ribbon

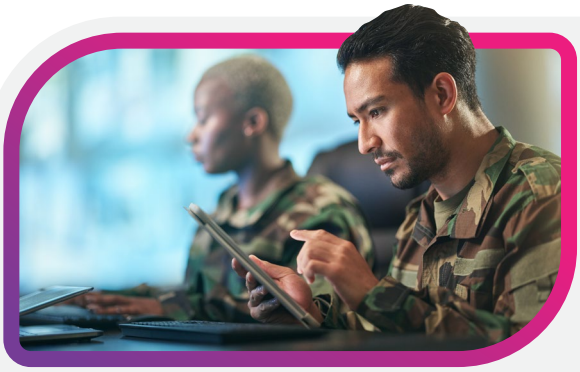
White Paper

OODA (Observe-Orient-Decide-Act) with AI-driven Operations in Assured ISR Networks

Your Path to Autonomonus Networks

Introduction

Intelligence, Surveillance, and Reconnaissance (ISR) traffic is becoming more dynamic, more distributed, and more decisive than ever before. Defense networks must move drone video, sensor telemetry, SIGINT feeds, and targeting updates — while simultaneously sustaining mission voice and Command and Control (C2) — across fixed strategic backbones, operational backbones, and tactical edge aggregation domains. As decisions have to be made as quickly as possible, coping with the enormous amount of information that needs to be "understood" has become the biggest challenge. But fortunately, US Air Force Colonel John Boyd in the Cold War era discovered a model for decision-making in the face of uncertainty.



In the Korean War in the 1950s, American fighters regularly outmaneuvered their North Korean and Chinese counterparts, even though their planes were faster and had more firepower. The victory-to-loss ratio was an astounding — 10:1. Colonel Boyd spent the next decades trying to understand why the F-86 fighter scored such a better ratio against a supposedly superior opponent. The answer was that the American fighters processed information faster than their counterparts, so they were always a step ahead.

Digging deeper, Boyd noticed that decision-making occurs in a recurring cycle: Observe, Orient, Decide, and Act; the famous OODA loop. Cycling through these steps faster than their adversaries enables individuals and organizations to outmaneuver their opponents. The later were still somewhat practicing PDCA (Plan – Do – Check – Act/Adjust), an operational framework for quality control and process improvement, not targeted at agile decision-making and out-maneuvering competition.

