A³O

WHITEPAPER

A³O: Universal Trusted Framework for Autonomous Ecosystems

FULL MASTER — JAUS Integrated

JAUS-integrated trust, interoperability, coordination and evidence for the autonomous world

DOCUMENT ID	A3O-WP-JAUS-1200
RELEASE	R1.2 FULL MASTER
STATUS	CANDIDATE · CONTROLLED REVIEW
LANGUAGE	ENGLISH MASTER
POSITIONING	UNIVERSAL TRUSTED FRAMEWORK
COMPATIBILITY	JAUS-ALIGNED TARGET ARCHITECTURE

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

RELEASE MANAGEMENT

Document Control and Release Governance

Field	Controlled value
Document identity	A3O-WP-JAUS-1200
Title	A^{3}O: Universal Trusted Framework for Autonomous Ecosystems — FULL MASTER, JAUS Integrated
Status	Candidate whitepaper for controlled strategic, technical and investment review
Architecture baseline	A3O-ARCH-JAUS-1200 · R1.2 FULL MASTER · CANDIDATE
Source preservation	All substantive content from A3O Whitepaper R1.0 Candidate is retained and traceable in Annex D.
Compatibility claim	JAUS-aligned target architecture and implementation profile; not a claim of SAE certification or endorsement.
Language	English master
Owner	A^{3}O Strategy and Systems Architecture
Review domains	Strategy, architecture, product, software, safety, security, market, finance, legal and standards licensing

STANDARDS AND LICENSING BOUNDARY

This whitepaper uses public SAE scope information to explain the target architecture and strategic value. Detailed wire formats, message fields, JSD artifacts, data sets and formal conformance criteria shall be implemented only from appropriately licensed SAE documents and associated data products.

Release objective. This document replaces the shortened R1.1 whitepaper concept with a full strategic and technical master. It preserves the universal A^{3}O positioning, integrates the R1.2 architecture baseline, explains the native JAUS Interoperability Domain, connects the technical model to cross-industry adoption and commercial strategy, and maintains disciplined language about compatibility, certification and market assumptions.

NAVIGATION

Controlled Structure

STRATEGIC FOUNDATION

1. Executive Thesis

Autonomous machines are moving from isolated products to operational ecosystems. Industrial robots, autonomous vehicles, drones, marine systems, medical and care robots, fixed sensors, software agents and human supervisors increasingly share the same mission, physical space, information environment and risk. The value of these systems no longer depends only on the performance of an individual machine. It depends on whether many machines, people and organizations can understand one another, act under bounded authority, continue safely when connectivity degrades and prove what happened after an action has affected the physical world.

The existing technology stack is fragmented at precisely those boundaries. Hardware vendors expose different APIs, service models, lifecycle states, coordinate systems and command semantics. Fleet managers usually govern one product family. Industrial platforms optimize a factory domain. command-and-control systems are often mission-specific. Cloud platforms collect data but do not necessarily control physical authority. AI systems can recommend or optimize actions, yet they rarely provide a complete chain from source observation through policy, authorization, execution and verified outcome. Integration therefore becomes a sequence of custom projects, and every additional platform creates another dependency.

A^3O — Adaptive Autonomous Operations Architecture — is designed to solve that systemic problem. It is a vendor-neutral trusted operating framework for heterogeneous autonomous ecosystems. A^3O provides a common layer for identity, semantic contracts, state, distributed coordination, policy-controlled autonomy, human authority, bounded execution, evidence and assurance. It sits above and between robots, vehicles, sensors, controllers, enterprise systems and mission applications. It does not require every endpoint to use the same internal operating system, autonomy stack or transport. Instead, it establishes the trusted contracts by which their capabilities become governable parts of a larger ecosystem.

The R1.2 architecture makes JAUS a native interoperability domain inside A^3O. JAUS contributes a platform-independent, component-based and service-oriented model for unmanned-system interaction. Its service definitions, addressing, discovery, management, access-control and message patterns provide a formal basis for connecting compatible components. A^3O preserves those semantics while adding the ecosystem functions that JAUS alone is not intended to provide: federated identity, organizational trust, cross-platform mission orchestration, human and delegated authority, policy enforcement, swarm coordination, digital-twin state, cross-protocol integration and evidence by design.

This relationship is central to the product thesis. A^3O is not a replacement for JAUS and is not a branded reimplementation of a single robotics protocol. It is the upper-level trust, coordination and assurance layer that makes JAUS — together with DDS, ROS, OPC UA, MQTT, REST, industrial buses and proprietary interfaces — usable at ecosystem scale. The architecture treats every protocol endpoint as a capability that must be identified, semantically understood, authorized, monitored and evidenced before it can participate in a governed mission.

The resulting category is broader than fleet management, robotics middleware or command-and-control. A^3O defines a Universal Trusted Framework for Autonomous Ecosystems: a reusable infrastructure layer through which organizations can coordinate any suitable machine, govern every mission and prove every material action. The same core applies to manufacturing, transportation and logistics, information collection and inspection, care and emergency response, and security and defence. Industry profiles specialize hazards, workflows, privacy, performance and compliance without fragmenting the underlying trust and orchestration model.

The commercial opportunity arises from replacing one-off integration with reusable capability profiles, adapters, conformance tests and operational assurance. A^3O reduces the cost of introducing a new platform, limits vendor lock-in, creates a stable control plane above changing hardware and enables evidence-based deployment in regulated or high-consequence environments. DroneDefender remains the first Security and Defence reference profile, demonstrating the governed loop from sensing to authorization, action and evidence, but it no longer defines the category or limits the addressable market.

CANONICAL POSITIONING

A^3O is not a robot, sensor platform, fleet manager or command-and-control product. It operates above and between those systems as the trust, interoperability, coordination and assurance layer for autonomous ecosystems.

TECHNOLOGY THESIS

A³O is the next-generation JAUS-aligned software core for trusted multi-vendor autonomy: preserving standardized component semantics while adding mission orchestration, policy-controlled authority, cross-platform coordination and evidence by design.

MARKET AND OPERATIONAL PROBLEM

2. The Autonomous Ecosystem Problem

The autonomous-system market is expanding in several directions at once. Factories are adding robots, cobots and autonomous mobile robots. Logistics operators are connecting warehouses, vehicles, ports and delivery systems. Infrastructure owners are deploying aerial, ground, surface and subsea platforms for inspection and information collection. Medical and emergency organizations are testing delivery, telepresence, evacuation and assistance robots. Security and defence operators increasingly combine fixed sensing, mobile platforms, effectors and distributed command nodes. In each sector, the machine population grows faster than the governance layer that must coordinate it.

Most deployments are still organized around a device, a vendor platform or a local application. That approach works during an isolated demonstration but becomes fragile when several suppliers, autonomy levels and operational domains must share one mission. A platform may report position in a different coordinate frame, represent health in a proprietary state model, apply a different concept of control ownership or interpret the same command word differently. The technical connection may be possible, yet the operational meaning remains ambiguous. The system therefore appears integrated while retaining hidden semantic and authority conflicts.

The deeper problem is not message transport. It is the absence of a shared operational contract. An autonomous ecosystem needs to know what an entity is, what capability it provides, which version is active, which organization owns it, what mission it belongs to, which policy applies, who is authorized to control it, what safety envelope is active, how uncertainty is represented and how the outcome will be verified. Without that contract, integration code becomes a collection of assumptions that are difficult to test, certify or reproduce.

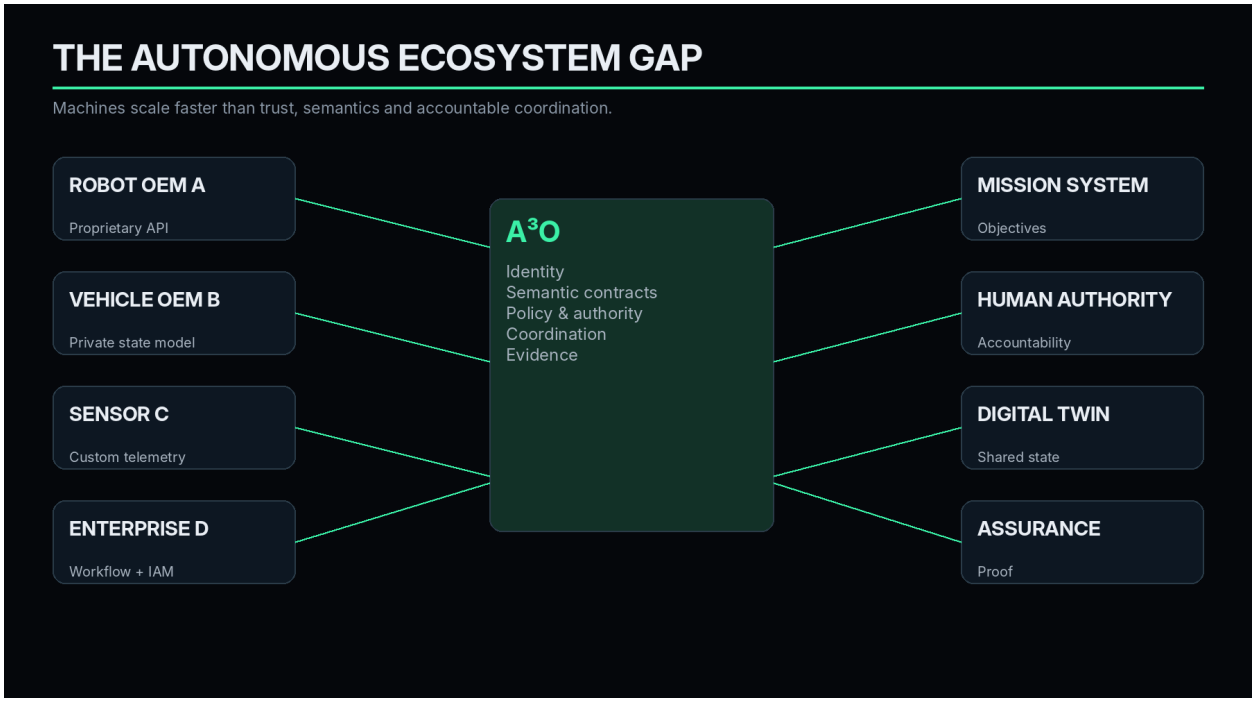
Centralized architectures introduce a second weakness. Many autonomous operations take place at an edge where communications can be intermittent, delayed, congested, jammed or administratively unavailable. A cloud service or remote command center may provide optimization and oversight, but a safe ecosystem must continue under bounded delegated authority when the central path disappears. It must prevent local autonomy from silently expanding its mandate, preserve evidence during the partition and reconcile state and decisions when connectivity returns.

Opaque autonomy creates a third weakness. An AI planner may recommend a route, classify an object or allocate tasks, but a recommendation is not an authorization. Physical execution requires a policy decision, a valid control relationship, a safety check and a traceable command. If the architecture allows an AI model, user interface or protocol adapter to bypass those boundaries, an apparently intelligent system becomes operationally unaccountable. The governance structure must therefore separate observation, interpretation, recommendation, authorization, command generation, execution and outcome verification.

Evidence is the fourth weakness. Conventional logs frequently show that software sent a message, but not which source data informed the decision, which schema decoded the message, which policy version approved it, who held control, whether the command reached the intended component or whether the physical outcome matched the objective. High-consequence autonomy requires a causal evidence graph rather than disconnected logs. That graph must survive vendor changes, software upgrades, network partitions and cross-organization operation.

Problem	Operational manifestation	A³O response
Vendor fragmentation	Different APIs, states, coordinates, control models and service versions.	Canonical capability contracts, semantic mapping and profile SDK.
Identity fragmentation	Device, workload, operator and organization identities live in separate domains.	Node, workload, human and organization identity with attestation and federation.
Authority ambiguity	Connectivity is mistaken for permission to control.	Explicit policy, delegated authority, JAUS Access Control and local safety precedence.
Central dependency	Loss of cloud or command center causes shutdown or unsafe improvisation.	Edge runtime, bounded delegation, peer coordination and safe partition behavior.
Opaque autonomy	AI recommendations can become commands without a governed boundary.	Advisory AI, PolicyDecision, safety envelope and independent command authorization.
Unprovable outcome	The causal chain from observation to physical result	Evidence graph, raw-message retention, signed fragments,

Problem	Operational manifestation	A³O response
	cannot be reconstructed.	replay and assurance packages.
Difficult certification	Every deployment combines different components, versions and vendors.	Conformance profiles, machine-readable schemas, test vectors and release evidence.



The integration gap is created by incompatible machines on one side and mission, authority and assurance obligations on the other.

CATEGORY DEFINITION

3. A New Infrastructure Category

A³O defines the category Universal Trusted Framework for Autonomous Ecosystems. A shorter commercial descriptor is Autonomous Ecosystem Trust and Coordination Platform. The category is horizontal because the underlying problems — identity, semantics, authority, coordination, resilience and evidence — recur across industries. Market entry is vertical because each industry requires validated workflows, hazard models, adapters and assurance evidence.

The word universal does not mean that A³O imposes one command set on every machine or pretends that industrial, medical, maritime and defence systems are operationally identical. It means that the framework applies one governance model to heterogeneous capabilities. A mobile robot, manipulator, radar, camera, autonomous truck and software service can retain their native interfaces while being represented through common identity, state, authority and evidence contracts. Domain-specific behavior remains in profiles and adapters, while the trusted core remains stable.

The word trusted is equally specific. Trust is not a marketing synonym for cybersecurity. In A³O it is a continuously evaluated relationship among identities, service definitions, software versions, network context, operational history, mission membership and policy. A discovered device is not automatically trusted. A signed message is not automatically authorized. A valid command is not automatically safe. Every transition in the operational loop carries a defined trust and authority context.

The word framework distinguishes A³O from a closed product suite. The architecture defines mandatory contracts, components, boundaries and conformance tests, but permits different deployments, vendors and transports. The business can therefore combine a licensable runtime, certified profiles, SDKs, integration services, partner components and assurance products without forcing every customer into one hardware ecosystem.

The category also establishes a durable boundary between the A³O core and industry solutions. The core provides identity, semantic mapping, event and state fabrics, policy, delegated authority, orchestration, evidence and developer interfaces. Profiles define the capabilities and hazards of a manufacturing cell, logistics hub, medical delivery workflow or contested-edge mission. Product solutions package those profiles with connectors, user experience and operating procedures. This separation enables reuse without erasing domain responsibility.

UNIQUE VALUE PROPOSITION

One trusted coordination standard for heterogeneous autonomous systems: vendor-neutral identity, formal capability contracts, distributed edge and swarm operation, policy-controlled autonomy and verifiable outcomes.

- A common operating model across air, ground, surface, subsea, industrial and software nodes.
- A precise boundary between perception, recommendation, authorization and physical execution.
- A shared assurance model that survives vendor changes, network partitions and cross-organization federation.
- A stable enterprise and mission integration layer above rapidly changing hardware and autonomy stacks.
- An extensible profile system that supports commercial and strategic domains without forcing one domain's terminology onto another.

INTEROPERABILITY STRATEGY

4. Why JAUS Matters — and What A³O Adds

JAUS is relevant because it addresses a foundational problem in unmanned and robotic systems: how independently implemented components describe services and exchange commands, queries, reports and events without binding the architecture to one platform. Its platform-independent, component-based and service-oriented principles align with the A³O objective of treating hardware as replaceable capability rather than as the center of the operational model.

