL implement governed information flows, quality management, lineage, synchronization and complete end-to-end traceability.

A3O-3000_System_Architecture_PartE_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartE R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part E — Integration and Interoperability

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Integration and Interoperability Architecture governing system interaction, APIs, messaging, event exchange, protocol mediation and federation across A3O systems.

2. Integration Principles

INT-001 Every integration SHALL use canonical contracts.

INT-002 Interoperability SHALL preserve semantic consistency.

INT-003 Interfaces SHALL be versioned and governed.

INT-004 Cross-system exchanges SHALL be observable and traceable.

INT-005 Integration Architecture SHALL remain implementation independent.

3. Canonical Integration Components

4. Governance Constraints

ING-001 Every integration endpoint SHALL have a canonical identifier.

ING-002 Interface compatibility SHALL be validated before deployment.

ING-003 Integration events SHALL generate immutable evidence.

ING-004 Contract changes SHALL be governed through ADRs.

ING-005 Federated integrations SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed integration, interoperable interfaces, canonical contracts and complete end-to-end traceability.

A3O-3000_System_Architecture_PartF_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartF R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part F — Distributed System Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Distributed System Architecture governing distributed execution, node coordination, consistency, resilience, federation and scalability across A3O systems.

2. Distributed System Principles

DSP-001 Distributed systems SHALL be composed of governed runtime nodes.

DSP-002 Distributed coordination SHALL preserve semantic consistency.
DSP-003 State synchronization SHALL be observable and traceable.
DSP-004 Distributed execution SHALL tolerate partial failures.
DSP-005 Distributed Architecture SHALL remain implementation independent.

3. Canonical Distributed Components

4. Governance Constraints

DSG-001 Every distributed node SHALL have a canonical identifier.
DSG-002 Distributed topology SHALL be governed and versioned.
DSG-003 Replication and synchronization SHALL generate traceable evidence.
DSG-004 Distributed configuration changes SHALL be governed through ADRs.
DSG-005 Federated distributed systems SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed distributed execution, coordination, resilience, synchronization and complete end-to-end traceability.

A3O-3000_System_Architecture_PartG_R0.1.docx

COMPONENT OVERLAY
This A3O-3000 System Architecture PartG R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part G — Cyber-Physical System Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Cyber-Physical System (CPS) Architecture governing integration of physical assets, sensors, actuators, digital twins, real-time control and operational intelligence across A3O systems.

2. Cyber-Physical Principles

CPS-001 Every physical asset SHALL have a governed digital representation where applicable.
CPS-002 Cyber-physical interactions SHALL preserve semantic consistency.
CPS-003 Operational state SHALL be observable and traceable.
CPS-004 Safety-critical actions SHALL comply with governance and security policies.
CPS-005 CPS Architecture SHALL remain implementation independent.

3. Canonical CPS Components

4. Governance Constraints

CPG-001 Every cyber-physical asset SHALL have a canonical identifier.
CPG-002 Sensor and actuator interactions SHALL generate immutable operational evidence.
CPG-003 Digital Twin synchronization SHALL be continuously validated.
CPG-004 Safety policy changes SHALL be governed through ADRs.
CPG-005 Federated CPS deployments SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed cyber-physical integration, real-time coordination, Digital Twin synchronization, operational safety and complete end-to-end traceability.

A3O-3000_System_Architecture_PartH_R0.1.docx

COMPONENT OVERLAY
This A3O-3000 System Architecture PartH R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part H — System Security Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical System Security Architecture governing protection of services, information, identities, runtime environments, cyber-physical assets and AI capabilities across the A3O platform.

2. Security Principles

SSP-001 Security SHALL be integrated across every architectural layer.

SSP-002 Every access SHALL be authenticated, authorized and auditable.

SSP-003 Security controls SHALL preserve confidentiality, integrity and availability.

SSP-004 Security events SHALL generate immutable evidence.

SSP-005 Security Architecture SHALL remain implementation independent.

3. Canonical Security Components

4. Governance Constraints

SEG-001 Every security control SHALL have a canonical identifier.

SEG-002 Security policies SHALL be versioned and governed.

SEG-003 Security incidents SHALL generate immutable evidence.

SEG-004 Cryptographic assets SHALL follow approved lifecycle policies.

SEG-005 Federated security SHALL preserve identity, policy and trust consistency.

5. Conformance

Conforming System Architectures SHALL implement governed security services, policy enforcement, incident response and complete end-to-end security traceability.

A3O-3000_System_Architecture_PartI_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartI R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part I — System Operations and Lifecycle

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical System Operations and Lifecycle Architecture governing deployment, operation, monitoring, maintenance, change control, support and retirement of A3O systems.

2. Operations Principles

SOP-001 Every system SHALL operate under governed operational policies.

SOP-002 Operational activities SHALL be observable and auditable.

SOP-003 Lifecycle transitions SHALL preserve integrity and traceability.

SOP-004 Operational changes SHALL be controlled through governance.

SOP-005 Operations Architecture SHALL remain implementation independent.

3. Canonical Operations Components

4. Governance Constraints

SOG-001 Every operational change SHALL reference an approved change record.

SOG-002 Lifecycle transitions SHALL generate immutable evidence.

SOG-003 Configuration baselines SHALL be versioned.

SOG-004 Maintenance activities SHALL be planned and auditable.

SOG-005 Federated operations SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed operations, lifecycle management, controlled change processes and complete operational traceability.

A3O-3000_System_Architecture_PartJ_R0.1.docx

COMPONENT OVERLAY

This A3O-3000 System Architecture PartJ R0.1 source artifact is extended by JAUS component and service boundaries. Externally useful, independently discoverable capabilities may be exposed as JAUS components. Internal microservices remain internal unless addressability, lifecycle, control ownership or replaceability justify a formal JAUS interface.

A3O-3000 System Architecture
Part J — System Evolution and Governance

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical System Evolution and Governance Architecture governing architectural evolution, lifecycle governance, maturity management, compliance and continuous improvement of A3O systems.

2. Evolution and Governance Principles

SEGP-001 System evolution SHALL follow approved architecture baselines.

SEGP-002 Governance SHALL be evidence-driven and auditable.

SEGP-003 Evolution SHALL preserve interoperability and semantic consistency.

SEGP-004 Every architectural change SHALL be traceable throughout the lifecycle.

SEGP-005 Evolution Architecture SHALL remain implementation independent.

3. Canonical Evolution Components

4. Governance Constraints

SGG-001 Every architectural baseline SHALL have a canonical identifier and version.

SGG-002 Architectural decisions SHALL be recorded as governed ADRs.

SGG-003 Compliance assessments SHALL generate immutable evidence.

SGG-004 Evolution plans SHALL preserve backward compatibility where required.

SGG-005 Federated system governance SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming System Architectures SHALL implement governed architectural evolution, lifecycle governance, compliance management and complete end-to-end architectural traceability.

A3O-4000_Solution_Architecture_PartA_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartA R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A^3O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part A — Canonical Solution Architecture Framework

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Architecture Framework governing the design, composition, deployment and lifecycle management of complete business and mission solutions built on the A3O platform.

2. Solution Architecture Principles

SAF-4000-001 Every solution SHALL be composed from approved Architecture Building Blocks and Solution Building Blocks.

SAF-4000-002 Every solution SHALL implement governed business and mission capabilities.

SAF-4000-003 Solution architecture SHALL preserve semantic consistency, interoperability and traceability.

SAF-4000-004 Solution evolution SHALL follow approved baselines and governance policies.

SAF-4000-005 Solution Architecture SHALL remain implementation independent.

3. Canonical Solution Building Blocks

4. Governance Constraints

SLG-001 Every solution SHALL reference an approved architecture baseline.

SLG-002 Every solution SHALL have a canonical identifier and version.

SLG-003 Solution dependencies SHALL be explicitly documented and traceable.

SLG-004 Solution changes SHALL be governed through ADRs.

SLG-005 Federated solutions SHALL preserve policy, semantic and identity consistency.

5. Conformance

Conforming Solution Architectures SHALL implement the canonical solution framework, governed composition, lifecycle management and complete architectural traceability.

A3O-4000_Solution_Architecture_PartB_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartB R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part B — Solution Composition

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Composition Architecture governing decomposition, modular assembly, dependency management and hierarchical composition of enterprise and mission solutions within the A3O framework.

2. Solution Composition Principles

SCP-4000-001 Every solution SHALL be composed from governed Solution Building Blocks (SBBs).

SCP-4000-002 Solution composition SHALL preserve semantic and structural consistency.

SCP-4000-003 Dependencies between solution components SHALL be explicit and traceable.

SCP-4000-004 Solutions SHALL support modular and reusable composition patterns.

SCP-4000-005 Solution Composition SHALL remain implementation independent.

3. Canonical Composition Components

4. Governance Constraints

SCPG-001 Every solution composition SHALL have a canonical identifier and version.
SCPG-002 All component dependencies SHALL be explicitly declared and validated.
SCPG-003 Composition validation SHALL occur prior to deployment.
SCPG-004 Composition changes SHALL be governed through ADRs.
SCPG-005 Federated compositions SHALL preserve semantic, policy and identity consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed composition mechanisms, modular assembly, dependency validation and complete traceability of solution structures.

A3O-4000_Solution_Architecture_PartC_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartC R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part C — Solution Patterns and Blueprints

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Patterns and Blueprints Architecture providing reusable, governed architectural templates for enterprise, mission and domain solutions built on A3O.

2. Pattern Principles

SPB-001 Every solution pattern SHALL be governed and versioned.

SPB-002 Patterns SHALL be reusable across domains.

SPB-003 Blueprints SHALL preserve semantic consistency and interoperability.

SPB-004 Blueprint usage SHALL be traceable and auditable.

SPB-005 Pattern Architecture SHALL remain implementation independent.

3. Canonical Pattern Types

4. Governance Constraints

SPG-001 Every blueprint SHALL have a canonical identifier and version.

SPG-002 Blueprint modifications SHALL be governed through ADRs.

SPG-003 Approved patterns SHALL reference supported architecture baselines.

SPG-004 Pattern validation SHALL precede publication.

SPG-005 Federated blueprint repositories SHALL preserve semantic and policy consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed reusable patterns, validated blueprints, controlled lifecycle management and complete architectural traceability.

A3O-4000_Solution_Architecture_PartD_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartD R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part D — Business Solution Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Business Solution Architecture governing business capabilities, processes, value streams, KPIs and organizational alignment within A3O solutions.

2. Business Architecture Principles

BSA-001 Business capabilities SHALL be explicitly modeled and governed.

BSA-002 Business processes SHALL be traceable to system capabilities.

BSA-003 Value streams SHALL be measurable and evidence-based.

BSA-004 Business architecture SHALL align with system and AI architecture.

BSA-005 Business architecture SHALL remain implementation independent.

3. Canonical Business Components

4. Governance Constraints

BSG-001 Every business capability SHALL have a canonical identifier.

BSG-002 Business processes SHALL be traceable to system services.