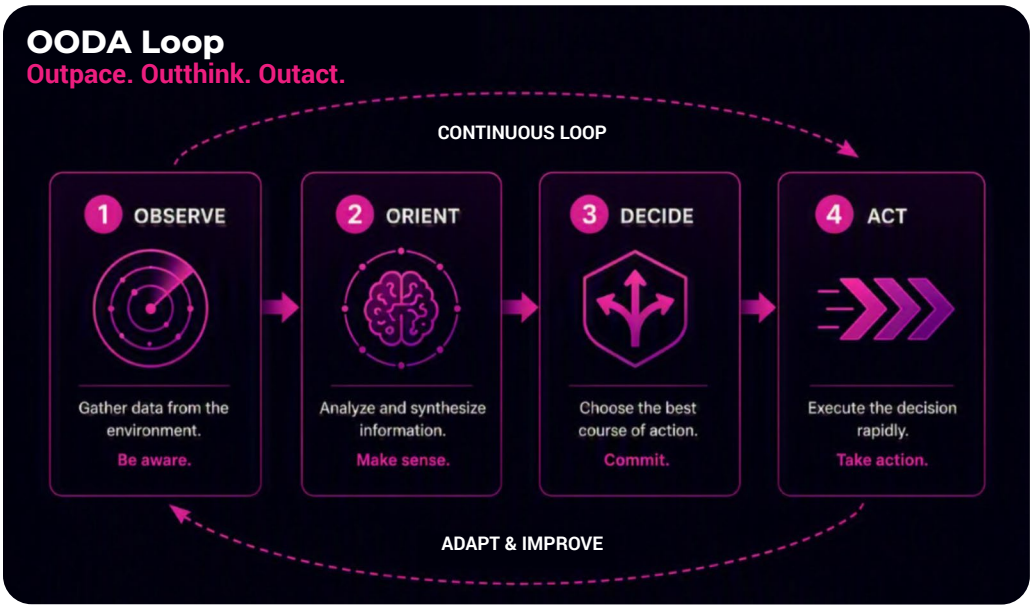


Figure 1 — The OODA Loop

An entity that can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent, can thereby "get inside" the opponent's decision cycle and gain the advantage. Boyd emphasized that the "loop" is in fact a series of interacting loops continuously executed during engagement, and that the phase of engagement strongly influences the ideal distribution of one's energies — a nuance often lost in the popular "loop faster" interpretation.

The OODA Loop

The OODA process is reactive, proactive, and continuous. In Boyd's words, it is a series of interacting loops — not a single sequential cycle — that must be continuously executed. AI-driven operations require high-quality, time-aligned data across all domains. The Observe step is all about gathering it:

Observe

- End-to-end visibility across optical, IP, (voice) services and management-plane telemetry
- Alarms, events, logs, Quality of Experience (QoE), sensor and SIGINT feeds

Orient is the step Boyd called the most important: cultural traditions, history, prior experience, and new analysis are all synthesized here. In an AIOps context, Orient is where topology, Shared-Risk Groups (SRGs), historical baselines, traffic signatures, and mission doctrine combine to interpret the situation. Orient is where raw telemetry becomes understanding:

Orient

- Correlation across layers and Anomaly detection
- Impact prognosis in operational context

In the *Decide* step, the analysis functions take control, like a human being is making up his mind:

Decide

- AI-assisted analysis produces ranked options with risk/benefit and confidence scores

In the final *Act* step, finally the results of the previous steps are causing action:

Act

- Agentic workflows execute approved mitigations through closed-loop automation, with policy-based human-in-the-loop gates
- Outcomes are verified and rolled back if needed

The OODA Loop in AI-driven Operations

By definition, the OODA loop aims to facilitate efficient and reliable decision. The objective is therefore narrow and concrete: reduce noise, accelerate triage, and trigger consistent mitigations — with humans in control as policy requires. Translated into operational language for assured ISR networks, the ultimate result of a successful OODA implementation is fewer, higher-quality alerts; impact prognosis in mission context; ranked options for the operator; and evidence packs for after-action review (AAR).