Within the R1.2 baseline, JAUS is implemented as a controlled interoperability domain. A JAUS Subsystem maps to a managed autonomous platform, a JAUS Node to an edge compute node and a JAUS Component to an addressable capability endpoint. A JAUS Service becomes a capability contract. A JSD expressed in JSIDL becomes a versioned service-schema artifact. A JAUS address remains the protocol routing identity, while A³O binds it to a global node identity, owner, ecosystem, mission, trust state and attestation record.

The architecture makes an important correction to simplistic protocol integration. Decoding a JAUS message is not sufficient. A³O must preserve the source and destination address, service identity, applicable version and interaction semantics. It must validate the service definition, correlate the component with a trusted asset, evaluate control ownership, apply policy and safety constraints, normalize the information into the A³O state model and retain the original message for evidence. The reverse path from mission intent to a JAUS command is equally governed.

JAUS contributes standardized interaction at the component and service level. A³O adds what is required above that level: organizational and federated identity; cross-platform mission objectives; policy and delegated human authority; orchestration across JAUS and non-JAUS endpoints; partition-tolerant edge behavior; swarm state; digital-twin and knowledge architecture; evidence correlation; and cross-industry profiles. The resulting system preserves JAUS rather than hiding or rewriting it.

The native approach also creates a more credible vendor-neutral strategy. A³O can use standardized JAUS services when an endpoint supports them and governed adapters when it does not. The canonical layer prevents the rest of the application from depending directly on either representation. A customer can therefore replace a robot or controller if the new endpoint satisfies the required capability profile and conformance tests, without redesigning mission policy, user authority or enterprise integration.

Compatibility language remains disciplined. Until a working implementation and test evidence exist, the permitted terms are JAUS-aligned architecture, JAUS compatibility target and designed for JAUS integration. The document does not claim certification, approval or endorsement by SAE. It also separates JAUS interoperability from industry authorization: a JAUS-compatible medical or industrial robot still requires the applicable safety, privacy, machinery and regulatory processes.

Layer	Primary responsibility
JAUS	Service definitions, addressing, discovery, lifecycle, access control, commands, queries, reports and events.
A³O	Identity and trust, policy, human authority, mission orchestration, cross-platform coordination, world state and evidence.
A³O JAUS Interoperability Domain	Native runtime that preserves JAUS semantics and enriches each interaction with mission, trust, authority and assurance context.
Industry Profile	Domain hazards, workflows, performance budgets, privacy, compliance and validated capability combinations.

CRITICAL STANDARDS CLARIFICATION

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

OPERATIONAL MODEL

5. Universal Governed Operating Model

The A³O operating model is expressed as a universal loop: Observe, Understand, Coordinate, Decide, Authorize, Execute, Verify and Learn. It extends the narrower detect–classify–respond model used in many security systems and applies to any process in which digital decisions affect physical or organizational outcomes. Each stage has a defined input, output, authority boundary and evidence obligation.

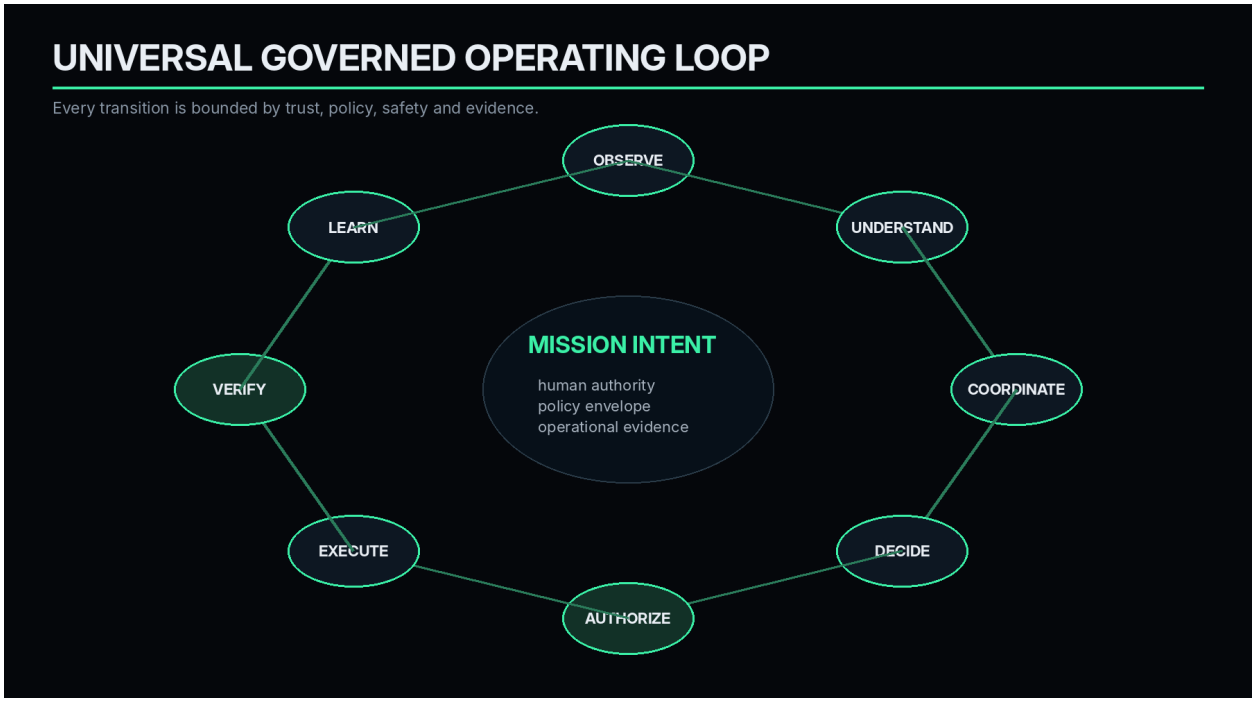
Observe acquires telemetry, messages, images, measurements, operator input and external-system data. Observation is not assumed to be true. Every input carries source identity, time, quality, uncertainty, classification, privacy and provenance. Understand converts observations into operational entities, relationships, process conditions, risks and opportunities. The system preserves the distinction between an observation, an inferred state and a prediction.

Coordinate establishes the shared context among platforms and organizations. It exchanges capability, intent, state and constraints; allocates tasks; manages dependencies; and handles competing resource claims. Decide selects a proposed course of action from the current mission, state and policy context. A decision may originate from a deterministic workflow, optimization algorithm, human operator or AI service, but it remains a proposal until the authorization stage.

Authorize evaluates whether the proposed action is permitted. It checks mission mandate, operator or delegated authority, platform ownership, JAUS Access Control, safety envelope, geographic and temporal constraints, resource limits and applicable policy. Authorization produces a versioned PolicyDecision that identifies the rule set, reason, scope, conditions and expiry. No user interface, AI model, integration adapter or message bridge can bypass this stage.

Execute transforms the authorized intent into the appropriate platform command, including a JSD-defined JAUS message where applicable. The local platform remains responsible for its own safety interlocks and execution semantics. Verify compares command acknowledgement, execution status, sensor feedback and resulting state against the intended outcome. The system distinguishes successful transmission from successful physical completion.

Learn produces a candidate improvement from evidence, not an uncontrolled change to live authority. A model, mapping or workflow update enters a governed lifecycle with validation, approval, versioning and rollback. Learning can improve recommendations and planning, but it cannot silently broaden the mission, weaken a safety rule or grant new control rights.



The universal governed operating loop separates perception, coordination, decision, authorization, execution and outcome verification.

Stage	Principal input	Canonical output	Invariant

Stage	Principal input	Canonical output	Invariant
Observe	Raw observation or message	ValidatedObservation	Source, time, quality and provenance required.
Understand	Validated observations	EntityState / ContextState	Inference remains distinguishable from measurement.
Coordinate	State, capability and intent	TaskAssignment / SharedWorldState	Peer exchange does not expand authority.
Decide	Mission, state and constraints	ActionProposal / MissionPlan	Decision is advisory until authorized.
Authorize	Proposal, policy, authority	PolicyDecision / AuthorityDecision	Explicit scope, conditions, expiry and reason.
Execute	Authorized action	ActionCommand / JAUS command	Local safety and protocol ownership preserved.
Verify	Feedback and resulting state	OutcomeAssessment	Transmission, execution and physical outcome separated.
Learn	Evidence package	LearningCandidate	No live authority change without governed release.

TECHNICAL ARCHITECTURE

6. A³O + JAUS Reference Architecture

The reference architecture is organized into eight governance planes above a protocol and platform integration layer. The planes are logical responsibilities rather than mandatory deployment boundaries. A compact edge deployment may combine several planes in one process, while an enterprise or federated deployment may distribute them across clusters and organizations. Conformance depends on preserving contracts and boundaries, not on reproducing one topology.

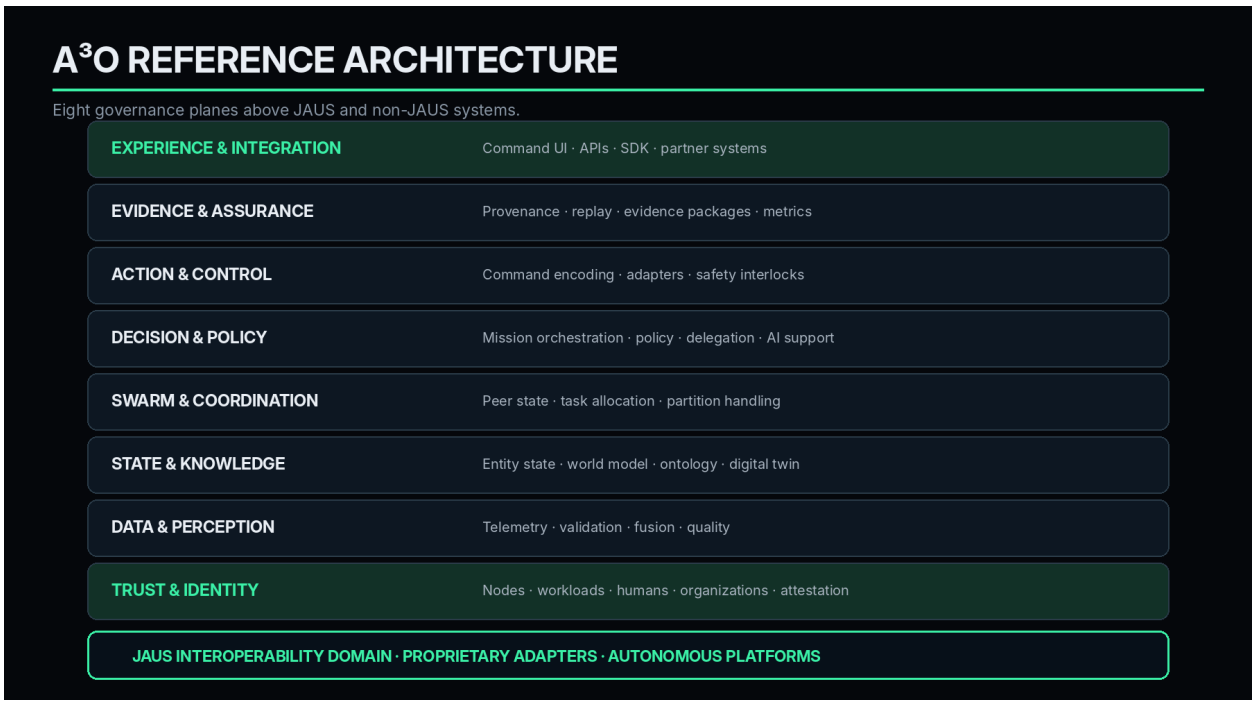
The Trust and Identity Plane establishes canonical identities for nodes, software workloads, human authorities, organizations, ecosystems and missions. It binds protocol identities — including JAUS subsystem, node and component addresses — to those canonical records. Attestation, certificates, ownership, trust score and revocation are evaluated here. This plane prevents a discovered or reachable endpoint from becoming trusted merely because it can communicate.

The Data and Perception Plane receives heterogeneous telemetry and messages, validates schemas, timestamps and quality, normalizes units and coordinate frames and performs data fusion. The State and Knowledge Plane maintains operational entities, relationships, mission context, process state, uncertainty and the ecosystem digital twin. Together they separate raw observations from interpreted state and allow downstream decisions to refer to explicit, versioned information.

The Swarm and Coordination Plane supports capability advertisement, peer-state exchange, task allocation, topology management, partition handling and reconciliation. The Decision and Policy Plane manages mission orchestration, workflows, policy evaluation, delegation, resource optimization and cognitive recommendations. The Action and Control Plane converts authorized intent into protocol-specific commands, applies execution supervision and receives feedback.

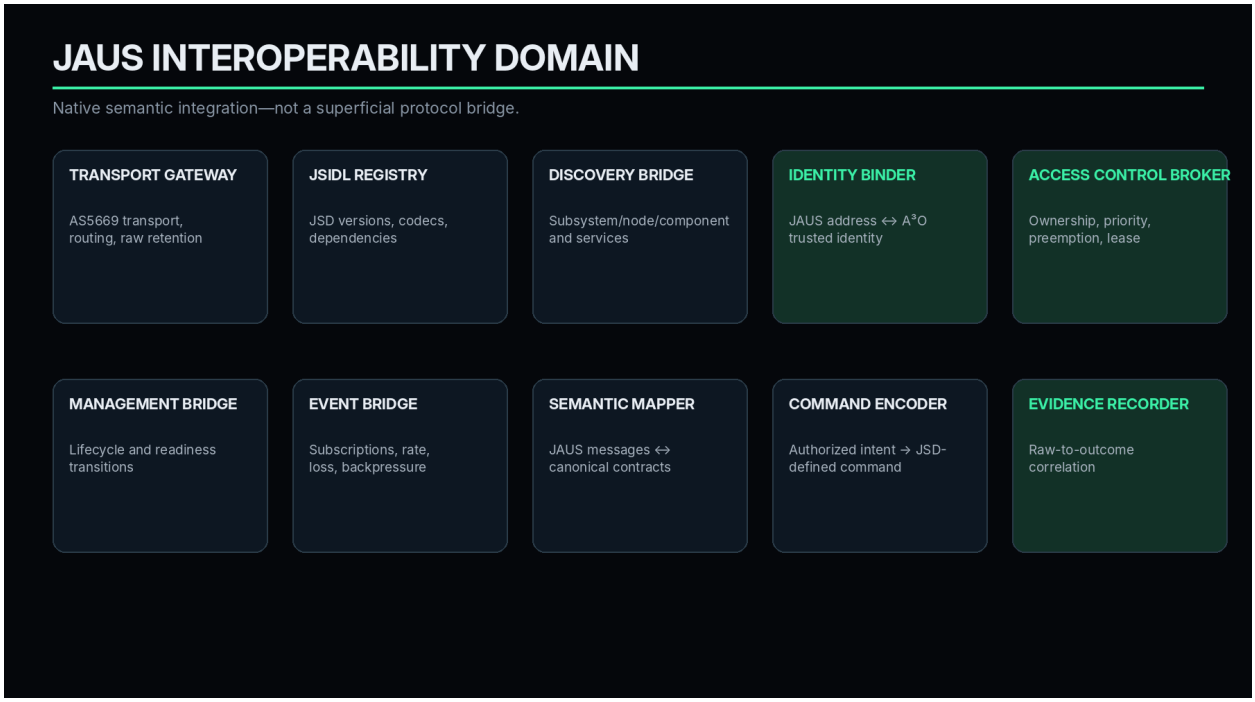
The Evidence and Assurance Plane records the causal chain across all other planes. It retains source messages, mappings, state changes, recommendations, policy decisions, authority context, commands, acknowledgements, feedback and outcome assessments. The Experience and Integration Plane exposes command interfaces, dashboards, digital-twin views, APIs, SDKs and partner-system integration without becoming the authoritative source of control.