BSG-003 KPIs SHALL be derived from governed data sources.

BSG-004 Business changes SHALL be governed through ADRs.

BSG-005 Federated business models SHALL preserve semantic consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed business modeling, capability alignment, KPI traceability and end-to-end business visibility.

A3O-4000_Solution_Architecture_PartE_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartE R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part E — Mission Solution Architecture

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Mission Solution Architecture governing mission threads, operational objectives, cross-domain coordination, execution planning and mission lifecycle management within A3O solutions.

2. Mission Architecture Principles

MSA-001 Every mission SHALL be explicitly defined and governed.

MSA-002 Mission execution SHALL be traceable end-to-end.

MSA-003 Mission objectives SHALL be measurable and evidence-based.

MSA-004 Missions SHALL coordinate across systems, agents and services.

MSA-005 Mission Architecture SHALL remain implementation independent.

3. Canonical Mission Components

4. Governance Constraints

MSG-001 Every mission SHALL have a canonical identifier.

MSG-002 Mission state transitions SHALL generate immutable evidence.

MSG-003 Mission plans SHALL be governed and versioned.

MSG-004 Mission changes SHALL require governance approval.

MSG-005 Federated missions SHALL preserve semantic and policy consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed mission execution, cross-domain coordination, objective tracking and complete mission traceability.

A3O-4000_Solution_Architecture_PartF_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartF R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A^{3}O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part F — Enterprise Solution Integration

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Enterprise Solution Integration Architecture governing integration of solutions with enterprise systems, external ecosystems, legacy platforms and cross-organizational infrastructures within A3O.

2. Enterprise Integration Principles

ESI-001 Every enterprise integration SHALL use governed interfaces and contracts.

ESI-002 Integration SHALL preserve semantic consistency across organizational boundaries.

ESI-003 Legacy systems SHALL be abstracted via integration layers.

ESI-004 Cross-enterprise data exchange SHALL be traceable and auditable.

ESI-005 Integration Architecture SHALL remain implementation independent.

3. Canonical Enterprise Integration Components

4. Governance Constraints

ESG-001 Every enterprise integration SHALL have a canonical identifier.
ESG-002 All integration contracts SHALL be governed and versioned.
ESG-003 Data exchanges SHALL generate immutable evidence.
ESG-004 Integration changes SHALL require governance approval.
ESG-005 Federated enterprise integrations SHALL preserve policy and semantic consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed enterprise integration, legacy abstraction, cross-domain interoperability and complete traceability.

A3O-4000_Solution_Architecture_PartG_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartG R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part G — Digital Solution Platform

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Digital Solution Platform Architecture governing unified platform services, shared capabilities, runtime foundation, and ecosystem enablement for all A3O solutions.

2. Platform Principles

DSP-4000-001 The platform SHALL provide unified capabilities for all solutions.

DSP-4000-002 Platform services SHALL be reusable and composable.

DSP-4000-003 Platform SHALL enforce governance and policy uniformly.

DSP-4000-004 Platform operations SHALL be observable and traceable.

DSP-4000-005 Platform Architecture SHALL remain implementation independent.

3. Canonical Platform Components

4. Governance Constraints

DSPG-001 Every platform capability SHALL have a canonical identifier.
DSPG-002 Platform services SHALL enforce consistent policies across all solutions.
DSPG-003 Platform state SHALL be fully observable and auditable.
DSPG-004 Platform changes SHALL require governance approval.
DSPG-005 Federated platform deployments SHALL preserve semantic and policy consistency.

5. Conformance

Conforming Solution Architectures SHALL implement a unified digital platform, shared services, governance enforcement and complete lifecycle traceability.

A3O-4000_Solution_Architecture_PartH_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartH R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part H — Solution Security & Compliance

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Security and Compliance Architecture governing security, privacy, risk management, regulatory compliance and assurance for all A3O solutions.

2. Security & Compliance Principles

SSC-4000-001 Every solution SHALL enforce security by design and by default.

SSC-4000-002 Compliance SHALL be continuously verifiable and evidence-based.

SSC-4000-003 Risk SHALL be assessed across all solution components.

SSC-4000-004 Security controls SHALL be uniformly enforced across platform layers.

SSC-4000-005 Security and Compliance Architecture SHALL remain implementation independent.

3. Canonical Security & Compliance Components

4. Governance Constraints

SSC-001 Every compliance control SHALL be mapped to a regulatory requirement.
SSC-002 Security incidents SHALL generate immutable evidence.

SSC-003 Risk assessments SHALL be continuously updated.
SSC-004 Policy violations SHALL trigger governance workflows.
SSC-005 Federated compliance SHALL preserve consistency across domains.

5. Conformance

Conforming Solution Architectures SHALL implement governed security and compliance, continuous assurance and complete auditability.

A3O-4000_Solution_Architecture_PartI_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartI R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part I — Solution Lifecycle Management

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Lifecycle Management Architecture governing planning, design, implementation, deployment, operation, maintenance, modernization and retirement of A3O solutions.

2. Lifecycle Principles

SLM-001 Every solution SHALL follow a governed lifecycle.
SLM-002 Lifecycle transitions SHALL be traceable and evidence-based.
SLM-003 Configuration and releases SHALL be version controlled.
SLM-004 Operational feedback SHALL drive continuous improvement.
SLM-005 Lifecycle Architecture SHALL remain implementation independent.

3. Canonical Lifecycle Components

4. Governance Constraints

SLMG-001 Every lifecycle stage SHALL have defined entry and exit criteria.
SLMG-002 Every release SHALL reference an approved baseline.
SLMG-003 Lifecycle events SHALL generate immutable evidence.
SLMG-004 Major lifecycle changes SHALL require governance approval.
SLMG-005 Federated lifecycle management SHALL preserve policy and semantic consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed lifecycle management, controlled releases, operational feedback integration and complete lifecycle traceability.

A3O-4000_Solution_Architecture_PartJ_R0.1.docx

SOLUTION OVERLAY

This A3O-4000 Solution Architecture PartJ R0.1 source artifact is extended into cross-industry profiles for logistics, manufacturing, inspection, medical robotics, security and defence. The universal A³O core remains unchanged; each profile adds domain ontology, hazards, workflow, privacy, compliance and conformance requirements.

A3O-4000 Solution Architecture
Part J — Solution Evolution & Portfolio Governance

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Evolution and Portfolio Governance Architecture governing long-term evolution of solutions, portfolio management, strategic alignment, capability investment prioritization, and continuous optimization of A3O solution ecosystems.

2. Evolution & Portfolio Principles

SEP-4000-001 Solution portfolios SHALL be governed as strategic assets.
SEP-4000-002 Evolution SHALL be evidence-driven and value-oriented.
SEP-4000-003 Portfolio decisions SHALL preserve semantic and architectural consistency.

SEP-4000-004 Investment prioritization SHALL be traceable to business capabilities and missions.

SEP-4000-005 Portfolio Architecture SHALL remain implementation independent.

3. Canonical Portfolio Components

4. Governance Constraints

SPGJ-001 Every portfolio element SHALL have a canonical identifier and version.
SPGJ-002 Portfolio decisions SHALL be recorded as governed ADRs.
SPGJ-003 Investment decisions SHALL be justified by measurable value evidence.
SPGJ-004 Evolution roadmap changes SHALL require governance approval.
SPGJ-005 Federated portfolios SHALL preserve semantic and policy consistency.

5. Conformance

Conforming Solution Architectures SHALL implement governed portfolio management, strategic evolution planning, value-based prioritization and full lifecycle traceability.

A3O-5000_Architecture_Compliance_Framework_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Architecture Compliance Framework R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Architecture Compliance Framework

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical compliance framework governing verification, validation, conformance assessment and certification of A3O implementations.

2. Scope

Applies to all architecture levels from Meta Model through Implementation.

3. Architectural Position

Compliance is a cross-cutting architecture capability owned by Enterprise Governance and applied to every domain.

4. Canonical Compliance Model

5. Normative Requirements

CCR-001 Every architecture artifact SHALL be assessable.
CCR-002 Every normative requirement SHALL have objective verification criteria.
CCR-003 Compliance evidence SHALL reference governing architecture requirements.
CCR-004 Non-conformance SHALL trigger corrective action records.
CCR-005 Certification SHALL require successful verification and validation.
CCR-006 Compliance records SHALL remain immutable.
CCR-007 Continuous compliance SHALL be supported throughout the lifecycle.
CCR-008 Compliance SHALL be technology independent.
CCR-009 Compliance metrics SHALL be measurable.
CCR-010 Every implementation SHALL support independent audit.

6. Conformance Classes

Level C0 – Informative
Level C1 – Foundation
Level C2 – Domain Conformant
Level C3 – Runtime Conformant
Level C4 – Enterprise Certified

7. Traceability

Every compliance decision SHALL be traceable to Meta Model, governing requirements, verification evidence, approval records and certification status.

8. Conformance

A conforming implementation SHALL satisfy all mandatory requirements applicable to its declared conformance class.

A3O-5000_Enterprise_Mission_Solutions_PartA_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartA R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part A — Canonical Enterprise & Mission Solutions Framework

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Enterprise & Mission Solutions Framework governing design, composition, deployment and governance of integrated enterprise, governmental, defense and cross-domain mission solutions built on A3O.

2. Enterprise & Mission Principles

EMS-001 Every solution SHALL align with approved enterprise and mission objectives.

EMS-002 Enterprise and mission capabilities SHALL be governed throughout their lifecycle.

EMS-003 Cross-domain collaboration SHALL preserve semantic consistency.

EMS-004 Operational outcomes SHALL be measurable and evidence-based.

EMS-005 The framework SHALL remain implementation independent.

3. Canonical Solution Domains

4. Governance Constraints

EMG-001 Every enterprise or mission solution SHALL have a canonical identifier and version.

EMG-002 Solution governance SHALL reference approved architecture baselines.

EMG-003 Operational evidence SHALL be retained for audit.

EMG-004 Strategic changes SHALL require governance approval.

EMG-005 Federated ecosystems SHALL preserve policy, identity and semantic consistency.

5. Conformance

Conforming Enterprise & Mission Solutions SHALL implement governed solution architectures, measurable outcomes, lifecycle governance and complete end-to-end traceability.

A3O-5000_Enterprise_Mission_Solutions_PartB_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartB R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part B — Enterprise Business Solutions

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Enterprise Business Solutions Architecture governing design and execution of business-focused enterprise solutions including strategy, operations, value delivery and enterprise capability alignment within A3O.

2. Business Solution Principles

EBS-001 Business solutions SHALL be aligned with enterprise capabilities and objectives.

EBS-002 Value delivery SHALL be measurable and evidence-based.

EBS-003 Business processes SHALL be traceable to system services.

EBS-004 Organizational alignment SHALL be explicitly modeled.

EBS-005 Architecture SHALL remain implementation independent.