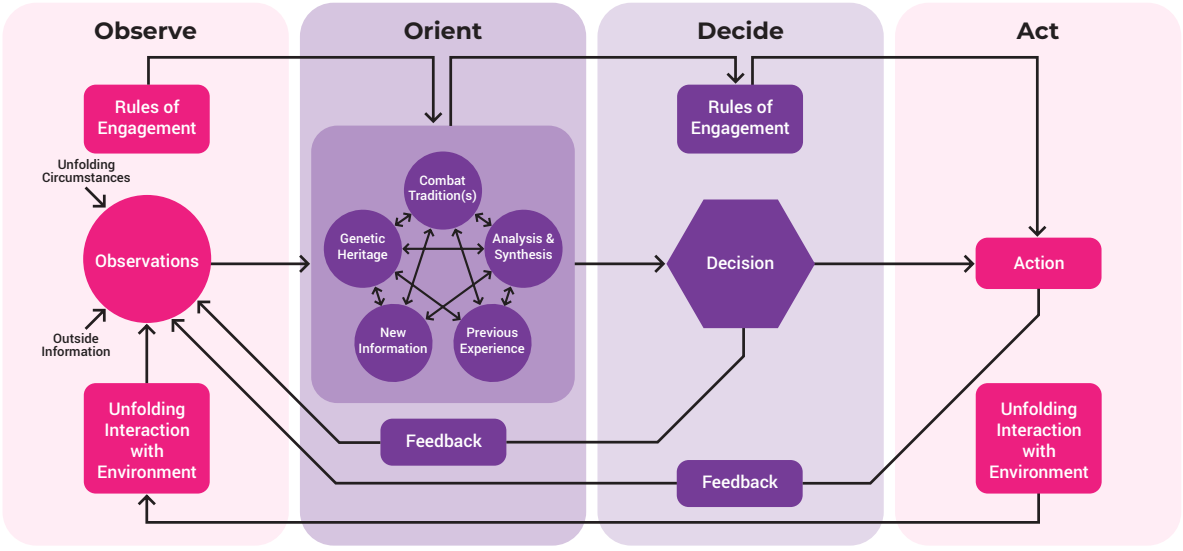


Figure 2 — Automated OODA AIOps Workflow

OODA goes Acumen

AI-enabled "Super-OODA Loops" can compress decision cycles to the max. A specialized AI solution like Acumen is the ideal AIOps tool to provide network-truth at machine speed, targeting the domains depicted below.

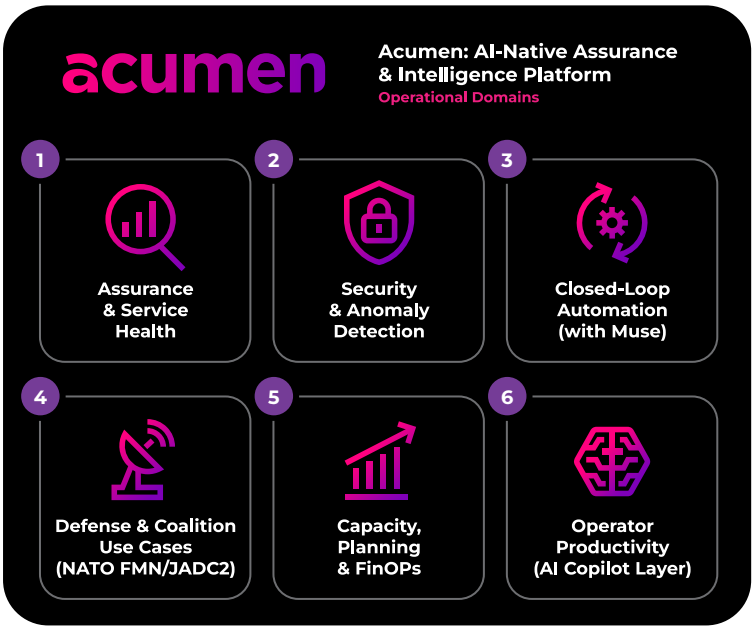


Figure 3 — Operational Domains

The architectural diagram below finally shows how the OODA loop principle is transposed into an AI system.