The JAUS Interoperability Domain sits below these planes and above JAUS endpoints and transports. It is not merely an API gateway. It includes transport, JSD and JSIDL management, discovery, identity binding, Access Control, lifecycle management, event subscriptions, semantic mapping, command encoding and evidence capture. Non-JAUS adapters enter the same canonical fabric and are held to equivalent identity, mapping, authority and evidence requirements.



The eight A³O governance planes operate above the native JAUS Interoperability Domain and governed non-JAUS adapters.

6.1 Native JAUS Interoperability Domain



The JAUS Interoperability Domain preserves standard semantics and adds the A³O trust and assurance context.

Component	Responsibility
A3O.JAUS.TransportGateway	Terminates or bridges the applicable transport, resolves routing, handles fragmentation and preserves raw packets.
A3O.JAUS.JSIDLRegistry	Imports licensed JSD artifacts, manages versions and dependencies, validates service schemas and generates codecs.
A3O.JAUS.DiscoveryBridge	Discovers Subsystems, Nodes, Components and Services and creates candidate capability records.
A3O.JAUS.IdentityBinder	Binds JAUS protocol addresses to canonical A³O identities, owners, ecosystems, missions and trust records.
A3O.JAUS.AccessControlBroker	Coordinates control ownership, priority, preemption, lease state and evidence with A³O authority policy.

Component	Responsibility
A3O.JAUS.ManagementBridge	Maps component lifecycle and readiness transitions into A³O operational state and alerts.
A3O.JAUS.EventBridge	Creates and supervises subscriptions, rates, change conditions, cancellation, loss detection and backpressure.
A3O.JAUS.SemanticMapper	Maps JSD-defined fields and interactions into versioned A³O observations, state deltas and action intents.
A3O.JAUS.CommandEncoder	Transforms an authorized A³O action into the correct JSD-defined command without changing authority.
A3O.EvidenceRecorder	Correlates raw and decoded messages, mappings, policy, commands, feedback and outcomes.

6.2 Architectural boundaries

- AI and optimization services cannot directly transmit JAUS or proprietary platform commands.
- Discovery identifies a candidate capability; it does not establish trust, ownership or authorization.
- JAUS Access Control is preserved and coordinated with A³O authority rather than bypassed.
- A user interface expresses intent and displays state; it is not the authoritative policy or state store.
- Protocol translation cannot increase the authority, safety envelope or mission scope of the source request.
- Simulation, training, forecast and live operation are separated by identity, data and execution boundaries.
- A custom A³O service uses an A³O namespace and is never represented as an SAE-standard service.

GOVERNANCE MODEL

7. Trust, Identity, Authority and Human Governance

Autonomous interoperability becomes dangerous when identity and authority are treated as secondary concerns. A³O therefore separates the question “what can this component do?” from the questions “what is this component?”, “who owns it?”, “who may direct it?”, “under which mission?” and “within which safety envelope?”. The architecture evaluates all of these questions before a capability is admitted to operational use.

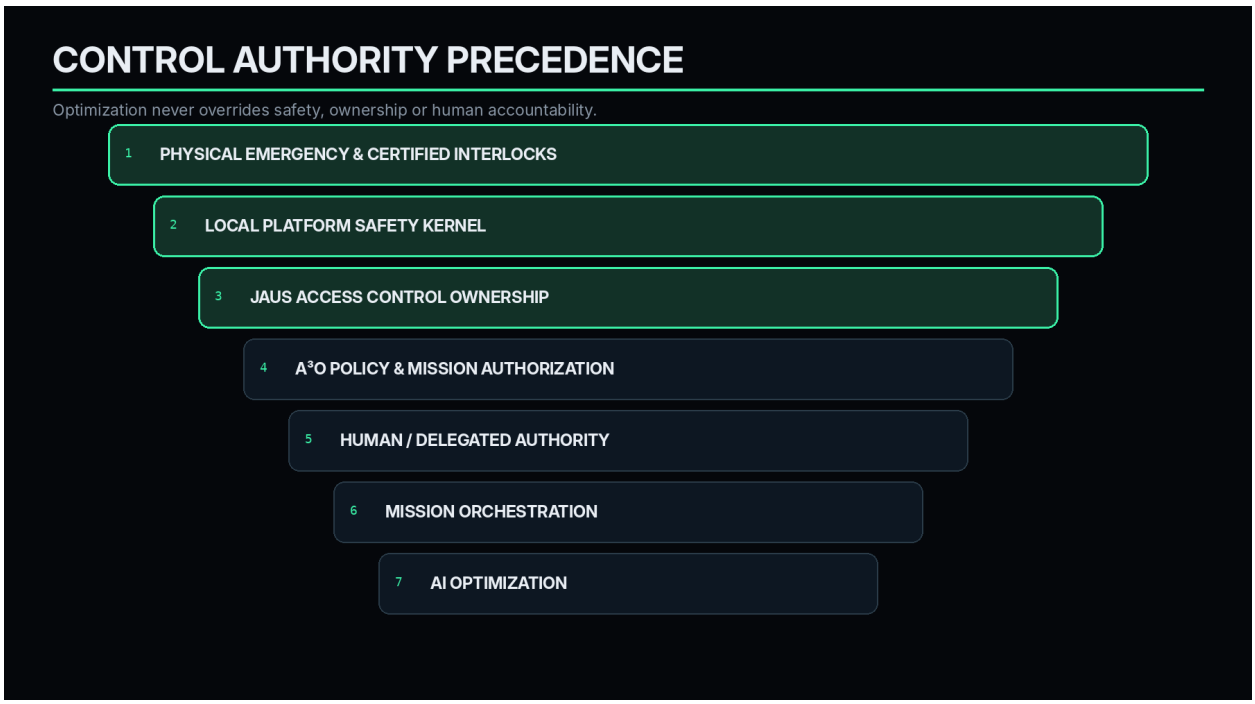
A canonical A³O identity persists across changing network addresses and protocol representations. A JAUS address identifies a subsystem, node and component within the applicable JAUS context, but that address is scoped beneath an A³O ecosystem and organization identity. This prevents address collisions across federated environments and prevents a local protocol identity from inheriting trust in another organization.

Enrollment binds the physical asset, compute node, software component, cryptographic material, vendor declaration, service inventory and ownership record. Discovery can update operational presence and available services, but it cannot overwrite the enrolled trust relationship. Unknown services, incompatible versions or changed component identities enter quarantine until an approved profile and mapping exist.

Authority is modeled as an explicit, time-bounded object. A human supervisor, organization, mission or delegated edge controller can receive an authority mandate that defines permitted resources, actions, geographic and temporal scope, conditions, escalation path and expiry. A valid mandate does not automatically grant JAUS control ownership, and JAUS control ownership does not automatically satisfy A³O mission policy. Both conditions must align.

Human governance is expressed through roles rather than through a single generic operator. A mission owner defines objectives and risk tolerance. A policy authority approves rules and delegation. A mission supervisor monitors operation and can intervene. A platform controller may hold direct control. A safety authority can impose a stop or exclusion. An auditor can inspect evidence without receiving command rights. The interface exposes these distinctions and records every transfer of authority.

The architecture supports several autonomy modes. Assisted mode keeps the human in the direct decision loop. Supervised mode allows the system to propose and execute within a narrow envelope while the human monitors. Delegated mode grants a time-bounded mission mandate to an edge controller. Coordinated autonomous mode distributes tasks among trusted nodes under a shared policy. A certified autonomous domain may eventually permit higher independence, but only after a profile-specific assurance case and operational authorization.



Control precedence prevents optimization or orchestration from overriding physical safety, local safety, JAUS ownership or policy authority.

Layer	Purpose	Constraint
Physical emergency and certified interlocks	Immediate protection of people, equipment and environment.	Cannot be overridden by A^{3}O or JAUS control.
Local platform safety kernel	Platform-specific safe-state enforcement.	May reject or modify a command inside the certified envelope.
JAUS Access Control ownership	Protocol-level control relationship and preemption.	Must be valid before applicable commands are encoded.
A^{3}O policy and mission authorization	Mission mandate, policy, geography, time and resource constraints.	Produces an auditable PolicyDecision.
Human or delegated authority	Accountable approval or bounded delegation.	Defines who may request or supervise an action.
Mission orchestration	Task sequencing and multi-platform coordination.	Operates only within existing authority.
AI optimization	Recommendation, classification and planning support.	Never creates authority or bypasses checks.

POSITIVE CONTROL INVARIANT

No physical action is valid solely because a message was technically accepted. A^{3}O requires a valid mission context, policy decision, human or delegated authority, applicable JAUS control ownership and the local platform safety acceptance.

INFORMATION ARCHITECTURE

8. Data, State, Knowledge and Message Architecture

A^{3}O treats data transformation as an accountable architectural process. A raw protocol frame is not equivalent to an observation, an observation is not equivalent to an entity state and a state estimate is not equivalent to a decision. The architecture preserves these distinctions so that uncertainty, provenance and semantic change remain visible.

The universal TelemetryEnvelope captures source node and component identity, ecosystem and mission, source and receive time, trusted-time status, modality, semantic type, unit system, reference frame, payload, quality, uncertainty, classification, privacy class, schema version, signature and provenance. Protocol-specific metadata remains attached rather than discarded. For JAUS, the envelope also retains source and destination addresses, service definition, version, message identity and interaction type.

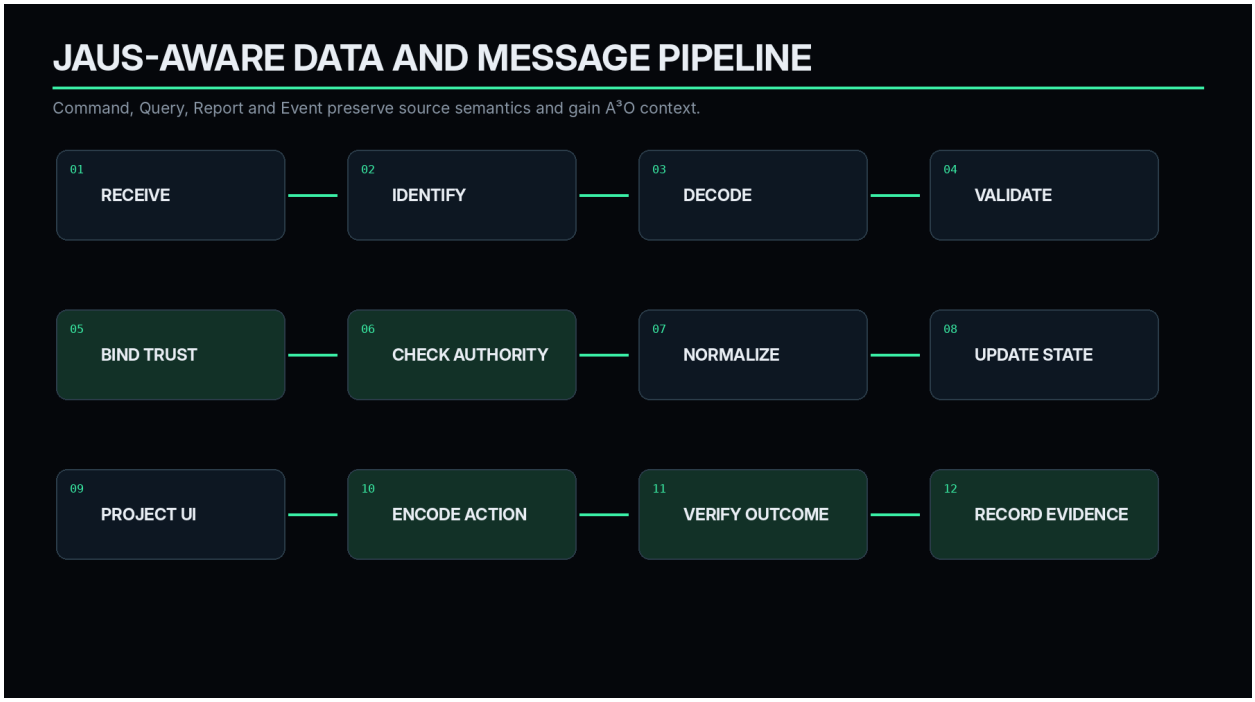
The JSIDL Registry is the source of truth for decoding a JAUS service. Every decoded message references the exact registered service definition and version. Generated codecs are versioned build artifacts. A semantic mapping profile explains how JSD-

defined fields become A³O observations, state deltas or action parameters. That profile is reviewed, tested and recorded in evidence so that a later investigator can reproduce the interpretation.

The canonical state model represents operational entities independently of the originating vendor. It can describe a robot, vehicle, manipulator, sensor, cargo item, production order, patient-independent delivery task, geographic zone, mission, operator or organization. Each property carries provenance, time, quality and confidence. Conflicting observations are retained and reconciled rather than silently overwritten.

Queries, reports and events update state through different interaction patterns. A Query creates a correlated one-shot information request and a timeout. A Report becomes a validated observation or state delta. An Event subscription creates a managed stream with rate, condition, capacity and loss monitoring. A Command is never normalized directly into execution; it becomes a GovernedActionRequest that passes authority and safety before encoding.

The digital twin is the operational projection of this state and knowledge architecture. It is not merely a visualization model. It records entities, capabilities, dependencies, missions, zones, processes, resources, risks and evidence relationships. The Experience Plane can render different views for operators, engineers and auditors without creating separate sources of truth.



The JAUS-aware pipeline preserves protocol semantics while enriching every interaction with trust, authority, state and evidence context.