3. Canonical Business Solution Components

4. Governance Constraints

EBSG-001 Every business solution SHALL have a canonical identifier.
EBSG-002 Business capabilities SHALL be governed and versioned.
EBSG-003 Value metrics SHALL be evidence-backed.
EBSG-004 Changes SHALL require governance approval.
EBSG-005 Federated business solutions SHALL preserve semantic consistency.

5. Conformance

Conforming Enterprise Solutions SHALL implement governed business capability alignment, measurable value delivery and full lifecycle traceability.

A3O-5000_Enterprise_Mission_Solutions_PartC_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartC R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part C — Government & Public Sector Solutions

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Government & Public Sector Solutions Architecture governing eGovernment systems, public services delivery, regulatory compliance, citizen services, transparency and inter-agency interoperability within A3O.

2. Public Sector Principles

GPS-001 Public sector solutions SHALL ensure transparency and accountability.

GPS-002 Citizen services SHALL be accessible, secure and traceable.

GPS-003 Regulatory compliance SHALL be embedded by design.

GPS-004 Inter-agency data exchange SHALL be governed and auditable.

GPS-005 Architecture SHALL remain implementation independent.

3. Canonical Public Sector Components

4. Governance Constraints

GPSG-001 Every public service SHALL have a canonical identifier.
GPSG-002 All citizen interactions SHALL be auditable.
GPSG-003 Regulatory rules SHALL be versioned and traceable.
GPSG-004 Data sharing SHALL comply with governance policies.
GPSG-005 Federated government systems SHALL preserve policy and identity consistency.

5. Conformance

Conforming Government Solutions SHALL implement governed public services, transparency, regulatory compliance and full lifecycle traceability.

A3O-5000_Enterprise_Mission_Solutions_PartD_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartD R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part D — Defense & Security Solutions

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Defense & Security Solutions Architecture governing national security systems, defense operations, cyber defense, intelligence support systems and critical security infrastructures within A3O.

2. Defense & Security Principles

DSS-001 Defense solutions SHALL operate under strict governance and control policies.

DSS-002 Security operations SHALL be traceable, auditable and evidence-based.

DSS-003 Threat response SHALL be real-time and coordinated.

DSS-004 Sensitive systems SHALL enforce zero-trust principles.

DSS-005 Architecture SHALL remain implementation independent.

3. Canonical Defense Components

4. Governance Constraints

DSSG-001 Every defense capability SHALL have a canonical identifier.
DSSG-002 Sensitive operations SHALL be fully audited and traceable.
DSSG-003 Threat intelligence SHALL be governed and validated.
DSSG-004 Access to defense systems SHALL follow zero-trust principles.
DSSG-005 Federated defense systems SHALL preserve policy and operational consistency.

5. Conformance

Conforming Defense Solutions SHALL implement governed security operations, intelligence processing, real-time response and full lifecycle traceability.

A3O-5000_Enterprise_Mission_Solutions_PartE_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartE R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part E — Industrial & Critical Infrastructure Solutions

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Industrial & Critical Infrastructure Solutions Architecture governing industrial systems, energy systems, transportation, utilities, and critical national infrastructure within A3O.

2. Industrial Principles

ICS-001 Industrial systems SHALL be safety-critical and governed.

ICS-002 Infrastructure operations SHALL be continuously monitored.

ICS-003 Fail-safe and resilience SHALL be mandatory design properties.

ICS-004 Cyber-physical integration SHALL be traceable and secure.

ICS-005 Architecture SHALL remain implementation independent.

3. Canonical Industrial Components

4. Governance Constraints

ICSG-001 Every industrial asset SHALL have a canonical identifier.
ICSG-002 Safety-critical operations SHALL be fully auditable.
ICSG-003 Infrastructure failures SHALL generate immutable evidence.
ICSG-004 Control systems SHALL enforce strict access policies.
ICSG-005 Federated industrial systems SHALL preserve safety and operational consistency.

5. Conformance

Conforming Industrial Solutions SHALL implement governed critical infrastructure management, safety controls, monitoring and full lifecycle traceability.

A3O-5000_Enterprise_Mission_Solutions_PartF_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartF R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part F — Smart City & Digital Twin Solutions

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Smart City & Digital Twin Solutions Architecture governing urban systems, smart infrastructure, real-time city operations, digital twins, and urban intelligence across A3O ecosystems.

2. Smart City Principles

SCT-001 Cities SHALL be modeled as integrated digital-physical systems.

SCT-002 All urban assets SHALL have digital twin representations where applicable.

SCT-003 City operations SHALL be real-time and data-driven.

SCT-004 Citizen-centric services SHALL be secure and accessible.

SCT-005 Architecture SHALL remain implementation independent.

3. Canonical Smart City Components

4. Governance Constraints

SCTG-001 Every urban asset SHALL have a canonical identifier.
SCTG-002 City-wide data SHALL be governed and auditable.
SCTG-003 Digital twin synchronization SHALL be continuous.
SCTG-004 Citizen data SHALL be protected under strict policies.
SCTG-005 Federated smart city systems SHALL preserve semantic consistency.

5. Conformance

Conforming Smart City Solutions SHALL implement governed urban intelligence, digital twins, real-time operations and full lifecycle traceability.

A3O-5000_Enterprise_Mission_Solutions_PartG_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartG R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part G — Cross-Domain Mission Solutions

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Cross-Domain Mission Solutions Architecture governing coordination of complex missions spanning multiple domains including government, defense, industry, cyber-physical systems and enterprise ecosystems within A3O.

2. Cross-Domain Principles

CDM-001 Missions SHALL operate across multiple governed domains.

CDM-002 Cross-domain coordination SHALL preserve semantic consistency.

CDM-003 Execution SHALL be traceable end-to-end across all domains.

CDM-004 Domain boundaries SHALL be explicitly modeled and governed.

CDM-005 Architecture SHALL remain implementation independent.

3. Canonical Cross-Domain Components

4. Governance Constraints

CDMG-001 Every cross-domain mission SHALL have a canonical identifier.
CDMG-002 Domain transitions SHALL be governed and audited.
CDMG-003 Cross-domain data flows SHALL be policy controlled.
CDMG-004 Mission execution SHALL maintain full traceability across domains.
CDMG-005 Federated missions SHALL preserve semantic and policy consistency.

5. Conformance

Conforming Mission Architectures SHALL implement governed cross-domain coordination, unified execution, and complete mission lifecycle traceability.

A3O-5000_Enterprise_Mission_Solutions_PartH_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartH R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part H — Federated Enterprise Ecosystems

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Federated Enterprise Ecosystems Architecture governing interoperability, federation, governance alignment and shared operations across multiple enterprises, agencies and domains within A3O.

2. Federation Principles

FEE-001 Ecosystems SHALL support multi-organization federation.

FEE-002 Federation SHALL preserve semantic consistency across participants.

FEE-003 Governance policies SHALL be interoperable and enforceable.

FEE-004 Shared services SHALL be discoverable and reusable.

FEE-005 Architecture SHALL remain implementation independent.

3. Canonical Ecosystem Components

4. Governance Constraints

FEG-001 Every federation SHALL have a canonical identifier.
FEG-002 Inter-organizational interactions SHALL be auditable.
FEG-003 Policy alignment SHALL be continuously enforced.
FEG-004 Shared resources SHALL be governed and versioned.
FEG-005 Federated ecosystems SHALL preserve identity, policy and semantic consistency.

5. Conformance

Conforming Enterprise Ecosystems SHALL implement governed federation, shared services, identity trust and complete cross-organization traceability.

A3O-5000_Enterprise_Mission_Solutions_PartI_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartI R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part I — Solution Operations & Mission Assurance

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Solution Operations & Mission Assurance Architecture governing operational execution, mission reliability, assurance, monitoring, resilience and continuous validation of enterprise and mission solutions within A3O.

2. Operations & Assurance Principles

OMA-001 All operations SHALL be continuously observable.

OMA-002 Mission assurance SHALL be evidence-based and continuously validated.

OMA-003 System resilience SHALL be designed for partial failure tolerance.

OMA-004 Operational execution SHALL be governed and traceable.

OMA-005 Architecture SHALL remain implementation independent.

3. Canonical Operations Components

4. Governance Constraints

OMG-001 Every operational event SHALL generate immutable evidence.
OMG-002 Mission assurance checks SHALL be continuous.

OMG-003 SLA violations SHALL be traceable and actionable.
OMG-004 Operational changes SHALL require governance approval.
OMG-005 Federated operations SHALL preserve consistency and traceability.

5. Conformance

Conforming Solutions SHALL implement governed operations, mission assurance, resilience and full lifecycle observability.

A3O-5000_Enterprise_Mission_Solutions_PartJ_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5000 Enterprise Mission Solutions PartJ R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5000 Enterprise & Mission Solutions
Part J — Strategic Transformation & Enterprise Evolution

Release: R0.1 Working Draft
Status: Extended Draft

1. Purpose

Defines the canonical Strategic Transformation & Enterprise Evolution Architecture governing long-term enterprise change, digital transformation, capability evolution, modernization strategy and adaptive enterprise restructuring within A3O.

2. Transformation Principles

STE-001 Enterprise transformation SHALL be capability-driven.

STE-002 All transformation initiatives SHALL be evidence-based.

STE-003 Evolution SHALL preserve interoperability and semantic consistency.

STE-004 Strategic change SHALL be governed and traceable.

STE-005 Architecture SHALL remain implementation independent.

3. Canonical Transformation Components

4. Governance Constraints

STEG-001 Every transformation initiative SHALL have a canonical identifier.
STEG-002 Strategic changes SHALL be approved via governance boards.
STEG-003 Transformation outcomes SHALL be measured and audited.
STEG-004 Roadmap updates SHALL be traceable and versioned.
STEG-005 Federated transformation SHALL preserve semantic and policy consistency.

5. Conformance

Conforming Enterprise Systems SHALL implement governed transformation management, capability evolution, modernization planning and full lifecycle traceability.

A3O-5100_Architecture_Governance_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5100 Architecture Governance R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5100 Architecture Governance

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical governance model controlling the evolution, approval, operation and retirement of A3O architectural assets.

2. Scope

Applies to all architecture levels, domains, specifications, products and implementations.

3. Governance Principles

Governance SHALL be evidence-driven.

Every architectural decision SHALL have an accountable owner.

Changes SHALL preserve backward traceability.

Governance SHALL be technology independent.

4. Governance Model

5. Normative Requirements

AGR-001 Every architectural artifact SHALL have an owner.
AGR-002 Architectural changes SHALL be reviewed before approval.
AGR-003 Approved changes SHALL update traceability records.
AGR-004 Governance decisions SHALL be auditable.
AGR-005 Policies SHALL supersede implementation-specific rules.
AGR-006 Exceptions SHALL include rationale and expiry.
AGR-007 Governance metrics SHALL be collected.
AGR-008 Every baseline SHALL be reproducible.
AGR-009 Governance SHALL support federation.
AGR-010 Implementations SHALL comply with approved governance.

6. Decision Lifecycle

Proposal → Review → Assessment → Approval → Publication → Monitoring → Revision → Retirement

7. Conformance

Conforming organizations SHALL operate an Architecture Authority, maintain decision records, preserve traceability and enforce governance policies.