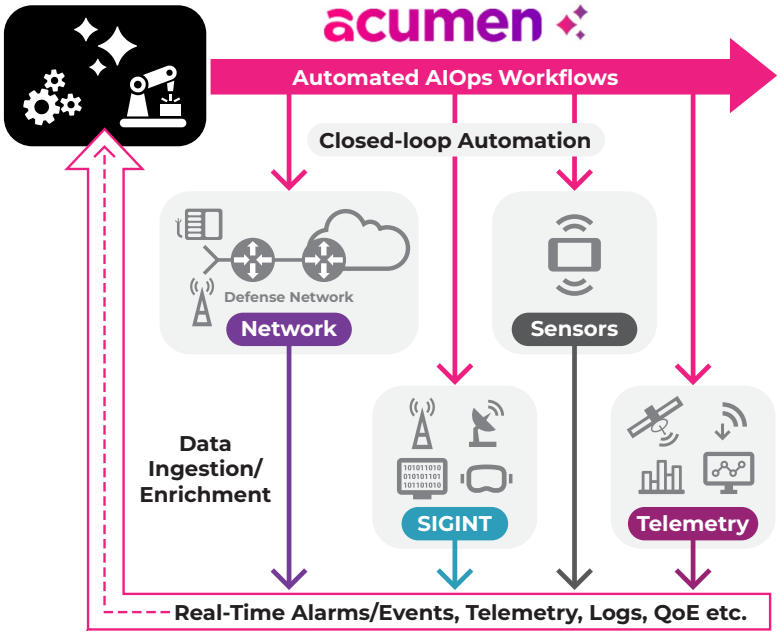


Figure 4 — Automated AIOps Workflow

Ribbon Acumen ↔ Defense & Intelligence Analysis Platforms

Most defense organizations are already working with AI driven Data & Intelligence Analysis Platforms (DIAP). AIOps platforms like Acumen ensure the transport layer remains operational and the data is fused. Feeding into a DIAP (mission-truth), Acumen (network-truth at machine speed) forms the other part of the dual engines of AI-enabled defense networks. Together they deliver command advantage. Acumen collects telemetry, network status, security events, and other information from defense network components. It runs the OODA loop within the network and exchanges data and insight bidirectionally with the Battlefield AI System.

The Battlefield AI Systems then performs higher-order functions on the same evidence base:

- **Global Operational Picture** — fusing network state with the broader mission picture.
- **Threat Detection** — cross-referencing network anomalies with intelligence indicators.
- **Real-time Decision Support** — presenting commanders with mission-ranked options.
- **Mission Analysis** — closing the loop from network event → mission consequence → command decision.

The result is shared situational awareness, faster and more consistent decisions, mission continuity and resilience, and evidence-based command advantage.

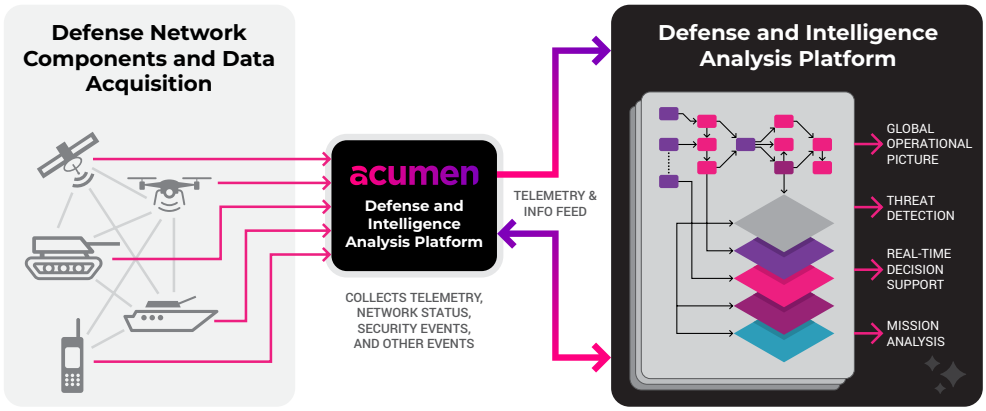


Figure 5 — Ribbon Acumen ↔ Defense & Intelligence Analysis Platforms Integration

Conclusion

The future battlespace rewards those who can Observe, Orient, Decide, and Act faster than the adversary. AI-driven operations enable closed-loop decision cycles that reduce alert noise, improve decision quality, and ensure mission outcomes. By combining end-to-end observability, AI-assisted decision support, and policy-controlled execution, Acumen AIOps helps operators maintain human authority while achieving machine-speed execution, embodying the spirit of Boyd's original framework, which prioritizes agility over raw force. The result is resilient, assured ISR networks that sustain command advantage in contested, coalition environments.