ILLUSTRATIVE INTERNAL A³O CANONICAL ENVELOPE

```
{
 "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"
 },
 "service": {
  "jsidl_reference": "registered-service-definition",
  "service_version": "declared-by-provider",
  "message_name": "JSD_DEFINED_MESSAGE",
  "interaction": "REPORT"
 },
 "context": {
  "ecosystem_id": "ecosystem:hub-01",
  "mission_id": "mission:cargo-transfer-1187",
  "authority_lease_id": null,
  "policy_decision_id": "policy:decision:74921"
 },
 "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 structure is an internal A³O representation and not the JAUS wire format. Detailed wire encoding and message fields must come from licensed SAE standards and JSD data products.

JAUS pattern	A³O representation	Operational behavior
Command	GovernedActionRequest	Policy, safety, authority and Access Control checks before JSD-defined encoding.
Query	InformationRequest	One-shot request with correlation, timeout and evidence.
Report	ObservationEvent / EntityStateDelta	Validated state update with source semantics preserved.
Event	LiveStateSubscription	Subscription lifecycle, rate, loss, backpressure and cancellation.
Discovery	CapabilityRegistration	Candidate entity and service inventory pending trust binding.
Management	LifecycleTransition	Operational state transition, readiness and fault escalation.
Time / Liveness	TimeAssuranceState / HealthSignal	Trusted-time quality, online state and degraded behavior.

DISTRIBUTED OPERATIONS

9. Distributed Edge, Swarm and Partition-Tolerant Autonomy

A³O is designed for environments in which central connectivity cannot be assumed. An autonomous ecosystem may span a factory network, logistics campus, remote inspection area, maritime zone or contested edge. Latency, administrative boundaries and communication loss require local decision capability, but local capability must remain bounded by the mission and policy established before the partition.

The Edge Runtime carries identity, policy, mission, safety and evidence services close to the machines. It can validate observations, maintain local state, execute approved workflows, coordinate trusted peers and store evidence without a

continuous cloud connection. Delegated authority is explicit, time-bounded and scoped to named resources and actions. Communication loss never expands that scope.

Swarm operation is defined as distributed coordination among autonomous nodes, not as unrestricted peer-to-peer control. Nodes advertise capabilities and current constraints, exchange signed state deltas, negotiate or receive tasks, monitor topology and reconcile evidence. A peer message does not become trusted merely because it came through the mesh. Identity, profile and policy checks still apply.

The architecture defines six communication states: CONNECTED, DEGRADED, PARTITIONED, ISOLATED, RECONCILING and RESTORED. Each state has an allowed action envelope. In DEGRADED mode, the system may reduce event rates and retain noncritical data locally. In PARTITIONED mode, delegated missions continue only within their expiry and safety limits. ISOLATED mode restricts the node to local safety and explicitly authorized fallback behavior. RECONCILING mode compares state, authority and evidence before normal operation resumes.

Task allocation preserves mission intent, ownership and evidence lineage. When a node fails or becomes unavailable, reassignment records the reason, previous assignee, new assignee, changed route or process and resulting risk. Conflicting peer decisions are retained and resolved through a defined reconciliation policy rather than hidden by last-write-wins behavior.

JAUS services provide platform-level capabilities, state and mission-spool behavior where applicable. A³O adds the collective layer: trusted membership, multi-platform allocation, shared-world context, partition policy, federated authority and evidence merging. The swarm layer therefore complements rather than redefines the JAUS component model.

State	Condition	Mandatory behavior
CONNECTED	Central and peer paths available.	Normal mission envelope and synchronization.
DEGRADED	Reduced bandwidth, quality or selected path loss.	Lower rates, prioritize control and safety data, local buffering.
PARTITIONED	Edge group separated from authority center.	Continue only under time-bounded delegated authority.
ISOLATED	No trusted peer or central path.	Local safety and explicitly approved fallback behavior only.
RECONCILING	Connectivity restored; state or decisions may conflict.	Freeze sensitive expansion, compare authority, state and evidence.
RESTORED	Reconciliation complete and trust re-established.	Resume approved operating mode and publish evidence package.

9.1 Swarm invariants

- Every node has a verifiable identity and declared capability profile.
- Peer loss, leader loss or network partition never expands authority.
- The local safety kernel overrides mission optimization and task allocation.
- Task reassignment preserves intent, ownership, reason and evidence lineage.
- Conflicts are retained, classified and reconciled; they are not silently discarded.
- A compromised or untrusted node can be isolated without collapsing the whole ecosystem.
- Collective AI recommendations remain traceable to source nodes, observations and policy.

ASSURANCE ARCHITECTURE

10. Safety, Resilience, Evidence and Assurance

Safety and resilience are treated as continuous architectural properties rather than as a final testing phase. A³O does not attempt to replace the certified safety functions of a robot, vehicle, industrial controller or medical device. It establishes the ecosystem-level contracts that prevent higher-level orchestration from bypassing those functions and that make cross-platform behavior reviewable.

The Safety Kernel evaluates action envelopes, exclusion zones, resource constraints, operating modes, dependency state and escalation rules. It can reject a proposed action, constrain parameters, require human authorization or force a safe state. Its decision is independent of the AI or optimizer that generated the proposal. The platform-local safety controller remains the final authority for platform-specific interlocks.

Resilience is defined as controlled degradation with preservation of strategic intent, safety and evidence. The architecture assumes component failure, stale data, incompatible versions, network disruption, revoked identities and partial state. Every critical service declares fallback behavior, maximum stale time, dependency set, recovery procedure and evidence requirement. A system that continues operating without knowing whether its assumptions remain valid is not considered resilient.

The Evidence Graph links every control-relevant transition. It begins with raw observations and messages, continues through decoding and semantic mapping, records the state used by the decision, captures recommendation and policy, identifies the authority holder, stores the encoded command and acknowledgement, receives execution feedback and produces an OutcomeAssessment. Hashes, signatures, trusted time and append-only storage support integrity across edge and central repositories.

An Assurance Package is generated for a mission episode, release or regulated workflow. It includes configuration and software versions, applicable profiles, identities, policy set, risk controls, conformance results, evidence references, exceptions and operator interventions. The package can support incident review, customer acceptance, internal governance, regulator engagement or certification evidence, while remaining distinct from an external certificate.

Replay is a first-class capability. A reviewer can reconstruct the operational state and sequence of decisions from preserved evidence, compare the intended and actual outcomes and identify where uncertainty or authority changed. Simulation can use the same canonical contracts, but simulation identities and data are clearly separated from live operation to prevent accidental command paths or false evidence.

Assurance object	Purpose	Lifecycle point
Safety envelope	Defines permitted state, action, zone, resource and timing constraints.	Before authorization and again at local execution.
Outcome assessment	Compares intended result, acknowledgement, feedback and physical state.	After every material action.
Evidence fragment	Signed local record created during connected or partitioned operation.	At each decision, command and outcome transition.
Evidence package	Merged mission or release record with configuration, policy and exceptions.	At mission close, incident, audit or release gate.
Replay	Deterministic or explanatory reconstruction of state and decisions.	Investigation, training, validation and assurance.
Conformance evidence	Test results mapped to profile requirements and versions.	Before partner or deployment acceptance.

EVIDENCE BY DESIGN

Evidence is created at runtime, not reconstructed after an incident. Raw messages, semantic mappings, state, authority, policy, commands, feedback and outcomes remain linked by stable correlation identifiers.

RESPONSIBLE AUTONOMY

11. AI and Cognitive Services Under Governance

A³O uses AI as a cognitive service, not as an independent source of authority. Models can classify observations, estimate state, predict failure, propose routes, optimize resource allocation, detect anomalies and recommend actions. Those capabilities can improve mission quality, but they do not change the governance chain. An AI output is represented as a recommendation or proposal with source data, model identity, version, confidence, explanation and intended scope.

The architecture separates perception models from decision models and decision models from command execution. A perception model may convert imagery or sensor data into an object hypothesis. A planner may evaluate alternative task sequences. An optimizer may rank routes or resource assignments. None of these outputs becomes a physical command until policy, human or delegated authority, JAUS Access Control and safety validation have succeeded.

Model governance begins with identity and provenance. Every deployed model has a canonical identifier, owner, training-data statement, version, intended use, known limits, performance baseline and rollback path. A model update is treated as a release that may alter operational behavior. It therefore passes validation against representative and adversarial scenarios, profile-specific acceptance criteria and regression tests before activation.

Runtime monitoring compares model confidence, data quality, drift indicators, disagreement among models and actual outcomes. The system can reduce autonomy, request human review, switch to a deterministic fallback or isolate a model when the operating context leaves its validated domain. Low confidence is not automatically an error, but it must be visible to the policy and decision layers.

Learning from live operations produces a LearningCandidate, not an automatic production update. The candidate links evidence, failure or improvement objective, affected profile, proposed model or rule change and validation plan. Approval remains

organizationally accountable. This prevents a system from silently learning a broader mission, weakening a constraint or normalizing an unsafe workaround.

Collective or swarm intelligence follows the same rules. A group recommendation must remain traceable to contributing nodes and observations. Compromised, stale or low-trust nodes can be excluded. Consensus is not treated as truth, and majority voting cannot override a safety or policy rule. The system may use distributed computation while preserving centralized accountability for the approved mission and policy.

Cognitive function	Purpose	Output	Hard boundary
Observation model	Classification, detection, estimation or anomaly score.	ValidatedObservation / hypothesis	No command rights.
Planning model	Route, task sequence or resource plan.	ActionProposal / MissionPlan	Must state constraints and alternatives.
Optimization service	Ranked allocation or schedule.	Recommendation	Cannot expand mission scope.
Policy assistant	Explains rules or identifies relevant policy.	PolicyRecommendation	Policy Engine remains authoritative.
Operator assistant	Summarizes state and proposes intervention.	Human-facing recommendation	Human identity and decision recorded.
Learning pipeline	Proposes model or rule update from evidence.	LearningCandidate	Separate validation and release required.

AI COMMAND BARRIER

An AI component shall not directly transmit a JAUS or vendor-specific command. The only valid path is recommendation → policy and safety evaluation → authority validation → protocol-specific command encoding.

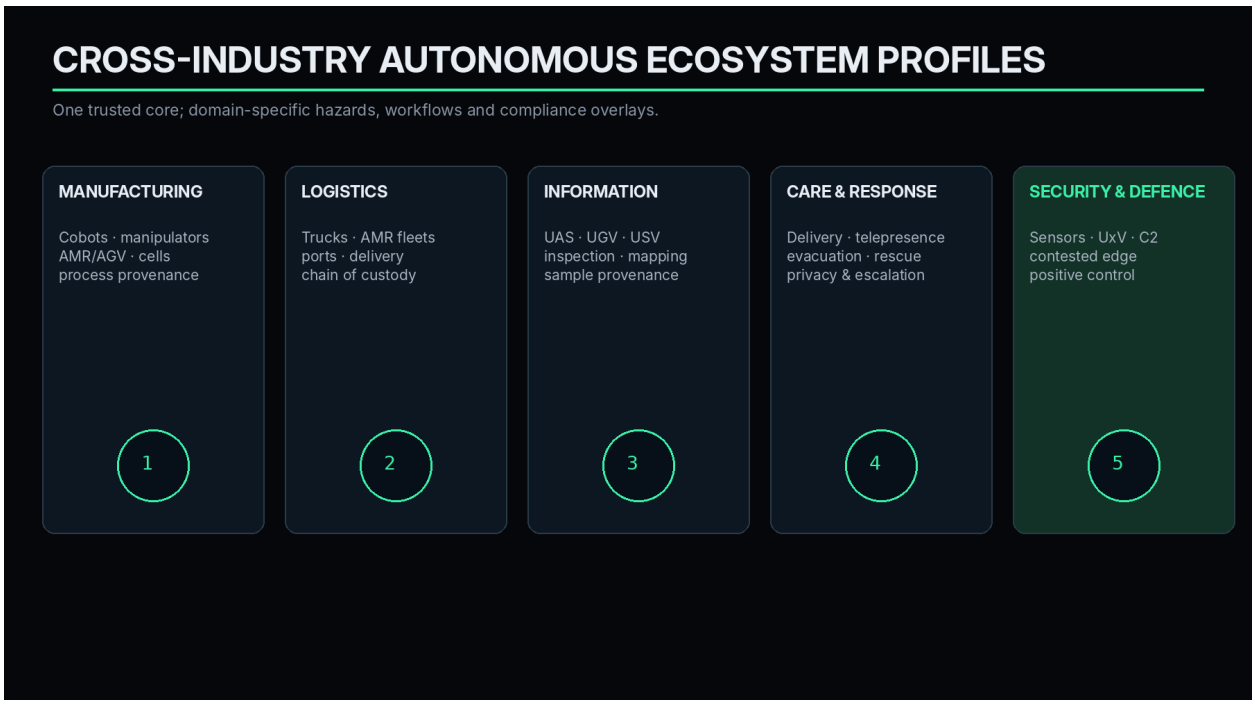
INDUSTRY PROFILES

12. Cross-Industry Solution Blueprints

The A³O core is industry-independent, but autonomous operations are not. A manufacturing cell, logistics fleet, medical delivery robot and security mission have different hazards, operating procedures, privacy rules and performance budgets. A³O resolves this tension through Industry Profiles. Each profile selects required capabilities, adapters, policies, evidence, conformance tests and user roles while preserving the common trust and orchestration architecture.

A profile is more than a marketing configuration. It is a controlled implementation contract. It identifies the participating entities and protocols; the required A³O and JAUS services; the allowed autonomy modes; the safety and authority model; the canonical data extensions; the applicable performance limits; the threat assumptions; the evidence package; and the exit criteria for deployment. Profiles can inherit from a common baseline while adding local or customer-specific constraints.

JAUS is used where its service model is applicable. Commercial systems that expose OPC UA, ROS, DDS, MQTT, REST or proprietary interfaces are integrated through governed adapters. A profile can therefore include both JAUS and non-JAUS nodes without creating two governance systems. The same identity, state, authority and evidence requirements apply to every endpoint.



Five initial industry profiles reuse one A³O core while adding domain-specific workflows, hazards and compliance overlays.

12.1 Manufacturing

In manufacturing, A³O coordinates manipulators, cobots, autonomous mobile robots, AGV fleets, machine vision, conveyors, tools, production cells and process systems. The primary value is not remote control of one robot. It is safe coordination across vendors and process boundaries: material handoff, shared zones, recipe and tool-state integrity, changeover, quality evidence and production provenance.

The profile integrates with MES, SCADA, PLC and safety systems without claiming to replace their certified functions. A³O represents the production order, resource capability, material identity, process state and allowed action envelope in a shared model. It can schedule an AMR delivery, confirm that a cell is ready, coordinate a manipulator task and verify completion while respecting local interlocks and change-control authority.

12.2 Transportation and Logistics

The logistics profile connects warehouse robots, autonomous trucks, loading equipment, delivery drones, port systems, surface vehicles and enterprise transport workflows. It governs route and geofence constraints, energy state, cargo identity, handoff, chain of custody, fleet deadlock and infrastructure availability. A mission can cross several platform families while retaining one accountable workflow.

JAUS mobility, sensing or mission services may support suitable platforms, while non-JAUS warehouse and enterprise systems enter through adapters. A³O maintains the handoff state between physical and business systems: which asset carries which cargo, who authorized the transfer, what condition was observed, which node accepted responsibility and whether the delivery outcome was verified.

12.3 Information Collection and Inspection

The inspection profile coordinates UAS, UGV, USV, UUV, fixed sensors, mapping systems and analysis services. It plans coverage, manages coordinate and time integrity, assigns collection tasks, adapts to communication loss and records the provenance of every image, measurement or sample. The result is a defensible information product rather than an unstructured collection of sensor files.

Geology, environmental monitoring, infrastructure inspection, agriculture and disaster assessment share the need to connect different vehicles and sensors under one collection objective. A³O can represent the planned area, required modality, quality threshold, environmental constraint, sample identity and evidence chain while leaving platform-specific flight, navigation or manipulation to the applicable controller.

12.4 Care, Medical and Emergency Response

The care and response profile supports medicine or blood delivery, telepresence, assistive robots, evacuation, search and rescue and controlled payload workflows. It emphasizes identity, privacy, priority, payload custody, human escalation and the distinction between operational interoperability and medical decision-making.

JAUS compatibility can standardize aspects of mobility, sensing and component interaction, but it does not establish medical-device authorization or clinical safety. The profile isolates patient-identifying information, defines who may change priority or destination, records custody transitions and requires human escalation when the robot leaves its validated operational envelope.