A3O-5200_Architecture_Views_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5200 Architecture Views R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5200 Architecture Views

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical architectural views used to describe, communicate and validate A3O architectures.

2. Scope

Applicable to all architecture levels and all conformant A3O implementations.

3. Architectural Principles

Every architecture description SHALL be expressed through one or more canonical views.

4. Canonical View Catalog

5. Normative Requirements

AVR-001 Every architecture SHALL include a Context View.
AVR-002 Every Capability SHALL appear in a Capability View.
AVR-003 Runtime behavior SHALL be documented in a Runtime View.
AVR-004 Deployment topology SHALL be represented separately from Runtime behavior.
AVR-005 Security concerns SHALL be documented in a Security View.
AVR-006 Every view SHALL reference canonical identifiers.
AVR-007 Cross-view consistency SHALL be maintained.
AVR-008 Views SHALL remain technology independent.
AVR-009 Every view SHALL support traceability.
AVR-010 Every published architecture SHALL declare its supported views.

6. Conformance

A conforming architecture description SHALL provide all mandatory canonical views applicable to its declared scope.

A3O-5300_Architecture_Viewpoints_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5300 Architecture Viewpoints R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5300 Architecture Viewpoints

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines canonical viewpoints governing how A3O architecture views are constructed, interpreted and evaluated by stakeholders.

2. Scope

Applies to all architecture descriptions, models and viewpoints within the A3O framework.

3. Viewpoint Principles

Every architecture view SHALL conform to exactly one primary viewpoint.

4. Canonical Viewpoint Catalog

5. Normative Requirements

VPR-001 Every viewpoint SHALL define stakeholder concerns.
VPR-002 Every viewpoint SHALL specify permitted architecture views.
VPR-003 Viewpoints SHALL reference canonical concepts only.
VPR-004 Viewpoints SHALL preserve semantic consistency.
VPR-005 Cross-viewpoint traceability SHALL be maintained.
VPR-006 Viewpoints SHALL remain technology independent.
VPR-007 Viewpoints SHALL define evaluation criteria.
VPR-008 Every architecture description SHALL declare supported viewpoints.
VPR-009 Viewpoint extensions SHALL preserve backward compatibility.
VPR-010 Conformance SHALL be objectively assessable.

6. Conformance

Conforming A3O architecture descriptions SHALL identify applicable viewpoints and satisfy all mandatory viewpoint requirements.

A3O-5400_Canonical_Registries_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5400 Canonical Registries R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5400 Canonical Registries

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical registries required to uniquely identify, govern and trace all architectural objects in A3O.

2. Scope

Applies to every architecture level, domain and implementation.

3. Registry Principles

Every canonical object SHALL be registered exactly once in its authoritative registry.

4. Canonical Registry Catalog

5. Normative Requirements

RGR-001 Every registry entry SHALL have a globally unique identifier.
RGR-002 Registry ownership SHALL be explicitly defined.
RGR-003 Registry updates SHALL be governed.
RGR-004 Historical versions SHALL remain available.

RGR-005 Registry records SHALL be traceable.
RGR-006 Registry schemas SHALL be technology independent.
RGR-007 Registry synchronization SHALL preserve semantic consistency.
RGR-008 Registry access SHALL be policy controlled.
RGR-009 Registry integrity SHALL be continuously verified.
RGR-010 Registry conformance SHALL be auditable.

6. Conformance

Conforming implementations SHALL maintain authoritative canonical registries and preserve their integrity, traceability and governance.

A3O-5500_Reference_Catalog_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5500 Reference Catalog R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5500 Reference Catalog

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical catalog of reference architecture assets, reusable specifications, patterns and normative artifacts used throughout A3O.

2. Scope

Applies to all reference artifacts, reusable models and architecture deliverables.

3. Catalog Principles

Every reusable architectural artifact SHALL be uniquely cataloged and version controlled.

4. Reference Catalog

5. Normative Requirements

CAR-001 Every catalog entry SHALL have a persistent identifier.
CAR-002 Every artifact SHALL identify its authoritative owner.
CAR-003 Catalog entries SHALL preserve version history.
CAR-004 Superseded artifacts SHALL remain accessible for traceability.
CAR-005 Catalog metadata SHALL be technology independent.
CAR-006 Reusable artifacts SHALL reference canonical registries.
CAR-007 Catalog publication SHALL follow governance approval.
CAR-008 Every baseline SHALL reference applicable catalog artifacts.
CAR-009 Catalog integrity SHALL be continuously verified.
CAR-010 Catalog conformance SHALL be auditable.

6. Conformance

Conforming A3O implementations SHALL reference only approved catalog artifacts applicable to their declared baseline and conformance class.

A3O-5600_Architecture_Decision_Records_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5600 Architecture Decision Records R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5600 Architecture Decision Records (ADR)

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical Architecture Decision Record (ADR) model used to capture, govern and trace architectural decisions throughout the A3O lifecycle.

2. Scope

Applies to every normative architectural decision affecting the A3O baseline, reference architectures and implementations.

3. ADR Principles

Every significant architectural decision SHALL be documented as an immutable Architecture Decision Record.

4. ADR Canonical Model

5. Normative Requirements

ADRR-001 ADRs SHALL be immutable after approval except through superseding ADRs.
ADRR-002 Every baseline change SHALL reference one or more ADRs.
ADRR-003 ADRs SHALL reference canonical object identifiers.
ADRR-004 Superseded ADRs SHALL remain accessible.
ADRR-005 ADRs SHALL support independent audit.
ADRR-006 ADR metadata SHALL be technology independent.
ADRR-007 ADR repositories SHALL be version controlled.
ADRR-008 ADR relationships SHALL be traceable.
ADRR-009 ADR publication SHALL follow governance approval.
ADRR-010 ADR conformance SHALL be objectively verifiable.

6. ADR Lifecycle

Proposed → Under Review → Approved → Effective → Superseded → Retired

7. Conformance

Conforming A3O organizations SHALL maintain Architecture Decision Records for all normative architectural changes.

A3O-5700_Architecture_Conformance_Assessment_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5700 Architecture Conformance Assessment R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A^{3}O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5700 Architecture Conformance Assessment

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical assessment process used to determine conformance of architecture artifacts, systems and implementations with the A3O baseline.

2. Scope

Applies to all architecture levels, specifications, implementations and certified products.

3. Assessment Principles

Conformance assessment SHALL be objective, repeatable, evidence-based and traceable.

4. Assessment Model

5. Normative Requirements

ACA-001 Assessments SHALL evaluate all applicable mandatory requirements.
ACA-002 Assessment criteria SHALL be published before execution.
ACA-003 Assessment evidence SHALL reference canonical identifiers.
ACA-004 Assessment results SHALL be reproducible.
ACA-005 Corrective actions SHALL remain traceable.
ACA-006 Assessment reports SHALL be retained for audit.
ACA-007 Assessment tools SHALL NOT alter evaluated artifacts.
ACA-008 Reassessment SHALL verify corrective actions.
ACA-009 Assessment metrics SHALL be measurable.
ACA-010 Assessment processes SHALL be governed.

6. Conformance

Conforming organizations SHALL conduct architecture assessments according to this specification and maintain complete assessment evidence.

A3O-5800_Architecture_Certification_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5800 Architecture Certification R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5800 Architecture Certification

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical certification framework for A3O architectures, products, platforms and implementations.

2. Scope

Applies to organizations, products, runtime environments and implementations claiming A3O conformance.

3. Certification Principles

Certification SHALL be independent, evidence-based, repeatable and governed.

4. Certification Model

5. Normative Requirements

ACER-001 Certification SHALL be based on approved conformance assessments.
ACER-002 Certification evidence SHALL remain reproducible.
ACER-003 Certification SHALL reference the governing baseline release.
ACER-004 Certified artifacts SHALL retain persistent identifiers.
ACER-005 Certification changes SHALL be governed.
ACER-006 Certification records SHALL remain auditable.
ACER-007 Certification status SHALL be continuously maintainable.
ACER-008 Certification SHALL support federation.
ACER-009 Certification metadata SHALL be technology independent.
ACER-010 Certification SHALL preserve complete traceability.

6. Conformance

Organizations claiming A3O certification SHALL satisfy all applicable certification requirements and maintain valid certification evidence.

A3O-5900_Architecture_Metrics_R0.1.docx

CONFORMANCE OVERLAY

This A3O-5900 Architecture Metrics R0.1 source artifact is extended by J0–J4 compatibility levels, standards/profile/version matrices, negative testing, evidence completeness and explicit claim controls. A³O certification terminology shall identify the exact profile and shall not imply external SAE endorsement.

A3O-5900 Architecture Metrics

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the canonical metrics framework for measuring architecture quality, maturity, compliance and operational effectiveness.

2. Scope

Applies to all architecture domains, specifications, implementations and certified solutions.

3. Metric Principles

Metrics SHALL be objective, repeatable, comparable and traceable.

4. Canonical Metrics Catalog

5. Normative Requirements

AMR-001 Every metric SHALL have a canonical definition.
AMR-002 Metric calculations SHALL be reproducible.
AMR-003 Metrics SHALL reference canonical identifiers.
AMR-004 Metric collection SHALL preserve traceability.

AMR-005 Metrics SHALL support governance decisions.
AMR-006 Historical metric values SHALL be retained.
AMR-007 Metric thresholds SHALL be governed.
AMR-008 Metric reporting SHALL be auditable.
AMR-009 Metric models SHALL remain technology independent.
AMR-010 Certified implementations SHALL publish applicable architecture metrics.

6. Architecture Maturity Levels

Level M0 – Initial
Level M1 – Managed
Level M2 – Defined
Level M3 – Measured
Level M4 – Optimized

7. Conformance

Conforming organizations SHALL collect, maintain and report architecture metrics according to this specification.

A3O-6000 Autonomous Governance & Self-Evolving Systems

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance & Self-Evolving Systems source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000_Autonomous_Governance_PartA_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartA R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part A — Autonomous Governance Framework

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Governance Framework enabling evidence-driven, policy-governed, adaptive and self-improving operation of A3O ecosystems while maintaining human oversight where required.

2. Autonomous Governance Principles

AGF-001 Governance decisions SHALL be evidence-driven.
AGF-002 Policies SHALL be machine-interpretable and versioned.
AGF-003 Autonomous actions SHALL remain fully explainable and traceable.
AGF-004 Human oversight SHALL be configurable according to governance policy.
AGF-005 Autonomous Governance SHALL remain implementation independent.

3. Canonical Governance Components

4. Governance Constraints

AGG-001 Every autonomous governance policy SHALL have a canonical identifier and version.
AGG-002 Every autonomous decision SHALL generate immutable evidence.
AGG-003 Policy evolution SHALL be governed and auditable.
AGG-004 Explainability SHALL be available for autonomous governance actions.
AGG-005 Federated governance SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support governed policy execution, explainable autonomous decisions, continuous compliance verification and complete end-to-end traceability.