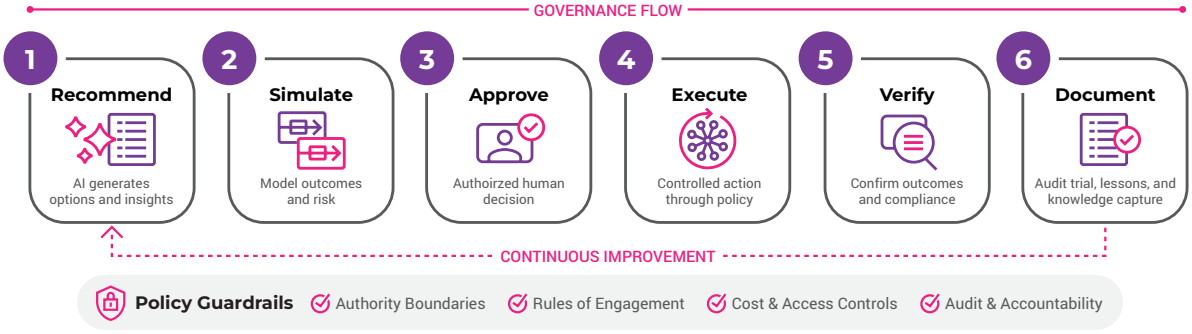


Figure 6 — Core Principles and Governance Flow

AIOps Example Application per Operational Domain

1. Assurance & Service Health

- **Multi-layer fault correlation** correlates alarms across Apollo (optical), Neptune (IP/MPLS-SR), and voice/SBC layers into a single root-cause event.
  — Cuts MTTR by 60–80%; eliminates alarm storms
- **Predictive optical degradation** checks OSNR, BER, pre-FEC trends to predict fiber/amplifier failures hours-to-days ahead.
  — Pre-emptive maintenance; avoids SLA breach
- **Silent failure detection** detects "grey failures" (latency creep, micro-loss) invisible to thresholds
  — Protects mission-critical voice/data flows
- **QoE assurance for voice** measures real-time MOS, jitter, packet-loss scoring per SBC session
  — Defense secure-voice and carrier VoIP assurance

2. Security & Anomaly Detection

- **Behavioral anomaly detection** on control-plane and management-plane telemetry — flags lateral movement, rogue configuration changes, or unexpected BGP/IS-IS events.
- **SIGINT / Sensor-feed fusion** for defense deployments — correlates network telemetry with external threat feeds to surface coordinated cyber-physical attacks.
- **Post-quantum readiness monitoring** — tracks cryptographic posture (e.g., ML-KEM rollout status) across the transport fabric.
- **Insider-threat indicators** — unusual operator command patterns, off-hours config pushes, or privilege escalations.

3. Closed-Loop Automation (with Muse)

- **Auto-remediation playbooks** — Acumen detects → Muse orchestrates (e.g., reroute λ around degrading span, redirect SR-policy, rebalance SBC sessions).
- **Capacity auto-scaling** — predicts congestion on IP/optical links and triggers pre-provisioned capacity activation.
- **Self-healing voice trunks** — automatic SBC failover based on real-time call-quality scoring.
- **Intent-based assurance** — continuously verifies that the deployed network state matches business/mission intent; auto-corrects drift.