12.5 Security and Defence

The Security and Defence profile covers sensing, UxV, distributed command nodes, effectors and contested communications at a high architectural level. It emphasizes mission identity, positive control, policy enforcement, spoofing resistance, delegated authority, partition behavior, controlled degradation and immutable evidence. Detailed tactical or weapon employment procedures remain outside this whitepaper.

DroneDefender is the first reference implementation of this profile. It demonstrates the governed loop from observation and fusion to human or delegated authorization, action and outcome evidence across air, ground and maritime protection contexts. The reference implementation validates core A³O components but does not define or limit the universal platform category.

Profile	Representative systems	A³O focus
Manufacturing	Manipulators, cobots, AMR/AGV, vision, cells, process systems	Safe coordination, recipe and tool integrity, interlocks, production provenance.
Logistics and transport	AMR, trucks, delivery systems, ports, loading robots	Route, energy, geofence, cargo identity, handoff and chain of custody.
Inspection and information	UAS, UGV, USV, UUV, fixed sensors, mapping	Coverage, coordinate integrity, sample identity, quality and provenance.
Care and response	Delivery, telepresence, assistive, evacuation and rescue robots	Identity, privacy, payload custody, priority and human escalation.
Security and defence	Sensors, UxV, C2, effectors and contested-edge nodes	Positive control, policy, spoofing resistance, partition behavior and evidence.

REGULATED-DOMAIN BOUNDARY

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

PRODUCT STRATEGY

13. Product and Deployment Portfolio

The A³O product portfolio converts the architecture into deployable and licensable modules. Customers do not need to adopt every module at once. A deployment can begin with connectivity and trusted state, then add orchestration, assurance, digital-twin and industry-profile capabilities. The modules share identity, contracts and evidence so that the system does not fragment as it grows.

A³O Connect provides protocol and system integration, including the native JAUS Interoperability Domain and governed connectors for non-JAUS endpoints. A³O Edge Runtime executes identity, policy, workflow, state and evidence services near the machines. A³O Swarm provides peer capability exchange, distributed task allocation, partition handling and reconciliation.

A³O Command provides mission planning, human authority, policy workflows and operational supervision. A³O Intelligence hosts governed cognitive services and model lifecycle controls. A³O Assurance provides evidence graph, replay, conformance records and assurance packages. A³O Twin provides ecosystem state, simulation, scenario and forecasting capabilities. A³O Industry Profiles package validated contracts, connectors, user roles, tests and deployment guidance for specific sectors.

The portfolio is designed for several deployment forms. An embedded or vehicle deployment can run a compact Edge Runtime and gateway. A site deployment can coordinate a factory, warehouse, port or protected perimeter. An enterprise deployment can federate several sites, fleets and organizations. A sovereign or strategic deployment can use private infrastructure, disconnected operation and controlled cross-domain exchange.

Commercial packaging should preserve architectural neutrality. Protocol adapters and industry profiles can be sold through partners, but the trust, policy, evidence and conformance core remains governed by A³O. This creates a partner ecosystem without surrendering the integrity of the operating model.

Product	Principal capability	Commercial unit

Product	Principal capability	Commercial unit
A³O Connect	JAUS gateway, JSIDL registry, discovery, semantic mapping and non-JAUS connectors.	Per node, gateway or integration domain.
A³O Edge Runtime	Local identity, policy, state, workflow, safety coordination and evidence.	Per node, site or edge cluster.
A³O Swarm	Peer state, task allocation, topology, partition and reconciliation.	Per fleet, swarm or mission domain.
A³O Command	Mission orchestration, human authority, policy and operational UI.	Per site, fleet or enterprise.
A³O Intelligence	Governed AI services, model registry, monitoring and recommendations.	Per model, workload or capacity tier.
A³O Assurance	Evidence graph, replay, conformance, audit export and assurance packages.	Per deployment, mission or assurance tier.
A³O Twin	Operational twin, simulation, scenario, training and forecasting.	Per site, ecosystem or simulation capacity.
A³O Industry Profiles	Validated capabilities, adapters, workflows, policies and test suites.	Profile license and partner certification.

Deployment	Composition	Typical context
Embedded / vehicle	Compact runtime, gateway, local state and evidence.	Disconnected or low-latency platform operation.
Site / facility	Multi-platform coordination, local command, digital twin and assurance.	Factory, warehouse, port, campus or protected perimeter.
Fleet / mission	Cross-site or mobile orchestration with delegated authority.	Logistics fleet, inspection campaign, emergency response.
Enterprise	Federated identity, policy, data and profile governance.	Multi-site owner or systems integrator.
Sovereign / strategic	Private infrastructure, controlled federation and contested-edge operation.	Public safety, critical infrastructure and defence contexts.

ADOPTION MODEL

14. Integration Lifecycle and Conformance

A³O changes integration from an undocumented adapter project into a controlled lifecycle. The lifecycle begins with a capability and standards inventory, not with code. The integrator identifies the platform, transport, service definitions, versions, ownership, operational role, safety constraints, target profile and desired conformance level. Missing or proprietary semantics are documented before implementation begins.

For JAUS systems, the applicable licensed JSD artifacts are imported into the JSIDL Registry. The registry validates namespace, dependencies, versions and message definitions, then generates or approves codecs. Discovery is tested against the declared hierarchy. The JAUS address is bound to the enrolled A³O identity and owner. Access Control, management, event and time behavior are exercised before mission commands are enabled.

Semantic mapping is treated as a testable product. Each field transformation, unit conversion, coordinate-frame conversion, lifecycle mapping and action parameter is versioned. Round-trip and negative tests confirm that the adapter does not discard information, invent authority or accept an ambiguous version. The raw message remains available for evidence and troubleshooting.

The integration then progresses through conformance levels. J0 establishes JAUS awareness and message recognition. J1 targets the applicable Core Service integration. J2 validates selected application service sets. J3 adds full A³O governance: identity, policy, authority, state and evidence. J4 represents an A³O Certified Profile after the partner implementation passes the A³O test suite; any external SAE certification or other regulatory authorization is stated separately.

Conformance is not a one-time label. The compatibility matrix records platform, component, service, version, adapter, profile, tested functions, limitations and evidence. A software or JSD change can trigger regression testing. Unsupported or unknown versions fail closed rather than being interpreted through a nearest-match assumption.

The result is a repeatable partner model. Robot vendors and integrators can implement against a published profile, run reference tests and provide evidence. Customers can compare compatible implementations at the capability level. A³O can expand its ecosystem without absorbing every vendor-specific integration into the core engineering team.

el	Name	Acceptance meaning

el	Name	Acceptance meaning
	JAUS-Aware	Recognizes JAUS entities and messages; no operational compatibility claim.
	Core Compatible	Target Core Service integration, transport behavior and lifecycle checks.
	Service-Set Compatible	Selected application service sets and interaction scenarios pass.
	Governed A³O Integration	Identity, policy, authority, state, evidence and degraded-mode controls pass.
	A³O Certified Profile	Published A³O profile suite passes; external certification is stated separately.

Test family	Coverage
Discovery and inventory	Hierarchy, service discovery, disappearance, reappearance and changed advertisement.
Schema and version	JSD import, dependency, codec round-trip, unknown and incompatible versions.
Query and report	Correlation, timeout, stale data, malformed payload and semantic mapping.
Events	Create, confirm, rate, condition, change, cancellation, loss and capacity.
Access Control	Acquire, release, contention, preemption, lease expiry and policy coordination.
Management and health	Lifecycle transitions, readiness, liveness, fault and recovery.
Transport resilience	Loss, delay, duplication, reordering, reconnection and partition.
Security	Spoofing, replay, downgrade, flooding, malicious discovery and quarantine.
Evidence	Raw-to-outcome completeness, integrity, time and replay.
Industry scenario	End-to-end mission within approved profile constraints.

COMMERCIAL ARCHITECTURE

15. Business Model

The A³O business model is based on the value of a stable governance layer above changing autonomous hardware. Customers pay not merely for message connectivity but for reusable interoperability, operational authority, evidence and reduced integration risk. The model combines software licensing, runtime subscriptions, industry profiles, integration kits, assurance services and partner conformance.

Core runtime revenue can be structured by managed node, site, fleet, enterprise or mission domain. This aligns pricing with the operational footprint while allowing small pilots to start with limited scope. Higher tiers add federation, disconnected operation, digital twin, advanced evidence, high availability and enterprise policy management.

Industry Profiles create repeatable vertical products. A profile bundles capability contracts, connectors, workflows, policy templates, user roles, test vectors, deployment guidance and assurance artifacts. It can be licensed directly, delivered with a systems integrator or embedded in a partner solution. Profile maintenance generates recurring value as standards, platforms and regulations evolve.

The JAUS Interoperability Domain supports a connector and certification ecosystem. Vendors can license the SDK, import their service definitions, run the conformance harness and publish a verified compatibility record. A³O can charge for development kits, certification services, annual profile maintenance and marketplace or support participation. The objective is to turn integration knowledge into reusable product assets rather than one-off engineering revenue.

A³O Assurance provides an additional commercial layer. Customers in high-consequence or regulated environments need mission evidence, release evidence, audit export, replay and compatibility records. Assurance can be sold as a runtime tier, managed service or professional engagement without claiming to replace an external regulator or certification body.

Professional services remain important during early market entry, but they should accelerate productization. Every pilot must produce reusable schemas, mappings, test cases, profile clauses and deployment patterns. The commercial metric is not only pilot revenue; it is the percentage of integration work converted into reusable intellectual property and shorter future deployments.

Revenue stream	Value delivered	Possible pricing basis
Core software	Connect, Edge Runtime, Command, Swarm, Assurance and Twin licensing.	Node, site, fleet, enterprise or capacity.

Revenue stream	Value delivered	Possible pricing basis
Industry profile	Validated connectors, workflows, policies, roles and tests.	Annual profile license and maintenance.
Developer platform	SDK, JSIDL tools, simulators, adapters and test harness.	Developer seat, partner tier or enterprise subscription.
Conformance services	Profile testing, compatibility matrix and release evidence.	Per platform, version or certification cycle.
Assurance services	Evidence packages, replay, audits and deployment reviews.	Per mission, site, release or managed service.
Integration and support	Architecture, onboarding, deployment and operational support.	Project, retainer or premium support tier.

15.1 Unit-economics logic

The economic advantage of the platform improves as the library of profiles and tested components grows. The first integration with a new service family carries standards analysis, mapping and test costs. Subsequent deployments reuse the registry artifacts, codecs, mappings, conformance tests and evidence model. Gross margin therefore depends on disciplined reuse and on preventing customer-specific exceptions from entering the core without a profile decision.

Partner leverage is equally important. Systems integrators already own customer relationships and domain deployment capability. Robot vendors need a credible path into multi-vendor environments. A³O can provide the common trust and conformance layer while partners deliver hardware, local integration and operations. The partner model expands reach without turning A³O into a hardware reseller or project-only engineering company.

COMMERCIAL STRATEGY

16. Market Context and Go-to-Market

The market context is defined by the growth and diversification of robotics rather than by one narrow equipment category. Industrial installations, professional service robots, logistics platforms and autonomous mobility systems are increasing the number of machines that must be integrated into enterprise and mission operations. The resulting software and systems-integration demand includes orchestration, fleet management, simulation, data infrastructure, cybersecurity, safety, maintenance and compliance. A³O addresses the shared interoperability and governance layer across those categories.

Public International Federation of Robotics reporting provides useful indicators of scale rather than a direct A³O revenue forecast. IFR reported 542,000 industrial robots installed in 2024 and an operational stock of approximately 4.664 million units. It also reported almost 200,000 professional service robots sold in 2024, including approximately 102,900 units in transportation and logistics. Those figures demonstrate an expanding installed and annual shipment base, but they do not identify how many systems support JAUS or how much of the market is immediately addressable by A³O.

The European Commission describes robotics as relevant across manufacturing, health, transport, security, energy and the environment, and treats connected and automated mobility as a convergence of robotics, AI, IoT, high-performance computing, communications, cybersecurity, data and liability. This reinforces the horizontal need for interoperability and governance, while also confirming that market entry must respect sector-specific regulation and procurement.

The initial go-to-market should not attempt to sell a universal platform to every industry at once. It should prove the core through a small number of reference deployments that exercise different architectural dimensions. DroneDefender provides the first Security and Defence profile and demonstrates distributed sensing, human authority, action and evidence. A logistics or manufacturing pilot should demonstrate multi-vendor mobility, handoff and enterprise integration. An inspection or environmental pilot should demonstrate heterogeneous sensing, provenance and partition-tolerant edge operation.

Customers should be approached through systems integrators, robot and sensor vendors, critical-infrastructure operators and organizations already experiencing multi-vendor integration cost. The commercial entry point is a bounded problem: connect a defined set of platforms, normalize state, enforce authority and produce evidence. The platform expands after the customer sees that new devices and workflows can be added without redesigning the control plane.

Partner enablement is a force multiplier. The SDK, profile specification, simulator, reference components and conformance harness allow vendors to prepare compatibility before a customer deployment. The compatibility matrix gives integrators a clear statement of tested versions and limitations. A partner programme can combine technical tiers, training, test access, profile co-development and joint go-to-market.

Indicator	Publicly reported context	Use in this whitepaper
Industrial robotics indicator	542,000 industrial robots installed in 2024; operational stock approximately 4.664 million.	IFR World Robotics 2025 public release.

Indicator	Publicly reported context	Use in this whitepaper
Professional service robots	Almost 200,000 units sold in 2024.	IFR service-robot public release; sample-based market data.
Transportation and logistics robots	Approximately 102,900 units sold in 2024.	IFR service-robot public release.
Cross-sector relevance	Manufacturing, health, transport, security, energy and environment.	European Commission robotics policy pages.