A3O-6000_Autonomous_Governance_PartB_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartB R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part B — Autonomous Decision Architecture

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Decision Architecture governing evidence-driven decision making, closed-loop control, explainability, validation, risk-aware execution and adaptive optimization across the A3O ecosystem.

2. Autonomous Decision Principles

ADA-001 Decisions SHALL be evidence-driven.

ADA-002 Every autonomous decision SHALL be explainable and reproducible.

ADA-003 Decision confidence SHALL be quantified before execution.

ADA-004 Risk SHALL be evaluated continuously throughout the decision lifecycle.

ADA-005 Decision Architecture SHALL remain implementation independent.

3. Canonical Decision Components

4. Governance Constraints

ADG-001 Every autonomous decision SHALL have a canonical identifier.

ADG-002 Decision evidence SHALL be immutable and auditable.

ADG-003 High-impact decisions SHALL follow configured oversight policies.

ADG-004 Decision models SHALL be versioned and continuously validated.

ADG-005 Federated decision systems SHALL preserve semantic and policy consistency.

5. Conformance

Conforming implementations SHALL support explainable autonomous decisions, continuous validation, governed execution, closed-loop feedback and complete decision traceability.

A3O-6000_Autonomous_Governance_PartC_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartC R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part C — Self-Evolving Architecture

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Self-Evolving Architecture enabling the A3O ecosystem to assess itself, identify improvement opportunities, evolve architecture baselines safely, and continuously optimize capabilities using governed evidence-driven feedback loops.

2. Self-Evolution Principles

SEA-001 Architecture evolution SHALL be evidence-driven.

SEA-002 Evolution SHALL preserve architectural integrity and semantic consistency.

SEA-003 Every architectural adaptation SHALL be explainable and reversible.

SEA-004 Evolution SHALL operate within governed policy boundaries.

SEA-005 Self-Evolving Architecture SHALL remain implementation independent.

3. Canonical Self-Evolution Components

4. Governance Constraints

SEG-6000-001 Every evolution proposal SHALL have a canonical identifier.

SEG-6000-002 Evolution SHALL be validated before deployment.

SEG-6000-003 Every baseline change SHALL generate immutable evidence.

SEG-6000-004 Unsafe evolution SHALL be automatically halted or rolled back.

SEG-6000-005 Federated evolution SHALL preserve interoperability, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support governed self-evolution, architecture optimization, simulation, rollback, continuous learning and complete lifecycle traceability.

A3O-6000_Autonomous_Governance_PartD_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartD R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part D — Adaptive Policy Intelligence

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Adaptive Policy Intelligence Architecture enabling executable governance policies to learn from evidence, adapt within approved constraints, optimize decision quality and maintain continuous compliance.

2. Adaptive Policy Principles

API-001 Policies SHALL be machine-interpretable and executable.

API-002 Policy adaptation SHALL be evidence-driven.

API-003 Policy optimization SHALL preserve governance constraints.

API-004 Every policy change SHALL be explainable, versioned and auditable.

API-005 Adaptive Policy Intelligence SHALL remain implementation independent.

3. Canonical Adaptive Policy Components

4. Governance Constraints

APG-001 Every executable policy SHALL have a canonical identifier and version.

APG-002 Adaptive policy changes SHALL require automated validation before activation.

APG-003 Policy evolution SHALL generate immutable evidence.

APG-004 Unsafe policy adaptations SHALL be automatically rejected or rolled back.

APG-005 Federated policy intelligence SHALL preserve semantic, identity and governance consistency.

5. Conformance

Conforming implementations SHALL support executable adaptive policies, evidence-driven optimization, continuous compliance validation, safe policy evolution and complete end-to-end traceability.

A3O-6000_Autonomous_Governance_PartE_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartE R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part E — Autonomous Knowledge Evolution

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Knowledge Evolution Architecture enabling continuous acquisition, validation, refinement, federation and lifecycle governance of knowledge assets used by A3O autonomous systems.

2. Knowledge Evolution Principles

AKE-001 Knowledge evolution SHALL be evidence-driven.

AKE-002 New knowledge SHALL be validated before operational use.

AKE-003 Knowledge provenance SHALL be complete and immutable.

AKE-004 Knowledge evolution SHALL preserve semantic consistency.

AKE-005 Knowledge Architecture SHALL remain implementation independent.

3. Canonical Knowledge Evolution Components

4. Governance Constraints

AKG-001 Every knowledge asset SHALL have a canonical identifier and version.

AKG-002 Knowledge provenance SHALL be recorded and auditable.

AKG-003 Knowledge promotion SHALL require automated validation.

AKG-004 Invalid or conflicting knowledge SHALL be quarantined until resolved.

AKG-005 Federated knowledge evolution SHALL preserve semantic and policy consistency.

5. Conformance

Conforming implementations SHALL support governed knowledge evolution, evidence-based validation, semantic consistency, federated synchronization and complete lifecycle traceability.

A3O-6000_Autonomous_Governance_PartF_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartF R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part F — Autonomous Multi-Agent Governance

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Multi-Agent Governance Architecture governing coordination, delegation, collaboration, conflict resolution, trust and collective decision-making among autonomous agents operating within A3O ecosystems.

2. Multi-Agent Governance Principles

AMG-001 Autonomous agents SHALL operate under governed roles and authorities.

AMG-002 Agent collaboration SHALL be evidence-driven and policy-aware.

AMG-003 Collective decisions SHALL be explainable, auditable and reproducible.

AMG-004 Trust between agents SHALL be continuously evaluated.

AMG-005 Multi-Agent Governance SHALL remain implementation independent.

3. Canonical Multi-Agent Components

4. Governance Constraints

AMGG-001 Every autonomous agent SHALL have a canonical identity.

AMGG-002 Delegation chains SHALL be fully traceable.

AMGG-003 Collective decisions SHALL generate immutable evidence.

AMGG-004 Agent conflicts SHALL be resolved according to governed policies.

AMGG-005 Federated agent ecosystems SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support governed multi-agent collaboration, trusted delegation, collective decision-making, conflict resolution and complete end-to-end traceability.

A3O-6000_Autonomous_Governance_PartG_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartG R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part G — Autonomous Resilience & Recovery

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Resilience & Recovery Architecture governing autonomous detection, prediction, containment, recovery and continuous resilience improvement across A3O ecosystems.

2. Resilience Principles

ARR-001 Resilience SHALL be proactive and evidence-driven.

ARR-002 Failures SHALL be detected and classified autonomously.

ARR-003 Recovery actions SHALL be policy-governed and explainable.

ARR-004 System learning SHALL continuously improve resilience.

ARR-005 Resilience Architecture SHALL remain implementation independent.

3. Canonical Resilience Components

4. Governance Constraints

ARG-001 Every resilience event SHALL have a canonical identifier.

ARG-002 Recovery actions SHALL generate immutable evidence.

ARG-003 Autonomous recovery SHALL comply with approved governance policies.

ARG-004 Failed recovery SHALL trigger escalation according to governance rules.

ARG-005 Federated resilience SHALL preserve interoperability, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support autonomous resilience, governed recovery, continuous learning, explainable recovery actions and complete lifecycle traceability.

A3O-6000_Autonomous_Governance_PartH_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartH R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part H — Autonomous Trust, Ethics & Assurance

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Trust, Ethics & Assurance Architecture governing trustworthy autonomous behavior, ethical constraints, assurance, accountability and continuous verification for self-governing A3O ecosystems.

2. Trust, Ethics & Assurance Principles

ATE-001 Autonomous behavior SHALL be trustworthy, explainable and verifiable.

ATE-002 Ethical constraints SHALL be executable and continuously enforced.

ATE-003 Assurance SHALL be evidence-driven throughout the system lifecycle.

ATE-004 Accountability SHALL be preserved for every autonomous action.

ATE-005 Trust, Ethics & Assurance Architecture SHALL remain implementation independent.

3. Canonical Trust & Assurance Components

4. Governance Constraints

ATEG-001 Every trust policy SHALL have a canonical identifier and version.

ATEG-002 Every autonomous action SHALL generate immutable accountability evidence.

ATEG-003 Ethical policy violations SHALL trigger governed mitigation workflows.

ATEG-004 Assurance assessments SHALL be continuously validated.

ATEG-005 Federated trust ecosystems SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support governed trust evaluation, executable ethics, continuous assurance, accountable autonomous behavior and complete end-to-end traceability.

A3O-6000_Autonomous_Governance_PartI_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartI R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part I — Autonomous Ecosystem Orchestration

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Ecosystem Orchestration Architecture governing coordinated operation, resource optimization, goal alignment, federation and lifecycle orchestration across the complete A3O autonomous ecosystem.

2. Ecosystem Orchestration Principles

AEO-001 Ecosystem orchestration SHALL align all autonomous subsystems with strategic objectives.

AEO-002 Resource allocation SHALL be evidence-driven and continuously optimized.

AEO-003 Global objectives SHALL be decomposed into governed executable missions.

AEO-004 Orchestration decisions SHALL be explainable, auditable and reversible.

AEO-005 Ecosystem Orchestration SHALL remain implementation independent.

3. Canonical Orchestration Components

4. Governance Constraints

AEOG-001 Every orchestration plan SHALL have a canonical identifier and version.

AEOG-002 Strategic objective changes SHALL be governed and traceable.

AEOG-003 Resource allocation decisions SHALL generate immutable evidence.

AEOG-004 Unsafe orchestration actions SHALL be automatically blocked or rolled back.

AEOG-005 Federated orchestration SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support governed ecosystem orchestration, strategic goal alignment, adaptive resource optimization, synchronized evolution and complete end-to-end traceability.

A3O-6000_Autonomous_Governance_PartJ_R0.1

GOVERNED LEARNING OVERLAY

This A3O-6000 Autonomous Governance PartJ R0.1 source artifact is extended so learning and adaptation cannot silently modify JAUS service contracts, semantic mappings, authority, safety envelopes or conformance profiles. Model and rule changes require validation, rollback and runtime provenance.

A3O-6000 Autonomous Governance & Self-Evolving Systems
Part J — Autonomous Civilizational Governance & Continuous Evolution

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Autonomous Civilizational Governance & Continuous Evolution Architecture providing the highest governance layer for A3O. It coordinates long-term autonomous evolution, strategic adaptation, ecosystem sustainability, knowledge continuity, and responsible governance across globally distributed, federated autonomous systems.

2. Civilizational Governance Principles

ACG-001 Long-term evolution SHALL preserve mission, values and governance intent.

ACG-002 Strategic adaptation SHALL be evidence-driven and continuously evaluated.

ACG-003 Civilizational knowledge SHALL be preserved, validated and transferable.

ACG-004 Autonomous evolution SHALL remain bounded by executable governance policies.

ACG-005 Civilizational Governance Architecture SHALL remain implementation independent.

3. Canonical Civilizational Components

4. Governance Constraints

ACGG-001 Every strategic governance baseline SHALL have a canonical identifier and version.

ACGG-002 Long-term evolution SHALL generate immutable evidence.