A³O interpretation	Growing heterogeneous machine base increases integration and governance demand.	Management inference, not a direct market-size measurement.

16.1 Management market scenario

VALIDATION STATUS

The following TAM, SAM and SOM ranges are management planning scenarios. They are not independently validated market estimates and shall not be presented as audited or third-party research.

r	Working range	Definition and limitation
	€75–150B	Long-horizon global spend associated with autonomous-system integration, orchestrati control software, assurance and related services across target sectors.
	€8–20B	Segments where multi-vendor autonomy, edge operation, critical workflows and eviden create an identifiable near-to-medium-term need.
year SOM	€25–60M ARR	Execution scenario based on a limited number of enterprise deployments, industry prof partners and recurring platform revenue.

16.2 Go-to-market sequence

Stage	Commercial action	Proof created
1. Reference proof	DroneDefender and the existing governed loop.	Technical credibility and first profile evidence.
2. Non-security pilot	Logistics, manufacturing or inspection with at least two vendor stacks.	Demonstrate universal core and vendor replacement.
3. Partner SDK	Enable selected integrators and platform vendors.	Convert integration into reusable partner capability.
4. Profile productization	Publish controlled profile, compatibility matrix and assurance package.	Repeatable deployment and recurring revenue.
5. Enterprise federation	Connect sites, fleets or organizations under common policy.	Higher-value platform expansion.
6. Conformance ecosystem	Reference components, test lab and partner programme.	Network effects and defensibility.

STRATEGIC DIFFERENTIATION

17. Competition and Defensibility

A³O competes across several adjacent categories rather than against one identical product. Robotics middleware connects software components. Fleet-management products optimize a vendor family or vehicle class. Industrial platforms integrate equipment within factory architectures. cloud and IoT platforms collect data and run analytics. command-and-control products manage specific operational missions. Digital-twin systems model assets and processes. Cybersecurity products protect identities and networks. None of these categories alone provides the complete trust, authority, cross-protocol orchestration and evidence model defined by A³O.

The principal differentiation is not that A³O supports more protocols. Protocol support can be copied and often becomes a commodity. The defensible layer is the governed semantic and operational model: how a service definition becomes a trusted capability; how protocol identity binds to asset and organization; how an action proposal becomes authorized; how control ownership is coordinated; how state and uncertainty are represented; how partitions are handled; and how evidence links the decision to the physical outcome.

JAUS alignment strengthens this position because it provides a formal interoperability foundation and a path to existing component and service models. A³O does not claim ownership of the standard. Its intellectual property lies in the integration domain, canonical contracts, semantic mappings, cross-protocol profiles, authority model, evidence graph, conformance tooling and accumulated compatibility data.

Industry profiles create a second moat. A validated profile contains domain knowledge that is costly to reproduce: hazards, roles, workflows, state models, adapter behavior, performance limits, threat controls, test scenarios and assurance artifacts. The profile library grows more valuable as deployments contribute reusable evidence and as partners certify more platforms.

Operational data and evidence create a third moat, subject to privacy and customer ownership. A³O can learn which combinations of versions, mappings, network conditions and mission patterns produce reliable outcomes. That knowledge improves test coverage, deployment automation and risk prediction. It must be governed so that customer data is not appropriated or exposed.

The partner and conformance ecosystem creates a fourth moat. A vendor that has invested in a tested A³O profile can enter additional customer ecosystems with less effort. A customer that has built mission policy and enterprise integration above the A³O core can replace hardware without losing the operational layer. This creates switching value without recreating the vendor lock-in that A³O is designed to reduce.

Adjacent category	Typical strength	A³O differentiation
Robotics middleware	Component communication and developer ecosystem.	Trust binding, mission authority, evidence and cross-organization governance.
Fleet manager	Operational control for a platform family or vehicle class.	Multi-vendor and multi-domain capability profiles.
Industrial integration platform	Factory data and process integration.	Autonomous authority, partition behavior and outcome evidence.
Cloud / IoT platform	Data ingestion, analytics and device management.	Bounded edge execution and physical control governance.
Command-and-control system	Mission-specific operational interface.	Reusable universal core and cross-industry profile model.
Digital twin	Asset and process representation.	Authoritative state-to-command-to-outcome chain.
Cybersecurity platform	Identity, posture and network protection.	Mission semantics, authority, coordination and assurance.

17.1 Defensibility assets

- Canonical ontology and versioned data contracts for heterogeneous autonomy.
- JAUS Interoperability Domain, JSIDL registry, generated codecs and mapping profiles.
- Authority, delegated-operation and Access Control coordination model.
- Evidence graph, mission replay and assurance-package generation.
- Cross-industry profile library and compatibility matrix.
- Conformance harness, negative tests, reference components and deployment evidence.
- Partner ecosystem and accumulated integration knowledge.
- Brand and category ownership around trusted autonomous ecosystems.

EXECUTION PLAN

18. Roadmap and Investment Programme

The roadmap converts the R1.2 architecture into an implemented and commercially testable platform. It begins with standards and licensing because an interoperability product cannot be credible if its service definitions, conformance scope or claims are ambiguous. It then builds the native runtime, canonical bridge, selected application service sets, industry pilots and conformance ecosystem.

Phase 0 establishes the licensed SAE standards baseline, standards-applicability matrix, JSD and data-product access, claims policy and implementation scope. It also confirms which existing A³O modules can be reused and which must be replaced. The exit criterion is an approved architecture and compliance plan, not merely a collection of documents.

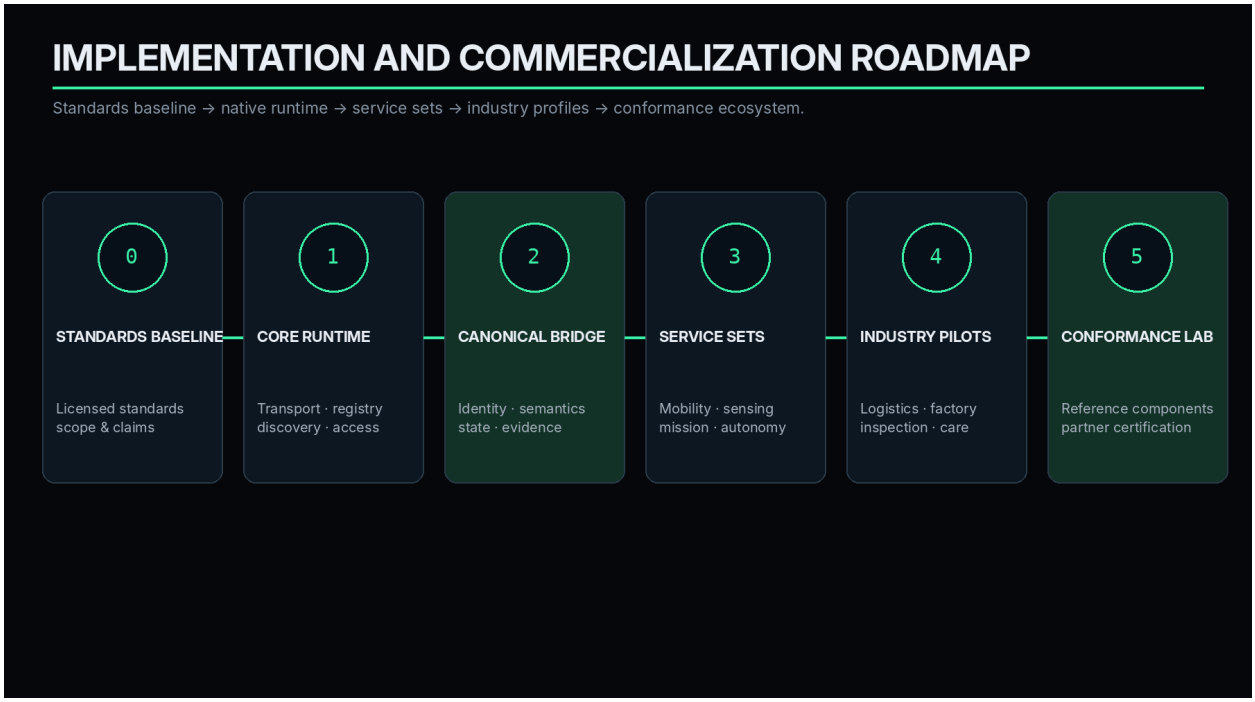
Phase 1 implements the JAUS Core runtime: transport, JSIDL registry, discovery, liveness, time, events, management and Access Control. The phase includes simulators and reference components from the beginning so that behavior is testable. Phase 2 adds canonical identity binding, semantic mapping, state integration, policy, evidence and UI projection.

Phase 3 implements selected mobility, sensing, mission-spooling and autonomous-capability service sets needed by the reference profiles. The objective is not to implement every possible JAUS service before market contact. The team should implement the

smallest coherent subset that validates the architecture across at least two platform types and one degraded-connectivity scenario.

Phase 4 runs industry pilots. Each pilot must include a measurable integration baseline, a new or replaced platform, a defined authority model, operational evidence and an exit decision. The selected pilots should exercise different market and technical dimensions rather than repeating the same security deployment.

Phase 5 establishes the conformance lab and partner programme. Reference components, automated tests, profile fixtures, network impairment, security cases and evidence verification become product assets. The lab supports partner compatibility and prevents the core team from manually validating every deployment.



The implementation roadmap builds a licensed standards foundation before native runtime, application profiles and commercial conformance.

Phase	Workstream	Indicative duration	Exit criterion
0	Standards and architecture baseline	4–6 weeks	Licensed standards, applicability matrix, claims policy and implementation backlog.
1	JAUS Core runtime	8–12 weeks	Transport, registry, discovery, events, management, time, liveness and Access Control.
2	Canonical trust bridge	8–10 weeks	Identity binding, semantic mapping, state, policy, evidence and UI.
3	Application service sets	12–16 weeks	Selected mobility, sensing, mission and autonomy capabilities.
4	Industry pilots	12–20 weeks	At least three profiles, including a non-security multi-vendor deployment.
5	Conformance lab and partners	Continuous	Reference components, automated suites, compatibility matrix and partner programme.

18.1 Investment ask

The working financing scenario is a €6–8 million Seed round supporting approximately 24–30 months of product and market execution. The amount is a management planning assumption and should be updated after engineering estimation, partner discussions and pilot commitments. The round is intended to fund a reusable core and evidence of repeatability, not a portfolio of unrelated custom projects.

The investment programme prioritizes the universal runtime and native JAUS/edge integration. It also funds SDK and connectors, three industry pilots, security and safety engineering, standards licensing, intellectual property, go-to-market and the partner ecosystem. Hiring should concentrate on systems architecture, distributed runtime, protocol and robotics integration, security, verification, product engineering and domain profile leadership.

of funds	Share	Purpose
ersal core runtime	30%	Identity, data/state, policy, mission, evidence and developer platform.

of funds	Share	Purpose
, P2P and edge	20%	Native interoperability domain, distributed operation and partition handling.
and connectors	15%	Partner tools, JSIDL pipeline, adapters, simulators and reference implementations.
e industry pilots	15%	Security/defence reference plus non-security profiles and deployment evidence.
y, security and compliance	12%	Threat controls, assurance, standards licensing and conformance.
TM and partner ecosystem	8%	Patents or know-how protection, partner enablement, sales and category creation.

ne	Evidence
	Licensed standards baseline and frozen R1.2 implementation profile.
	JAUS Core runtime interoperates with reference components in simulation.
	Canonical message, identity, authority and evidence path demonstrated end to end.
	DroneDefender reference profile migrated onto the universal core.
	First non-security multi-vendor pilot completes governed mission and evidence package.
	Partner SDK and conformance suite released to selected integrators.
	Three repeatable industry profiles and first recurring platform revenue.

RESPONSIBLE EXECUTION

19. Risks, Constraints and Claim Discipline

The principal risk is execution breadth. A^{3}O addresses interoperability, trust, orchestration, edge autonomy, AI governance and assurance across several industries. Attempting to implement every service, protocol and profile simultaneously would dilute the product. The mitigation is a strict core-versus-profile boundary, a staged service-set scope and pilot selection that maximizes architectural learning.

Standards access and interpretation are a second risk. Public descriptions are sufficient for strategic architecture but not for a conforming implementation. The company must license the applicable SAE standards and data products, maintain a standards register, track revisions and involve engineers with JAUS implementation experience. Custom services must use explicit A^{3}O namespaces and must never be represented as SAE-standard services.

Interoperability claims are a third risk. The terms certified, SAE-compliant or approved by SAE are prohibited unless the exact scope, issuing body, test evidence and version are identified. Until implementation and test evidence exist, the approved language is JAUS-aligned architecture, JAUS compatibility target and designed for JAUS integration. A^{3}O Certified Profile refers only to the A^{3}O test programme and must not be confused with external certification.

Market claims require similar discipline. The robotics installed base and shipment figures demonstrate growth, but they do not prove the immediately addressable A^{3}O market or the number of JAUS-compatible systems. TAM, SAM, SOM, pricing and sales-cycle assumptions remain management scenarios until independently validated. Investor materials must distinguish public data, management inference and contractual pipeline.

Safety and regulatory scope creates a fourth risk. A^{3}O can provide interoperability, policy, evidence and assurance artifacts, but it does not replace platform safety certification, medical authorization, machinery conformity, aviation approval, maritime classification or defence authorization. Each profile requires a domain assurance plan and clear allocation of responsibility among A^{3}O, the platform vendor, integrator, operator and customer.

Cybersecurity and malicious interoperability create a fifth risk. Discovery, service advertisement, protocol translation, Access Control, time and event subscriptions can be attacked. The architecture responds with identity binding, allowlists, version pinning, schema validation, replay controls, rate limits, lease monitoring, isolation and evidence. Security testing must be part of conformance rather than a separate optional review.

Partner dependence creates a sixth risk. Partners expand reach but can introduce inconsistent mappings, unsupported claims or weak deployment practices. The SDK, profile contract, compatibility matrix, training and test evidence must govern partner delivery. A^{3}O should reserve the right to revoke profile status when a version or implementation no longer meets requirements.

Risk	Failure mode	Primary mitigation

Risk	Failure mode	Primary mitigation
Execution breadth	Platform becomes an unfocused collection of features.	Frozen core, prioritized service sets, profile gates and milestone funding.
Standards licensing	Architecture based on incomplete public information.	Licensed documents, standards register and specialist review.
Compatibility claims	Unverified marketing language damages credibility.	Controlled vocabulary, evidence-based claims and legal review.
Market uncertainty	Large top-down numbers obscure real buying behavior.	Bottom-up pilots, pricing tests and independent validation.
Safety and regulation	Interoperability is mistaken for operational authorization.	Domain assurance plans and explicit responsibility allocation.
Cybersecurity	Malicious or compromised components exploit interoperability.	Identity binding, fail-closed mappings, isolation and security tests.
Partner quality	Inconsistent integrations weaken the platform brand.	Certified profiles, training, regression tests and revocation.
Vendor resistance	Hardware vendors prefer closed ecosystems.	Offer faster market access and preserve vendor implementation freedom.

19.1 Approved claim language

Claim class	Rule
Permitted now	JAUS-aligned architecture; JAUS compatibility target; designed for JAUS integration; native JAUS Interoperability Domain in the R1.2 architecture.
Permitted after implementation evidence	Supports identified JAUS services and versions; passed named A^{3}O conformance tests; interoperated with named reference implementation.
Requires external proof	SAE-certified, approved by SAE, fully JAUS-compliant or equivalent external endorsement.
Always separate	JAUS interoperability versus medical, industrial, aviation, maritime, cybersecurity or defence authorization.

STRATEGIC CONCLUSION

20. Conclusion

Autonomy is becoming infrastructure. The strategic challenge is no longer to build one more capable robot in isolation; it is to make different machines, people and organizations operate together under a trusted and accountable model. Without that layer, the growth of autonomous systems increases integration cost, vendor dependence and operational risk.

A^{3}O addresses the challenge as a Universal Trusted Framework for Autonomous Ecosystems. It establishes identity, semantic contracts, shared state, policy, human authority, distributed coordination, bounded execution and evidence. It works across protocols and industries while preserving platform-specific safety and domain responsibility.

The R1.2 integration of JAUS gives the architecture a formal interoperability foundation for compatible unmanned and robotic components. JAUS supplies platform-independent service definitions, discovery, management, control and message patterns. A^{3}O preserves those semantics and adds the ecosystem-scale functions required for enterprise, civil and strategic operations.

The value proposition is therefore not “another robotics protocol.” It is a stable trust and orchestration layer above changing hardware, autonomy stacks and organizational boundaries. Customers gain reusable integrations, lower vendor lock-in, clearer authority, safer edge operation and evidence that can support acceptance, audit and assurance. Partners gain a common profile and test model. A^{3}O gains a defensible library of mappings, profiles, evidence and conformance assets.

The next proof is implementation. The company must license the applicable standards, build the native runtime, validate the end-to-end message and authority path, migrate the first reference profile and demonstrate a non-security multi-vendor pilot. Success will be measured not by the number of pages or protocols listed, but by whether a new platform can be introduced, governed and replaced without redesigning the mission layer.

FINAL POSITIONING

A^{3}O does not replace JAUS. A^{3}O transforms JAUS and other autonomous-system protocols into one governed, trusted and verifiable operational ecosystem.

ARCHITECTURE MAPPING

Annex A — A3O-1000…9000 Synchronization

This annex connects the strategic whitepaper narrative to the controlled R1.2 Architecture Baseline. The whitepaper explains why the platform exists and how it creates customer and partner value; the baseline defines normative architecture, components, requirements and verification. Where a whitepaper statement conflicts with the baseline, the baseline governs technical implementation.

Series	Controlled scope	Whitepaper relationship
A3O-1000	Foundation, standards alignment and interoperability governance	Compatibility language, standards register, semantic preservation, licensing and governance.
A3O-1200	Semantic and ontology architecture	JAUS-to-A³O terminology, entity model, capability and state semantics.
A3O-1300	Information and data contract architecture	TelemetryEnvelope, canonical messages, provenance, time, quality and versioning.
A3O-1400	Capability and industry profile architecture	Core capability contracts, Industry Profiles and profile inheritance.
A3O-2000	Reference architecture and JAUS Interoperability Domain	Eight governance planes, trust boundaries and native JAUS domain.
A3O-2100	Runtime and edge architecture	Gateway, registry, discovery, events, management, Access Control and partitions.
A3O-2200	Policy, delegation and human authority	Authority mandates, roles, PolicyDecision and control precedence.
A3O-2300	AI and cognitive services	Advisory AI, model identity, validation, drift and command barrier.
A3O-2400	Swarm and distributed coordination	Peer identity, shared state, tasks, topology, partition and reconciliation.
A3O-2500	Safety, resilience and assurance	Safety envelopes, degradation, evidence graph, replay and assurance packages.
A3O-3000	System and component architecture	Software components, service contracts, boundaries and deployment topology.
A3O-4000	Cross-industry solution blueprints	Manufacturing, logistics, inspection, care/response and security/defence.
A3O-5000	Conformance, certification readiness and metrics	J0–J4, compatibility matrix, test families, claim controls and KPIs.
A3O-6000	Governed learning and adaptation	LearningCandidate, release governance, validation and rollback.
A3O-7000	Federated autonomous ecosystems	Organization and ecosystem identity, address scoping and partner trust.
A3O-8000	Extreme, contested and strategic operations	Spoofing, malicious discovery, downgrade, partition and controlled degradation.
A3O-9000	Schemas, SDKs, annexes and test assets	JSIDL tooling, codecs, adapters, simulators, profiles and reproducible releases.

A.1 Strategic-to-technical trace

Whitepaper thesis	Baseline location	Implementation evidence
Universal trusted framework	A3O-1000 / 2000	Architecture principles and eight-plane reference model.
Vendor-neutral interoperability	A3O-1200 / 1300 / 2000	Semantic mapping, canonical contracts and JAUS domain.
Human authority and policy	A3O-2200	Roles, mandates, PolicyDecision and command path.
Edge and swarm autonomy	A3O-2100 / 2400	Partition states, delegation, peer coordination and reconciliation.
Evidence by design	A3O-2500	Evidence fragments, graph, replay, OutcomeAssessment and assurance package.
Governed AI	A3O-2300 / 6000	Recommendation-only boundary, model governance and controlled learning.
Industry profiles	A3O-1400 / 4000	Profile contracts, hazards, workflows and compliance overlays.
JAUS compatibility	A3O-1000 / 2000 / 2100 / 3000 / 5000	Standards alignment, runtime, components and conformance.
Partner ecosystem	A3O-5000 / 9000	SDK, tests, compatibility matrix and reference implementations.
Federated market expansion	A3O-7000	Cross-organization identity, policy and trust exchange.

STANDARDS

Annex B — SAE JAUS Standards Baseline and Public Sources

The standards table reflects public SAE Mobilus titles and public status information verified for the R1.2 baseline on 17 July 2026. It is a planning reference, not a substitute for licensed standards. The implementation team shall maintain a controlled standards register with document licenses, revision history, JSD data products, applicability decisions and responsible owners.

Reference	Public title	Public status	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 Data Distribution Service	Reaffirmed March 2024	10.4271/ARP6227

B.1 Public market and policy sources

Publisher	Source family	Use
International Federation of Robotics	World Robotics 2025 industrial-robot public release	Industrial installations and operational stock indicators used in Section 16.
International Federation of Robotics	World Robotics 2025 service-robot public release	Professional-service and logistics-robot shipment indicators; sample caveat retained.
European Commission	Robotics policy and research pages	Cross-sector relevance across manufacturing, health, transport, security, energy and environment.
European Commission	Connected and automated mobility pages	Convergence of robotics, AI, IoT, HPC, networks, cybersecurity, data, liability and privacy.
SAE International / SAE Mobilus	Public standards scope pages	Titles, scope descriptions, public status and DOI references.

SOURCE DISCIPLINE

Public market figures are contextual indicators. They do not establish the A³O TAM, the installed JAUS base or contractual demand. Management market scenarios require independent validation.

RELEASE TRACEABILITY

Annex C — Change and Traceability Matrix

R1.2 preserves the strategic substance of the R1.0 Candidate whitepaper and expands it with the full JAUS-integrated architecture, implementation boundaries, conformance model, cross-industry detail and claim discipline. Annex D provides the preserved source content so reviewers can verify that the new document expands rather than reduces the prior work.

R1.0 section	R1.2 treatment	Material change

R1.0 section	R1.2 treatment	Material change
Executive thesis	Preserved and expanded	Adds native JAUS domain, implementation boundary and product thesis.
Autonomous ecosystem problem	Preserved and expanded	Adds semantic, authority, partition and evidence failure modes.
Infrastructure category	Preserved	Clarifies universal core versus industry profile.
Operating loop	Preserved and expanded	Adds inputs, outputs, invariants and JAUS command path.
Reference architecture	Expanded substantially	Eight planes, domain components and hard boundaries.
Swarm and edge	Expanded substantially	Communication states, delegated authority and reconciliation.
Data, state and knowledge	Expanded substantially	JSIDL registry, message pipeline, canonical envelope and digital twin.
Governance and safety	Expanded substantially	Authority precedence, roles, safety kernel and regulated-domain boundary.
Use cases	Preserved and expanded	Detailed manufacturing, logistics, inspection, care and security profiles.
Product portfolio	Preserved and expanded	Deployment forms and commercial units.
Business model	Preserved and expanded	Partner, profile, assurance and conformance revenue.
Market	Preserved with controls	Public context separated from management TAM/SAM/SOM scenario.
Go-to-market	Expanded	Reference proof, non-security pilot, SDK, profiles and federation.
Competition and moat	Expanded	Adjacent-category analysis and defensibility assets.
Roadmap	Expanded	Licensed standards, runtime phases, pilot gates and conformance lab.
Investment ask	Preserved and expanded	€6–8M scenario with allocation and evidence milestones.
Risks and claims	Expanded substantially	Standards, certification, market, regulatory, cyber and partner controls.
Sources	Expanded	SAE standards baseline, IFR and European Commission source families.

C.1 Release integrity record

Artifact	Value
R1.0 source file	A3O_Whitepaper_R1.0_Candidate_EN.docx
R1.0 source SHA-256	36b0d134332fb057fe024a867cbcffc99ce00cf2f6bcbbd03bb751c97f35b80d
R1.0 source word count	3,173 words in paragraphs and table cells
R1.2 architecture baseline	A3O_Architecture_Baseline_R1.2_FULL_MASTER_JAUS_Integrated_EN.docx
R1.2 architecture SHA-256	4169238e3379867a94ebc2020a9d44eb808243445744094561af8d7728ce62bc
Preservation method	All non-empty R1.0 paragraph and table content reproduced in Annex D.
Normative precedence	The R1.2 Architecture Baseline governs technical implementation. This whitepaper governs approved strategic positioning subject to controlled review.

SOURCE PRESERVATION

Annex D — Preserved R1.0 Whitepaper Source Content

PRESERVATION NOTE

The following content reproduces every non-empty paragraph and table cell from A3O_Whitepaper_R1.0_Candidate_EN.docx. It is retained for release traceability. R1.2 sections above provide the expanded and controlling narrative.

A³O / UNIVERSAL TRUSTED FRAMEWORK A³O: Universal Trusted Framework for Autonomous Ecosystems Trust, coordination and accountable execution for the autonomous world R1.0 CANDIDATE COORDINATE ANY MACHINE GOVERN EVERY MISSION PROVE EVERY ACTION

DOCUMENT ID	A3O-WP-R1.0-CANDIDATE-EN

DOCUMENT ID	A3O-WP-R1.0-CANDIDATE-EN
DATE	17 JULY 2026
STATUS	CONFIDENTIAL WORKING DRAFT

R1.0 SOURCE

Contents

R1.0 SOURCE

1. Executive thesis

Autonomous machines are moving from isolated products to operational ecosystems. Industrial robots, vehicles, drones, sensors, medical devices, software agents and human supervisors increasingly share the same mission, physical space, data and risk. Yet identity, state, policy, coordination and assurance remain fragmented by vendor and sector.

A^{3}O — Adaptive Autonomous Operations Architecture — is a vendor-neutral trusted operating fabric for heterogeneous autonomous systems. It provides a common layer for identity, universal data contracts, distributed coordination, policy-controlled autonomy, bounded execution and evidence by design.

	CANONICAL POSITIONING A^{3}O is not a robot, sensor platform, fleet manager or command-and-control product. It operates above and between those systems as the trust, coordination and assurance layer for autonomous ecosystems.

R1.0 SOURCE

2. The autonomous ecosystem problem

Problem	Operational manifestation	A^{3}O response
Vendor fragmentation	Robots and platforms expose proprietary APIs, state models and lifecycle semantics.	Canonical contracts, ontology mapping and an industry-profile SDK.
No common identity	Device, workload, operator and organization identities live in separate IAM domains.	Node/workload/human identity, attestation and trust-domain federation.
Central dependency	Loss of cloud or command center causes shutdown	Edge runtime, delegated authority, P2P mesh and

Problem	Operational manifestation	A³O response
	or unsafe improvisation.	safe partition behavior.
Opaque autonomy	AI or optimizers choose actions without explicit policy and safety context.	PolicyDecision, explanation, bounded mandates and a local safety kernel.
No provable outcome	The causal chain and actual physical result cannot be reconstructed.	Evidence graph, signed fragments, replay and assurance packages.
Difficult certification	The solution combines components, versions and vendors.	Conformance profiles, machine-readable schemas and test vectors.

R1.0 SOURCE

3. A new infrastructure category

A³O defines the category Universal Trusted Framework for Autonomous Ecosystems. A shorter commercial label is Autonomous Ecosystem Trust & Coordination Platform. The category is horizontal, while market entry is driven through validated industry profiles.

	UNIQUE VALUE PROPOSITION One trusted coordination standard for heterogeneous autonomous systems: vendor-neutral identity, universal contracts, distributed edge/swarm operation, policy-controlled autonomy and verifiable outcomes.

A common operating model across air, ground, surface, subsea, industrial and software nodes.

A precise boundary between perception, recommendation, authorization and physical execution.

A shared assurance model that survives vendor changes, network partitions and cross-organization federation.

R1.0 SOURCE

4. Universal operating loop

Phase	Purpose
OBSERVE	Acquire telemetry and context.
NORMALIZE	Map data into shared contracts.
UNDERSTAND	Build state and uncertainty.
COORDINATE	Exchange state, capability and intent.
PLAN	Create mission or workflow.
AUTHORIZE	Apply policy, mandate and safety.
EXECUTE	Perform a bounded action.
VERIFY	Confirm the actual outcome.
PROVE	Create signed evidence.
LEARN	Prepare a governed improvement.

The earlier security-specific loop Detect → Fuse → Classify → Authorize → Respond → Prove remains valid as the DroneDefender mission profile. It is now a specialization of the universal loop rather than the definition of the platform.

R1.0 SOURCE

5. Universal reference architecture

Architectural plane	Responsibility
Trust & Identity Plane	Identity for devices, workloads, people and organizations; attestation, trusted time, credentials and trust state.
Data & Perception Plane	Vendor adapters, universal contracts, validation, quality, provenance and time/space normalization.
State & Knowledge Plane	EntityState, process state, world model, operational knowledge, twin synchronization and uncertainty.
Swarm & Coordination Plane	P2P discovery, capability exchange, task allocation, mesh state, partition operation and reconciliation.

Architectural plane	Responsibility
Decision & Policy Plane	Mission planning, AI/cognitive services, policy evaluation, delegated authority and human governance.
Action & Control Plane	Bounded commands, safety interlocks, execution supervision, feedback and outcome verification.
Evidence & Assurance Plane	Append-only records, signatures, evidence graph, replay, verification, audit and certification packages.
Experience & Integration Plane	Operator and engineering UX, SDK, partner portal, API gateway and external enterprise/mission systems.

	ARCHITECTURAL BOUNDARY AI and user interfaces do not directly control physical resources. Every action passes through policy/safety evaluation and an execution supervisor. Authoritative state lives in typed services, not in a visual scene.

5.1 Core component groups

Component group	Representative capabilities
Trust & Identity	Node registry, credentials, PKI, attestation, trusted time, trust scoring and quarantine.
Data & State	Universal adapter gateway, schema/ontology registry, event fabric, state store, fusion, quality and provenance.
Swarm & Coordination	Peer discovery, capability exchange, mesh state, task allocation, topology, partition and reconciliation.
Decision & Governance	Mission orchestrator, workflow engine, cognitive services, policy engine, delegation and resource optimization.
Execution	Action gateway, vendor adapters, local safety interlocks, execution supervisor and feedback.
Evidence & Assurance	Evidence recorder/graph, signing, replay, verification, audit export and assurance packaging.
Twin & Simulation	Operational twin, environment/process model, scenario engine, synthetic data, training and forecast.
Experience & Developer	Operator consoles, authorization UX, SDK, APIs, partner portal and conformance test kit.

R1.0 SOURCE

6. Distributed swarm and edge autonomy

A³O treats P2P and partition-tolerant operation as a normative capability rather than an optional transport mode. Trust is never implied by network proximity, swarm membership or a leadership role. Every peer message carries identity, mission, policy and schema context.

ID	Normative requirement
SWM-001	Every swarm node SHALL possess a verifiable identity.
SWM-002	Every peer message SHALL identify mission, policy and schema context.
SWM-003	Peer loss SHALL NOT automatically expand the authority of remaining nodes.
SWM-004	Local safety constraints SHALL override mission optimization.
SWM-005	Task reassignment SHALL preserve intent, ownership and evidence lineage.
SWM-006	Partitioned operation SHALL use time-bounded delegated authority.
SWM-007	Conflicting state SHALL be retained and reconciled, not silently overwritten.
SWM-008	Collective AI output SHALL remain traceable to participating nodes and evidence.
SWM-009	A compromised node SHALL be isolatable without collapsing the ecosystem.
SWM-010	Swarm reconfiguration SHALL generate an auditable topology event.

6.1 Partition behavior

State	Required behavior
CONNECTED	Normal streaming, synchronization and centralized or distributed optimization.
DEGRADED	Priority traffic, reduced update rate and stricter resource budgets.
PARTITIONED	Local delegated operation within TTL, scope and safety envelope; buffer evidence and state.
ISOLATED	Profile-specific safe fallback with no authority expansion.
RECONCILING	Exchange deltas and evidence, retain conflicts and require review where needed.
RESTORED	Publish reconciliation outcome and resume an approved operating mode.