ACGG-003 Foundational governance policies SHALL remain continuously verifiable.

ACGG-004 Strategic evolution SHALL support safe rollback where applicable.

ACGG-005 Federated autonomous civilizations SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming implementations SHALL support autonomous strategic governance, continuous civilizational evolution, sustainable knowledge preservation, responsible adaptation and complete end-to-end governance traceability.

A3O Master Architecture Baseline R0.1 (Merged v3)

This consolidated edition appends the complete A3O-7000 Autonomous Civilization Platform & Global Ecosystem layer.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform & Global Ecosystem source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000_Autonomous_Civilization_Platform_PartA_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartA R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part A — Autonomous Civilization Platform Framework

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical platform architecture for globally federated autonomous ecosystems coordinating knowledge, governance, missions, infrastructure and civilization-scale services.

2. Principles

ACP-001 Platform governance SHALL be evidence-driven.

ACP-002 Platform services SHALL be reusable and composable.

ACP-003 Global interoperability SHALL be preserved.

ACP-004 Strategic objectives SHALL be continuously aligned.

ACP-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

ACPG-001 Every platform baseline SHALL have a canonical identifier.

ACPG-002 Strategic changes SHALL be governed.

ACPG-003 Platform evidence SHALL be immutable.

ACPG-004 Unsafe changes SHALL be rejected.

ACPG-005 Federation SHALL preserve semantic consistency.

5. Conformance

Conforming implementations shall support governed execution, evidence-driven operation, interoperability, resilience and complete lifecycle traceability.

Component	Responsibility	Primary Dependencies
Civilization Platform Core	Global platform foundation	A3O-6000
Global Service Fabric	Shared civilization services	Runtime

Mission Coordination Layer	Global mission execution	Mission Architecture
Knowledge Fabric	Global knowledge integration	Knowledge Graph
Policy Fabric	Platform-wide policy execution	Adaptive Policy Intelligence
Federation Hub	Cross-ecosystem federation	Integration
Observability Grid	Global monitoring	Observability
Platform Repository	Platform baselines	Information Architecture

A3O-7000_Autonomous_Civilization_Platform_PartB_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartB R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part B — Global Autonomous Ecosystems

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture for globally distributed autonomous ecosystems cooperating through federated governance, shared knowledge and coordinated execution.

2. Principles

GAE-001 Ecosystems SHALL cooperate through governed federation.

GAE-002 Shared knowledge SHALL remain semantically consistent.

GAE-003 Cross-ecosystem coordination SHALL be evidence-driven.

GAE-004 Resource sharing SHALL be policy-controlled.

GAE-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

GAEG-001 Every ecosystem SHALL have a canonical identifier.

GAEG-002 Federation SHALL be auditable.

GAEG-003 Knowledge exchange SHALL generate evidence.

GAEG-004 Cross-domain policies SHALL be validated.

GAEG-005 Global consistency SHALL be preserved.

5. Conformance

Conforming implementations shall support governed execution, evidence-driven operation, interoperability, resilience and complete lifecycle traceability.

Component	Responsibility	Primary Dependencies
Ecosystem Coordinator	Coordinate ecosystems	Platform Framework
Federation Gateway	Inter-ecosystem connectivity	Integration
Global Knowledge Exchange	Knowledge synchronization	Knowledge Evolution
Resource Exchange Engine	Shared resources	Runtime
Trust Federation	Cross-ecosystem trust	Trust & Assurance
Mission Exchange	Mission coordination	Mission Architecture
Global Policy Broker	Policy synchronization	Adaptive Policy
Ecosystem Repository	Store ecosystem baselines	Information Architecture

A3O-7000_Autonomous_Civilization_Platform_PartC_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartC R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part C — Planetary Digital Twin & Global Knowledge Fabric

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture for a planetary-scale digital twin integrated with a global knowledge fabric supporting simulation, prediction and coordinated decision-making.

2. Principles

PDT-001 Planetary models SHALL be evidence-driven.

PDT-002 Digital twins SHALL synchronize continuously.

PDT-003 Knowledge SHALL preserve provenance and semantics.

PDT-004 Simulations SHALL be reproducible and explainable.

PDT-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

PDTG-001 Every twin SHALL have a canonical identifier.

PDTG-002 Synchronization SHALL be auditable.

PDTG-003 Models SHALL be versioned.

PDTG-004 Invalid state updates SHALL be rejected.

PDTG-005 Knowledge provenance SHALL be preserved.

5. Conformance

Conforming implementations shall provide governed operation, continuous optimization, evidence-based control and full traceability.

Component	Responsibility	Primary Dependencies
Planetary Twin Core	Global digital twin	Digital Twin
Global Knowledge Fabric	Unified knowledge layer	Knowledge Graph
Simulation Engine	Scenario modelling	AI
Earth State Repository	Planetary state history	Information
Sensor Federation	Global sensing	Integration
Prediction Engine	Forecast evolution	AI
Semantic Harmonizer	Semantic consistency	Semantic
Twin Repository	Twin baselines	Information

A3O-7000_Autonomous_Civilization_Platform_PartD_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartD R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part D — Autonomous Economy & Resource Governance

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture governing autonomous allocation of resources, economic optimization, sustainability and value exchange across global autonomous ecosystems.

2. Principles

AER-001 Resource allocation SHALL be evidence-driven.

AER-002 Sustainability SHALL guide optimization.

AER-003 Economic policies SHALL be executable.

AER-004 Value exchange SHALL be transparent and auditable.

AER-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

AERG-001 Every governed resource SHALL have a canonical identifier.

AERG-002 Allocation decisions SHALL generate immutable evidence.

AERG-003 Policies SHALL be continuously validated.

AERG-004 Resource conflicts SHALL be governed.

AERG-005 Federated resource governance SHALL preserve consistency.

5. Conformance

Conforming implementations shall provide governed operation, continuous optimization, evidence-based control and full traceability.

Component	Responsibility	Primary Dependencies
Resource Governance Engine	Allocate shared resources	Governance
Economic Optimization Engine	Optimize value	AI
Sustainability Analyzer	Evaluate sustainability	Analytics
Value Exchange Hub	Coordinate exchanges	Integration
Resource Ledger	Track assets	Information
Policy Pricing Service	Govern incentives	Policy
Forecast Engine	Predict demand	AI
Economic Repository	Store economic baselines	Information

A3O-7000_Autonomous_Civilization_Platform_PartE_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartE R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part E — Collective Intelligence & Swarm Cognition

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture for collective intelligence, distributed cognition and swarm coordination enabling large populations of autonomous agents to solve complex global problems cooperatively.

2. Principles

CIS-001 Collective intelligence SHALL emerge through governed collaboration.

CIS-002 Swarm behavior SHALL remain explainable and policy-constrained.

CIS-003 Shared reasoning SHALL be evidence-driven.

CIS-004 Collective learning SHALL continuously improve ecosystem performance.

CIS-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

CISG-001 Every swarm SHALL have a canonical identifier.

CISG-002 Consensus SHALL be auditable.

CISG-003 Collective knowledge SHALL preserve provenance.

CISG-004 Unsafe swarm behavior SHALL be automatically contained.

CISG-005 Federated swarms SHALL preserve semantic consistency.

5. Conformance

Conforming implementations shall support governed operation, evidence-driven optimization, explainable autonomy, interoperability and complete lifecycle traceability.

Component	Responsibility	Primary Dependencies
Swarm Coordination Engine	Coordinate large-scale agent collaboration	Multi-Agent Governance
Collective Reasoning Engine	Distributed reasoning	AI Architecture
Consensus Service	Reach governed consensus	Autonomous Decision
Collective Memory	Shared long-term knowledge	Knowledge Evolution
Swarm Learning Engine	Collective learning	AI
Trust Mesh	Distributed trust	Trust & Assurance
Collective Goal Manager	Align swarm objectives	Mission Architecture
Swarm Repository	Store swarm baselines	Information Architecture

A3O-7000_Autonomous_Civilization_Platform_PartF_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartF R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part F — Autonomous Scientific Discovery & Innovation

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture for autonomous scientific discovery, hypothesis generation, experimentation, validation and innovation lifecycle management across the A3O ecosystem.

2. Principles

ASI-001 Scientific discovery SHALL be evidence-driven.

ASI-002 Hypotheses SHALL be reproducible and traceable.

ASI-003 Innovation SHALL be continuously validated.

ASI-004 Scientific knowledge SHALL preserve provenance.

ASI-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

ASIG-001 Every discovery SHALL have a canonical identifier.

ASIG-002 Experimental evidence SHALL be immutable.

ASIG-003 Scientific baselines SHALL be versioned.

ASIG-004 Invalid hypotheses SHALL remain traceable.

ASIG-005 Federated research SHALL preserve semantic consistency.

5. Conformance

Conforming implementations shall support governed operation, evidence-driven optimization, explainable autonomy, interoperability and complete lifecycle traceability.

Component	Responsibility	Primary Dependencies
Discovery Engine	Generate hypotheses	AI Architecture
Experiment Orchestrator	Coordinate experiments	Mission Architecture
Evidence Validation Lab	Validate findings	Evidence Services
Innovation Knowledge Base	Manage discoveries	Knowledge Graph
Simulation Laboratory	Virtual experimentation	Digital Twin
Research Collaboration Hub	Coordinate researchers and agents	Multi-Agent Governance
Innovation Portfolio Manager	Govern innovation pipeline	Governance
Scientific Repository	Store validated knowledge	Information Architecture

A3O-7000_Autonomous_Civilization_Platform_PartG_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartG R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part G — Interoperable Civilization Networks

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture for interoperable civilization-scale networks enabling trusted communication, knowledge exchange and coordinated execution across autonomous ecosystems.

2. Principles

ICN-001 Networks SHALL be policy-governed.

ICN-002 Interoperability SHALL preserve semantics.

ICN-003 Exchanges SHALL be evidence-driven.

ICN-004 Trust SHALL be continuously verified.

ICN-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

ICNG-001 Every network SHALL have a canonical identifier.

ICNG-002 Exchanges SHALL be auditable.

ICNG-003 Policies SHALL be validated.

ICNG-004 Unsafe exchanges SHALL be blocked.

ICNG-005 Semantic consistency SHALL be preserved.

5. Conformance

Conforming implementations shall provide governed interoperability, evidence-based adaptation, resilience and full lifecycle traceability.

Component	Responsibility	Primary Dependencies
Civilization Network Core	Global networking	Platform
Interoperability Gateway	Cross-network exchange	Integration
Semantic Translation Engine	Semantic interoperability	Knowledge
Trust Exchange Service	Distributed trust	Trust
Mission Routing Fabric	Mission routing	Mission
Identity Federation	Cross-network identity	Security
Network Observatory	Global monitoring	Observability
Network Repository	Network baselines	Information

A3O-7000_Autonomous_Civilization_Platform_PartH_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartH R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part H — Long-Term Sustainability & Resilience

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture governing long-term sustainability, resilience, adaptive capacity and continuity of autonomous civilization-scale ecosystems.