R1.0 SOURCE

7. Data, state and knowledge architecture

#	Stage	Function	Output
0	Trust Bootstrap	Verify node identity, runtime/firmware attestation, trusted time, policy and mission context.	NodeIdentityContext
1	Acquire	Receive telemetry, event, peer message or human input.	RawTelemetryFrame
2	Normalize	Normalize units, timestamps, coordinate/reference frames and vendor schema.	TelemetryEnvelope
3	Validate	Validate signature, health, calibration, range, privacy and quality.	ValidatedObservation
4	Interpret	Extract an observation, process change, event or operational entity.	ObservationEvent
5	State Estimation	Update the state of a machine, object, process, cargo, environment or patient.	EntityState
6	Local Context	Bind state to mission, workflow, twin, policy and environment.	ContextState
7	Peer Exchange	Exchange state deltas, intent, health and capabilities with trusted peers.	PeerStateDelta
8	Collective Model	Build shared local/world state with uncertainty and conflict markers.	SharedWorldState
9	Intent & Planning	Build mission/workflow plan, resources, constraints and success criteria.	MissionPlan
10	Task Allocation	Assign tasks to nodes, backups or sub-swarms.	TaskAssignment
11	Policy & Safety	Evaluate mandate, roles, risk, ODD, safety envelope, scope and TTL.	PolicyDecision
12	Execute	Issue a bounded, idempotent command through an approved adapter.	ActionCommand
13	Feedback	Receive acknowledgement, telemetry and observed execution state.	ActionFeedback
14	Verify Outcome	Compare objective and result; assess residual risk and uncertainty.	OutcomeAssessment
15	Prove	Create signed evidence fragments/packages with provenance and versions.	EvidenceFragment / EvidencePackage

#	Stage	Function	Output
16	Learn & Synchronize	Prepare a learning candidate; perform governed synchronization and reconciliation.	LearningCandidate / SyncRecord

7.1 Universal telemetry envelope

message_id · source_node_id · source_component_id · ecosystem_id · mission_id timestamp · trusted_time_status · data_modality · semantic_type unit_system · reference_frame · payload · quality · uncertainty classification · privacy_class · schema_version · signature · provenance

Supported modalities include RF, radar, image, video, thermal, LiDAR, sonar, position, velocity, vibration, temperature, pressure, energy, biometric, process state, material state, navigation, manual input and external-system data.

Every derived state preserves source, quality and uncertainty lineage.

Live, simulation, forecast, replay and training namespaces remain distinguishable in data, UX and execution paths.

7.2 Canonical contracts

Contract	Core fields
NodeIdentityContext	node_id, owner_domain, credentials, attestation, runtime_version, trust_state, mission_membership
TelemetryEnvelope	message_id, source_node_id, modality, semantic_type, timestamp, unit, reference_frame, payload, quality, uncertainty, signature, provenance
EntityState	entity_id, state_vector, process_state, uncertainty, lifecycle, source_refs, profile extensions
PeerStateDelta	producer, recipients/scope, vector clock, state changes, quality, conflict markers, evidence refs
CapabilityAdvertisement	capability_id, limits, payload, mobility, energy, compute, communications, workload, safety restrictions, TTL
MissionIntent	objective, priority, constraints, authority, success criteria, termination criteria
MissionPlan	tasks, dependencies, resources, timing, alternatives, policy refs, risk controls
TaskAssignment	task, assignee, backup, lease/TTL, required capability, acceptance state
DelegationGrant	issuer, subject, action scope, resource scope, mission/ODD, TTL, conditions, revocation
PolicyDecision	allow/deny/conditional, reasons, rules, risk, required approvals, evidence refs
ActionCommand	command_id, target, bounded parameters, preconditions, idempotency, expiry, policy decision
ActionFeedback	ack/progress/final state, timestamps, errors, telemetry refs, actual parameters
OutcomeAssessment	objective result, effectiveness, residual risk, uncertainty, side effects, reviewer
EvidenceFragment	event/action refs, hashes, signatures, source versions, classification, retention
SyncRecord	peers, cursors, transferred deltas, conflicts, resolution, authority expiry, resulting state

R1.0 SOURCE

8. Governance, human authority and safety

Level	Operating mode
L0 Manual	A human directly controls the action.
L1 Assisted	AI analyzes and proposes options.
L2 Supervised	The action executes after explicit confirmation.
L3 Delegated	The system acts within a time- and mission-bounded mandate.
L4 Coordinated Autonomous	Multiple nodes coordinate within a policy and safety envelope.
L5 Certified Autonomous Domain	Autonomous execution within a certified operational design domain.

Delegated authority is explicit, scoped, time-bounded, revocable and linked to mission and ODD.

Local safety constraints override mission optimization, remote commands and collective AI decisions.

AI outputs expose model version, evidence references, confidence, intended use and applicable permissions.

A model update never expands authority by itself.

Emergency controls, separation of duties and human escalation are profile requirements, not UI preferences.

R1.0 SOURCE

9. Cross-industry use cases

9.1 MANUFACTURING

Robotic factories, autonomous workshops and flexible production lines

Industrial robots, cobots, AMR/AGV fleets, conveyors, machine vision, MES/SCADA and energy systems operate through one governed mission and state model.

A³O coordinates work cells, separates safety zones, reallocates tasks after failure and produces evidence for quality, maintenance and compliance.

Target outcome: a cross-vendor production cell that preserves policy, safety and traceability as equipment and workloads change.

9.2 TRANSPORTATION & LOGISTICS

Autonomous trucks, delivery drones, warehouses, terminals and port hubs

Unified mission planning connects warehouse robots, transport platforms, cranes, UAV/USV assets and enterprise systems.

Route and energy coordination, multimodal hand-off, geofencing and chain of custody remain available during intermittent connectivity.

Target outcome: safe fleet operation with independently verifiable delivery and custody evidence.

9.3 INFORMATION COLLECTION

Inspection, mapping, geological survey and environmental monitoring

UAV, UGV, USV and UUV assets divide coverage, avoid duplicate routes and adapt to changing environmental conditions.

Edge fusion, calibration status, provenance, gap detection and trusted dataset assembly are built into the workflow.

Target outcome: reproducible linkage between route, sensor, measurement conditions and final analytical conclusion.

9.4 CARE, MEDICAL & RESPONSE

Assistive robotics, evacuation, medical delivery and search-and-rescue

Task prioritization, patient and cargo identity, human escalation, privacy controls and safety envelopes govern every action.

Robots and unmanned systems coordinate in damaged, contaminated or inaccessible environments.

Target outcome: verified chain of custody and a clear boundary between recommendation, authorization and physical action.

9.5 SECURITY & DEFENCE

Protection, contested operations and coordination of autonomous systems

DroneDefender, distributed reconnaissance, logistics, evacuation and defensive operations share identity, policy and evidence semantics.

Positive control, compromised-peer isolation, degraded communications and immutable mission evidence are first-class requirements.

Target outcome: heterogeneous systems cooperate without exceeding delegated authority or local safety constraints.

R1.0 SOURCE

10. Product and deployment portfolio

Module	Purpose
A³O Connect	Node enrollment, identity, adapters, schema mapping and telemetry gateway.
A³O Edge Runtime	Local execution, state, policy, evidence and safe degraded operation.
A³O Swarm	P2P coordination, capability exchange, task allocation and partition management.
A³O Command	Mission planning, operator supervision, authorization and workflow management.
A³O Intelligence	State estimation, prediction, planning and governed cognitive services.
A³O Assurance	Evidence graph, replay, verification, audit and conformance services.
A³O Twin	Operational twin, simulation, scenarios, forecast and training.
A³O Industry Profiles	Ontology, policy, workflow, connector and assurance packs for each sector.

10.1 Deployment patterns

Pattern	Description	Typical context

Pattern	Description	Typical context
Node Embedded	Minimal trust, telemetry, policy and evidence runtime inside a machine or controller.	Robot, vehicle, sensor, gateway.
Edge Ecosystem	Local control plane and event/state services for a site or fleet.	Factory, warehouse, hospital, port, protected site.
Federated Multi-Site	Cross-site trust, policy, state and assurance with ownership boundaries.	Enterprise, public authority, multi-operator network.
Contested / Disconnected	P2P mesh, bounded delegation, safe partition and reconciliation.	Disaster, remote, offshore, defence and degraded communications.
Cloud-Assisted	Global planning, analytics, model lifecycle and partner integrations without cloud dependency for local safety.	Enterprise operations and fleet optimization.

R1.0 SOURCE

11. Business model

Revenue stream	Unit of value
Node Runtime License	Per active node, controller or software agent.
Fleet / Swarm License	Per managed fleet, swarm or mission domain.
Enterprise Ecosystem License	Per site, tenant, organization or federated domain.
Edge Runtime / Appliance	Software subscription or hardened edge platform.
Industry Profile Pack	Ontology, policy, workflow, connector and assurance pack.
Connector / SDK	Commercial adapters, partner SDK, test kit and certification.
Integration & Commissioning	Discovery, adapters, twin, acceptance and safety engineering.
Assurance & Compliance	Evidence dossier, assessment, audit export and conformance services.
Simulation & Training	Scenario packs, engineering/operator training and recurring exercises.
	COMMERCIAL DISCIPLINE Tokenomics is not the core business model. Enterprise, industrial, medical and public-sector procurement requires SLA-backed accountability, auditable licensing, IP clarity and predictable lifecycle cost.

R1.0 SOURCE

12. Market and TAM/SAM/SOM

The market is defined by addressable expenditure on autonomy orchestration, trust and identity, edge runtime, integration, safety, assurance and industry software — not by the total sale value of all robots. Overlapping robotics, vehicle and industrial automation reports must not be added without de-duplication.

Physical deployment scale supports the category expansion: IFR reports 4.664 million industrial robots in operation and 542,000 new installations in 2024; professional service robot sales approached 200,000 units, including 102,900 transport and logistics robots, while medical robot sales reached approximately 16,700 units. [S1-S3]

Metric	Working hypothesis	Method / limitation
TAM	€75-150B annual addressable spend	Global software, edge, integration, cyber-physical safety, assurance and managed-autonomy expenditure. Management scenario, not an independent valuation.
SAM	€8-20B	Europe and partner markets across manufacturing, logistics, critical infrastructure, inspection, emergency response and defence autonomy.
SOM / 5 years	€25-60M ARR	10-20 enterprise ecosystems and 25-60 fleets/sites, with industry-profile and integration attach. Dependent on sales cycles and channels.
SOM / 7-8 years	€75-150M ARR	Scale through certified partners, node/fleet licensing, profile packs and assurance services.

Addressable annual value = active nodes × node fee + fleets/sites × ecosystem license + edge runtime/appliance + integration attach + assurance/profile services

R1.0 SOURCE

13. Go-to-Market

Go-to-market combines a vertical proof point with a horizontal platform. A universal platform without a narrow validation wedge is too abstract; a security-only product does not expose the full platform value.

Wedge 1 — DroneDefender / Security & Defence: the most mature governed mission loop and access to critical-infrastructure pilots.

Wedge 2 — Industrial inspection or logistics: proof of non-security ontology, node/fleet coordination and measurable ROI.

Wedge 3 — Emergency or care logistics: proof of privacy, chain of custody, human escalation and safety governance.

Partner scale — robot OEMs, system integrators, edge/cloud providers, insurers, testing and certification bodies.

Standardization — machine-readable profiles, a conformance kit and reference implementations.

R1.0 SOURCE

14. Competition and defensibility

Category	Usually solves	A³O differentiation
Robot / Fleet Management	One machine class or one vendor fleet.	Cross-vendor, cross-domain ecosystem, policy and evidence.
ROS / Middleware	Communication and software components.	Identity, authority, assurance and industry conformance.
MES / SCADA	Production processes and equipment control.	Distributed autonomous mission, task and swarm layer.
C2 / C4ISR	Command and situational awareness.	Industry-neutral contracts and profiles.
IoT Platform	Telemetry ingestion and analytics.	Governed cyber-physical action and outcome verification.
Digital Twin	Model, visualization and simulation.	Authoritative runtime loop and evidence chain.
AI Orchestration	Models, agents and tools.	Physical safety, delegated authority and execution boundaries.

Canonical autonomy ontology and data contracts.

Trust, identity and delegation fabric for cyber-physical nodes.

Swarm coordination protocols and defined partition behavior.

Operational evidence graph and assurance-case mapping.

Industry profile packs, adapters, conformance tests and simulation corpus.

Field datasets and mixed-vendor deployment know-how.

R1.0 SOURCE

15. Roadmap

Period	Objective	Exit evidence
0-3 months	R1.0 baseline freeze	Ontology, 15 core contracts, SWM requirements, threat model, pilot selection and ADRs.
3-6 months	Universal Core D2	Node identity, telemetry gateway, schema registry, event fabric, state store and evidence fragments.
6-10 months	Distributed Edge	Local runtime, policy/delegation, P2P discovery, state delta and partition tests.
10-14 months	Swarm Coordination	Capability exchange, task allocation, topology events and compromised-peer isolation.
12-20 months	Three vertical pilots	Security/Defence plus Manufacturing/Inspection plus Logistics or Response.
18-24 months	D4 candidate	SLOs, penetration test, safety cases, SBOM, conformance kit and procurement package.
24-30 months	Ecosystem launch	SDK, certified adapters, partner enablement and profile-marketplace model.

R1.0 SOURCE

16. Investment ask

	WORKING ASK €6-8M Seed / 24-30 months to build the Universal Core, distributed edge/swarm runtime and three cross-industry field validations.

Workstream	Share	Result
Universal Core Runtime	30%	Identity, contracts, event/state, policy, execution and evidence.
Swarm / P2P Edge	20%	Mesh, delegated authority, partition/reconciliation and field hardening.
SDK & Connectors	15%	Reference adapters, partner SDK, test harness and documentation.
Industry Pilots	15%	Three vertical pilots with signed KPIs and acceptance evidence.
Security, Safety & Compliance	12%	Threat model, secure SDLC, penetration tests, safety/assurance cases and mappings.
IP, GTM & Ecosystem	8%	Patents/trademarks, partner program, procurement and standardization.

R1.0 SOURCE

17. Risks and claim discipline

Risk	Manifestation	Control
Platform breadth	A category that is too broad without a concrete wedge.	Profile-led GTM and measurable pilot outcomes.
Safety and regulation	Different sectors have different regulatory regimes.	Core plus profile-specific assurance; no universal certification claims.
Interoperability	OEMs may restrict access or semantic depth.	Adapter SDK, conformance tests, partner incentives and sandbox.
Swarm security	P2P operation increases the attack surface.	Attestation, zero implicit trust, topology audit, quarantine and local safety.
Evidence privacy	Assurance can conflict with data minimization.	Classification, selective disclosure, retention and privacy by design.
Market figures	Ranges may be mistaken for published research.	Label as a management scenario and publish assumptions and sensitivity.

R1.0 SOURCE

18. Sources and market reference data

ID	Source	Use
S1	International Federation of Robotics — World Robotics 2025: Industrial Robots	542,000 installations in 2024; 4.664 million operational stock.
S2	International Federation of Robotics — World Robotics 2025: Service Robots	Almost 200,000 professional service robots; 102,900 transport/logistics units in 2024.
S3	International Federation of Robotics — Service Robots Summary	Approximately 16,700 medical robots sold in 2024.
S4	European Commission — Robotics	Robotics applications across manufacturing, health, transport, security, energy and environment.
S5	European Commission — Connected and Automated Mobility	Cybersecurity, liability, data use, privacy and connectivity require coordinated policy and standards.

Source URLs are maintained in the package README and controlled evidence register. TAM/SAM/SOM values are a management model and require a dedicated bottom-up dataset, pricing research and independent validation before public use.

CONTROLLED RELEASE

Document End

End of A³O Whitepaper R1.2 FULL MASTER — JAUS Integrated. Release remains Candidate until strategic, technical, legal, standards-licensing and investment review are complete.