2. Principles

LSR-001 Sustainability SHALL be continuously optimized.

LSR-002 Resilience SHALL be proactive.

LSR-003 Adaptation SHALL be evidence-driven.

LSR-004 Continuity SHALL preserve strategic intent.

LSR-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

LSRG-001 Every sustainability baseline SHALL have a canonical identifier.

LSRG-002 Long-term metrics SHALL be auditable.

LSRG-003 Adaptations SHALL generate immutable evidence.

LSRG-004 Critical degradation SHALL trigger governed response.

LSRG-005 Federated sustainability SHALL preserve policy consistency.

5. Conformance

Conforming implementations shall provide governed interoperability, evidence-based adaptation, resilience and full lifecycle traceability.

Component	Responsibility	Primary Dependencies
Sustainability Engine	Optimize sustainability	Analytics
Continuity Manager	Ensure long-term continuity	Governance
Resilience Coordinator	Coordinate resilience	A3O-6000
Impact Assessment Service	Evaluate long-term impact	Digital Twin
Resource Renewal Manager	Renew critical resources	Economy
Strategic Health Monitor	Monitor ecosystem health	Observability
Adaptive Planning Engine	Long-term planning	AI
Sustainability Repository	Store sustainability baselines	Information

A3O-7000_Autonomous_Civilization_Platform_PartI_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartI R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part I — Cross-Civilization Coordination

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture governing coordination, negotiation, interoperability and strategic synchronization among multiple autonomous civilizations, federations and global ecosystems.

2. Principles

CCC-001 Cross-civilization coordination SHALL be policy-governed.

CCC-002 Strategic synchronization SHALL be evidence-driven.

CCC-003 Negotiation SHALL be transparent and auditable.

CCC-004 Shared objectives SHALL preserve federation autonomy.

CCC-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

CCCG-001 Every coordination agreement SHALL have a canonical identifier.

CCCG-002 Negotiation outcomes SHALL generate immutable evidence.

CCCG-003 Strategic conflicts SHALL follow governed resolution policies.

CCCG-004 Federation autonomy SHALL be preserved.

CCCG-005 Semantic consistency SHALL be maintained across civilizations.

5. Conformance

Conforming implementations shall support governed coordination, adaptive governance, evidence-based optimization and complete end-to-end traceability.

Component	Responsibility	Primary Dependencies
Civilization Coordination Engine	Coordinate global civilizations	Platform Framework
Negotiation Service	Govern cross-civilization agreements	Autonomous Decision
Strategic Alignment Manager	Align long-term objectives	Mission Architecture
Federation Synchronizer	Synchronize federations	Global Ecosystems
Conflict Mediation Engine	Resolve strategic conflicts	Adaptive Policy Intelligence
Shared Knowledge Exchange	Exchange validated knowledge	Knowledge Evolution
Global Coordination Observatory	Monitor coordination status	Observability
Coordination Repository	Store agreements and evidence	Information Architecture

A3O-7000_Autonomous_Civilization_Platform_PartJ_R0.1

FEDERATION OVERLAY

This A3O-7000 Autonomous Civilization Platform PartJ R0.1 source artifact is extended by federated JAUS identity scoping. Local subsystem/node/component addresses are bound beneath organization and ecosystem identities so independent address spaces can interoperate without collision or inherited authority.

A3O-7000 Autonomous Civilization Platform & Global Ecosystem
Part J — Universal Adaptive Governance

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical Universal Adaptive Governance Architecture providing the highest governance layer for globally federated autonomous civilizations through adaptive policy, strategic evolution and universal interoperability.

2. Principles

UAG-001 Universal governance SHALL be evidence-driven.

UAG-002 Governance adaptation SHALL preserve foundational principles.

UAG-003 Universal interoperability SHALL be continuously maintained.

UAG-004 Strategic evolution SHALL remain explainable and auditable.

UAG-005 Architecture SHALL remain implementation independent.

3. Canonical Components

4. Governance Constraints

UAGG-001 Every universal governance baseline SHALL have a canonical identifier.

UAGG-002 Universal policy evolution SHALL generate immutable evidence.

UAGG-003 Strategic adaptation SHALL remain continuously verifiable.

UAGG-004 Unsafe governance evolution SHALL be automatically rejected.

UAGG-005 Universal governance SHALL preserve semantic, identity and policy consistency.

5. Conformance

Conforming implementations shall support governed coordination, adaptive governance, evidence-based optimization and complete end-to-end traceability.

Component	Responsibility	Primary Dependencies
Universal Governance Core	Highest governance authority	A3O-6000
Adaptive Strategy Engine	Optimize global strategy	Self-Evolving Architecture
Universal Policy Fabric	Global executable governance	Adaptive Policy Intelligence
Inter-Civilization Trust Authority	Global trust governance	Trust & Assurance
Universal Knowledge Nexus	Civilizational knowledge integration	Knowledge Fabric
Strategic Evolution Observatory	Monitor universal evolution	Observability
Governance Baseline Authority	Maintain master baselines	Information Architecture
Universal Repository	Store governance evidence and history	Information Architecture

A3O-8000 Interplanetary Autonomous Systems
Part B — Space & Multi-Orbital Infrastructure Ecosystems

CONTESTED OPERATIONS OVERLAY

This A3O-8000 Interplanetary Autonomous SystemsPart B — Space & Multi-Orbital Infrastructure Ecosystems source artifact is extended by threats including spoofed components, malicious discovery, service downgrade, Access Control abuse, replay, event exhaustion, mapping poisoning and evidence withholding. Degraded operation remains bounded, observable, reversible and testable.

Release: R0.1 Working Draft
Status: Initial Baseline

1. Purpose

Defines the canonical architecture governing orbital stations, satellites, transport infrastructure and distributed autonomous space assets.

2. Principles

- SMO-001 Orbital infrastructure SHALL be federated.
- SMO-002 Critical assets SHALL be continuously monitored.
- SMO-003 Resource sharing SHALL be policy-governed.
- SMO-004 Orbital operations SHALL be resilient.
- SMO-005 Architecture SHALL remain implementation independent.

3. Canonical Components

Component	Responsibility	Primary Dependencies
Orbital Infrastructure Hub	Coordinate orbital assets	Interplanetary Framework
Space Asset Registry	Track infrastructure	Information
Orbital Logistics Engine	Manage transport	Runtime
Autonomous Docking Service	Coordinate docking	Mission
Space Resource Exchange	Resource governance	Economy
Orbital Trust Fabric	Secure cooperation	Trust
Space Operations Center	Monitor ecosystem	Observability
Orbital Repository	Store baselines	Information

4. Governance Constraints

- SMOG-001 Every orbital asset SHALL have a canonical identifier.
- SMOG-002 Infrastructure events SHALL generate immutable evidence.
- SMOG-003 Shared resources SHALL be auditable.
- SMOG-004 Safety policies SHALL be enforced.
- SMOG-005 Federation SHALL preserve interoperability.

5. Conformance

Conforming implementations shall support autonomous operation, federated governance, evidence-driven adaptation and complete lifecycle traceability.

A3O-9000_Annexes_R0.1.docx

ANNEX AND SDK OVERLAY

This A3O-9000 Annexes R0.1 source artifact is extended by the controlled JSIDL Registry, generated codecs, mapping registry, reference components, simulator, conformance suites and reproducible release manifests. Licensed source artifacts and permitted-use records are retained.

A3O-9000 Annexes

Release: R0.1 Working Draft
Status: Draft Specification

1. Purpose

Defines the normative and informative annexes supporting the A3O Architecture Baseline.

2. Scope

Applies to all baseline releases and associated architecture specifications.

3. Annex Principles

Annexes SHALL complement, but SHALL NOT redefine, normative architecture requirements.

4. Annex Catalog

5. Normative Requirements

ANR-001 Every baseline release SHALL include a glossary.
ANR-002 Annexes SHALL use canonical identifiers.
ANR-003 Normative references SHALL be versioned.
ANR-004 Templates SHALL be governed.
ANR-005 Traceability matrices SHALL be maintained.
ANR-006 Change history SHALL be immutable.
ANR-007 Release notes SHALL identify baseline changes.
ANR-008 Annexes SHALL preserve consistency with the Meta Model.

ANR-009 Informative annexes SHALL be clearly distinguished from normative content.

ANR-010 Annexes SHALL support audit and long-term maintenance.

6. Conformance

A conforming A3O baseline SHALL include all mandatory annexes applicable to the released specification set.

ANNEX

Annex A — Normative Requirement Catalogue

This annex consolidates 170 JAUS-integration requirements introduced by R1.2. Requirements are architecture-level and require allocation to implementation components and test cases before a conformance claim is made.

irement ID	Normative statement
001	A³O SHALL implement JAUS integration through a bounded JAUS Interoperability Domain.
002	A³O SHALL preserve original JAUS source and destination identities.
003	A³O SHALL bind protocol-local JAUS addresses to persistent A³O identities before operational admission.
004	Discovery SHALL NOT automatically establish trust, ownership, safety or authority.
005	Every operational service SHALL reference its exact service definition, version and provenance.
006	Custom A³O services SHALL use namespaces distinguishable from SAE-standard services.
007	Compatibility claims SHALL identify the profile, version, test scope and evidence basis.
008	A³O SHALL NOT imply SAE certification or endorsement without explicit evidence and authorization.
009	Architecture decisions selecting services or mappings SHALL be recorded and traceable.
010	Retired address bindings and service versions SHALL remain reproducible for evidence and replay.
011	Unknown ownership or identity SHALL cause operational quarantine.
012	A protocol adapter SHALL NOT expand authority.
013	Licensed standards and data artifacts SHALL be governed through a use-rights record.
014	Service-definition and code-generation toolchains SHALL be reproducible.
015	The architecture SHALL support JAUS and non-JAUS endpoints under one governance model.
201	Every JAUS-to-A³O mapping SHALL be versioned and auditable.
202	Mappings SHALL identify source field, source unit, source frame, target field and validity conditions.
203	Ambiguous coordinate frames SHALL fail closed for control use.
204	Source values and units SHALL remain available in evidence after normalization.
205	Source, receive and transformation timestamps SHALL remain distinguishable.
206	Uncertainty, validity, quality and staleness SHALL be represented explicitly.
207	Simulation, training, forecast, replay and live data SHALL remain distinguishable.
208	Semantic loss or approximation SHALL be declared.
209	Reverse encoding SHALL be allowed only when the mapping is complete and validated.
210	Industry ontology extensions SHALL declare ownership, privacy and safety relevance.
301	A³O SHALL retain the unmodified received control-relevant message or a content-addressable equivalent.
302	Every decoded message SHALL reference the decoder and JSD version used.
303	Every canonical state delta SHALL reference its source message or derivation inputs.
304	Stale or invalid messages SHALL NOT update authoritative state.
305	Outgoing commands SHALL reference the originating mission intent and authority context.
306	Command results SHALL be correlated with resulting reports, state or timeout.
307	Evidence SHALL identify mapping, policy, safety and authority decisions.
308	Raw evidence and normalized state SHALL be separable by access policy without losing correlation.
309	Duplicate and replayed messages SHALL be detected and recorded.
310	Malformed messages SHALL be rejected, rate-limited and evidenced.

irement ID	Normative statement
311	Unsupported service versions SHALL fail closed.
312	Event loss and subscription failure SHALL be observable.
313	Data-retention policies SHALL distinguish control, state, diagnostics and bulk media.
314	Evidence integrity SHALL be verifiable independently of the operational database.
401	Capability contracts SHALL remain independent of vendor-specific APIs.
402	An applicable standard JAUS service SHOULD be preferred when semantics match.
403	Service composition SHALL declare authority and failure behavior.
404	A^{3}O extensions SHALL be separately named and versioned.
405	Non-JAUS adapters SHALL expose the same canonical capability and evidence obligations.
406	Every profile SHALL declare mandatory and optional services and versions.
407	Every profile SHALL declare safety, privacy and operational-domain constraints.
408	A capability realization SHALL include conformance tests.
409	A profile change SHALL undergo architecture review and regression.
410	A profile SHALL declare degraded and communications-loss behavior.
001	External JAUS traffic SHALL terminate at the JAUS Interoperability Domain.
002	Transport handling and semantic transformation SHALL be separable components.
003	Decoding SHALL require an approved service definition and compatible version.
004	Canonical state SHALL not directly confer action authority.
005	UI and AI components SHALL not bypass the command authorization path.
006	Trust boundaries SHALL be documented and tested.
007	Deployment patterns SHALL identify where control, state, policy and evidence execute.
008	Cloud loss SHALL not silently change the permitted autonomy level.
009	Federated exchange SHALL preserve organization and ecosystem identity scopes.
010	High-assurance deployments SHALL mediate external integrations.
011	A^{3}O SHALL support partition-tolerant operation with bounded delegated authority.
012	All architecture layers SHALL expose health and evidence-relevant metrics.
101	The Transport Gateway SHALL record transport identity, timestamps and failure state.
102	The JSIDL Registry SHALL reject unresolved dependencies and incompatible definitions.
103	The Discovery Bridge SHALL create candidate capabilities only.
104	The Identity Binder SHALL maintain revocation and lifecycle state.
105	The Access Control Broker SHALL coordinate A^{3}O authority and JAUS ownership.
106	The Management Bridge SHALL reject invalid lifecycle transitions.
107	The Event Bridge SHALL enforce rate and subscription quotas.
108	The Telemetry Normalizer SHALL not issue commands.
109	The Command Encoder SHALL reject ambiguous service or mapping selection.

irement ID	Normative statement
110	The Evidence Correlator SHALL link raw inputs through outcomes.
111	Delegated authority SHALL include scope, duration and revocation conditions.

irement ID	Normative statement
112	Partition actions SHALL be reconciled after recovery.
113	Conflicts SHALL be retained until resolved.
114	Runtime queues and backlogs SHALL be monitored.
115	Latency and freshness budgets SHALL be profile requirements.
301	AI components SHALL NOT directly transmit JAUS control messages.
302	AI outputs SHALL identify model, version, inputs, confidence and provenance.
303	AI recommendations SHALL pass policy, safety and authority validation.
304	A model update SHALL NOT expand authority or autonomy level.
305	Training and live data SHALL remain separated.
306	Model rollback SHALL be supported for operational deployments.
307	AI performance drift SHALL be monitored.
308	Learning datasets SHALL preserve protocol and mapping provenance.
001	A JAUS-addressable A^{3}O component SHALL have a defined lifecycle and service contract.
002	Component discovery metadata SHALL be validated before admission.
003	Component responsibilities and hard boundaries SHALL be documented.
004	Transport Gateway SHALL not perform policy authorization.
005	JSIDL Registry SHALL not own operational authority.
006	Discovery Bridge SHALL not assign trust.
007	Identity Binder SHALL not accept conflicting ownership silently.
008	Access Control Broker SHALL not override local safety.
009	Management Bridge SHALL not force invalid transitions.
010	Event Bridge SHALL enforce resource limits.
011	Telemetry Normalizer SHALL preserve source provenance.
012	RadarTrackFusionComponent SHALL identify derived state and source observations.
013	A fused-track extension SHALL not be misrepresented as an SAE-standard service.
014	MissionOrchestratorBridge SHALL preserve platform-local execution constraints.
015	Command Encoder SHALL encode only approved action intent.
016	Evidence Recorder SHALL capture runtime evidence, not only post-hoc summaries.
017	Components SHALL expose health and diagnostics.
018	Components SHALL declare supported service versions.
019	Components SHALL support deterministic negative tests.
020	Component replacement SHALL preserve the declared capability contract.
001	Industry profiles SHALL reuse the universal A^{3}O trust and evidence model.

irement ID	Normative statement
002	Logistics profiles SHALL address custody, geofencing, energy and fleet deadlock.
003	Manufacturing profiles SHALL address interlocks, recipe integrity and production provenance.
004	Inspection profiles SHALL address coverage, frame integrity and sample provenance.
005	Medical profiles SHALL address privacy, identity, payload custody and human escalation.

irement ID	Normative statement
006	Security and defence profiles SHALL address positive control, spoofing and partition behavior.
007	DroneDefender SHALL be treated as a reference profile, not the A³O category definition.
008	Industry certification SHALL remain separate from JAUS interoperability.
009	Every profile SHALL define an operational design domain.
010	Every profile SHALL define failure and recovery scenarios.
011	Every profile SHALL define evidence retention and access.
012	Every profile SHALL include at least one end-to-end scenario test.
001	Conformance claims SHALL identify J0–J4 level and profile.
002	J1 SHALL require the applicable core integration tests.
003	J2 SHALL require selected application service-set tests.
004	J3 SHALL require identity, policy, safety, authority, state and evidence tests.
005	J4 SHALL require an approved partner profile suite.
006	External certification SHALL be stated separately.
007	Negative tests SHALL cover unknown, malformed, stale and replayed messages.
008	Access Control tests SHALL cover contention, preemption and expiry.
009	Transport tests SHALL cover loss, delay, duplication and recovery.
010	Event tests SHALL cover lifecycle, rate, loss and exhaustion.
011	Evidence tests SHALL verify raw-to-outcome completeness.
012	Performance metrics SHALL be part of acceptance.
013	Regression SHALL cover supported service and mapping versions.
014	Known limitations SHALL be published with the profile.
015	Claim language SHALL be reviewed before release.
001	Learning changes SHALL be architecture-controlled.
002	Models SHALL not change service contracts.
003	Models SHALL not change semantic mappings without approval.
004	Models SHALL not expand authority.
005	Models SHALL be evaluated against profile scenarios.
006	Model versions SHALL be correlated to operational evidence.
007	Data governance SHALL apply to federated learning.
008	Rollback SHALL be verified before production activation.
001	Federated JAUS addresses SHALL be scoped by organization and ecosystem identity.

irement ID	Normative statement
002	Federation SHALL not inherit authority from connectivity.
003	Schema and mapping versions SHALL be negotiated and recorded.
004	Participants SHALL exchange trust and policy metadata before operational data.
005	Raw data sharing SHALL be governed separately from state summaries.
006	Conflicts and evidence gaps SHALL remain visible.
007	Federated missions SHALL define ownership and escalation.

irement ID	Normative statement
008	Revoked identities SHALL propagate according to policy.
009	Federation termination behavior SHALL be testable.
001	The threat model SHALL include spoofed JAUS components.
002	The threat model SHALL include malicious discovery and false capability advertisement.
003	The threat model SHALL include version and mapping downgrade.
004	The threat model SHALL include Access Control abuse.
005	The threat model SHALL include replay and duplicate messages.
006	The threat model SHALL include event-subscription exhaustion.
007	The threat model SHALL include mapping poisoning.
008	The threat model SHALL include evidence withholding.
009	The threat model SHALL include topology manipulation.
010	Degraded modes SHALL remain bounded and observable.
011	Loss of trusted time SHALL trigger defined behavior.
012	Compromised nodes SHALL be isolatable.
001	The release SHALL include a machine-readable manifest.
002	The release SHALL include service-definition provenance.
003	The release SHALL include a supported-version matrix.
004	Generated codecs SHALL be reproducible.
005	Mapping registries SHALL be versioned.
006	Reference components SHALL include negative-test variants.
007	Conformance tests SHALL produce evidence packages.
008	The SDK SHALL expose policy-aware APIs rather than raw control bypasses.
009	The release SHALL include migration and rollback guidance.
010	License and SBOM records SHALL be retained.

ANNEX

Annex B — Standards Baseline and Bibliography

The references below were verified against public SAE Mobilus scope pages on 17 July 2026. The architecture baseline does not reproduce proprietary standard content. Implementation teams shall use licensed documents and associated data sets.

erence	Citation	DOI
5665C	SAE International, Architecture Framework for Unmanned Systems, Stabilized May 2024.	https://doi.org/10.4271/AIR5665C
669A	SAE International, JAUS / SDP Transport Specification, Reaffirmed April 2019.	https://doi.org/10.4271/AS5669A
684B	SAE International, JAUS Service Interface Definition Language, Reaffirmed April 2025.	https://doi.org/10.4271/AS5684B
710A	SAE International, JAUS Core Service Set, Reaffirmed April 2015.	https://doi.org/10.4271/AS5710A
009A	SAE International, JAUS Mobility Service Set, Revised October 2023.	https://doi.org/10.4271/AS6009A
057A	SAE International, JAUS Manipulator Service Set, Reaffirmed April 2025.	https://doi.org/10.4271/AS6057A
060A	SAE International, JAUS Environment Sensing Service Set, Reaffirmed May 2026.	https://doi.org/10.4271/AS6060A
062A	SAE International, JAUS Mission Spooling Service Set, Reaffirmed March 2024.	https://doi.org/10.4271/AS6062A
091	SAE International, JAUS Unmanned Ground Vehicle Service Set, Reaffirmed April 2025.	https://doi.org/10.4271/AS6091

erence	Citation	DOI
5111	SAE International, JAUS Unmanned Maritime Vehicle Service Set, Issued September 2023.	https://doi.org/10.4271/AS6111
8024	SAE International, JAUS Autonomous Capabilities Service Set, Reaffirmed April 2025.	https://doi.org/10.4271/AS8024
P6227	SAE International, JAUS Messaging over the OMG Data Distribution Service (DDS), Reaffirmed March 2024.	https://doi.org/10.4271/ARP6227

ANNEX

Annex C — Baseline Integrity Record

rtifact	Value
Source file	A3O_Master_Architecture_Baseline_R0.1_FULL_MASTER_STAGE1.docx
Source SHA-256	42ccd003941c434a29bae1360d01dc11e4043082f6e34e9b266ff3d33d2562c8
Source word count	17,199 words (paragraphs and tables)
Preservation method	Complete source body copied into Part II; R1.2 overlays inserted after source artifact headings.
Output status	Candidate; requires architecture review and licensed-standard implementation work.