4. Defense & Coalition Use Cases (NATO FMN / JADC2)

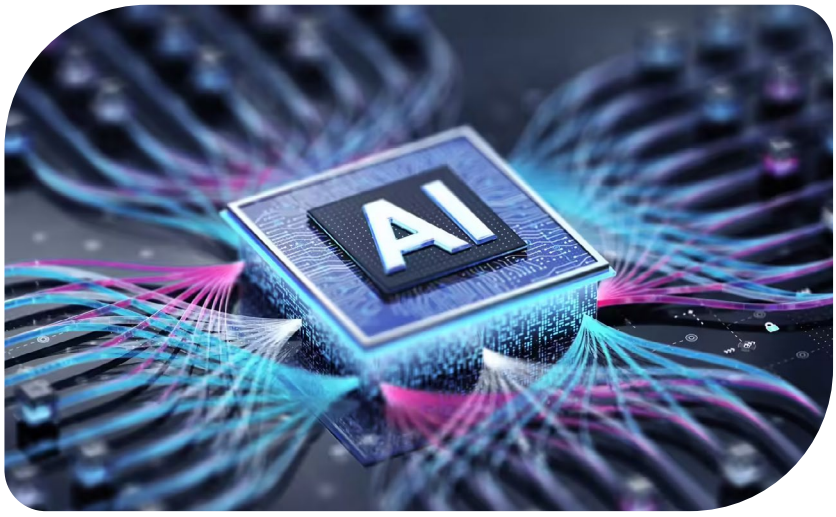
- **Coalition network-truth dashboard** — unified view across multi-national segments respecting data-sovereignty boundaries.
- **Tactical edge health** — monitors deployable nodes (Federal Edge 8300, Tactical Communications Platform) over constrained links; predicts link loss before mission impact.
- **TDM-to-IP migration assurance** — validates legacy-to-IP voice cutover quality in real time during modernization waves.
- **Mission-critical SLA proof** — provides forensic, time-stamped evidence of service performance for after-action reviews.
- **OODA-loop acceleration** — feeds the Observe and Orient phases with machine-speed network truth so commanders NOC act inside the adversary's decision cycle.

5. Capacity, Planning & FinOps

- **Traffic-pattern forecasting** — ML-based growth prediction per service, region, customer segment.
- **What-if simulation** — models impact of new wavelengths, SR-policies, or topology changes before deployment.
- **Energy & sustainability analytics** — per-watt-per-bit reporting across Apollo/Neptune; identifies inefficient cards/links.
- **Asset utilization optimization** — surfaces stranded capacity and over-provisioned circuits.

6. Operator Productivity (AI Copilot Layer)

- **Natural-language NOC queries** — "Show me all degrading 400G links in Kansas over the last 24h."
- **Auto-generated incident summaries** — post-event narratives for management and regulators.
- **Knowledge capture** — converts senior-engineer remediation actions into reusable playbooks.



Glossary

The following definitions clarify the operational, technical, and doctrinal terms used throughout this whitepaper.

AAR (After-Action Review) — Structured post-incident review of mission performance, captured automatically by AIOps as an evidence pack containing telemetry, decisions, actions, and outcomes.

Agentic Workflow — A goal-driven, AI-orchestrated sequence of actions that can plan, execute, and verify steps autonomously within authorized policy boundaries, with human-in-the-loop gates at defined checkpoints.

AIOps (AI for IT/Network Operations) — The discipline and platform that applies machine learning, anomaly detection, correlation, and automation to telemetry from network and service layers to improve operational outcomes.

Anomaly Detection — Statistical and ML techniques that identify deviations from learned baselines, often before conventional thresholds are crossed; the foundation of weak-signal early warning.

Assured ISR Network — A defense network engineered to sustain the mission-critical flows of Intelligence, Surveillance, and Reconnaissance operations (sensor video, telemetry, SIGINT, targeting, C2) under contested conditions and coalition policy constraints.

Blast Radius — The scope of services, sites, missions, or users impacted by a fault, change, or proposed mitigation; central to risk scoring in OODA decision support.

Boyd, John (1927–1997) — US Air Force Colonel and military strategist who developed the OODA Loop. His insight extended beyond "loop faster" to a deeper interaction model — see ooda.de for the original framework as documented by Benjamin Wittorf.

C2 (Command and Control) — The exercise of authority and direction over assigned forces; the most latency- and integrity-sensitive class of traffic on defense networks.

Closed-Loop Automation — An automation pattern in which the system both executes a change and verifies the outcome, rolling back if the change does not achieve the expected effect.

Coalition / FMN (Federated Mission Networking) — A NATO-driven architectural framework allowing partner nations to share information across their respective networks while preserving national caveats and security policies.

Confidence Score — A numerical estimate of how reliable an AI-generated recommendation is, based on signal strength, model uncertainty, and historical accuracy.

Cross-Layer Correlation — The process of linking symptoms observed in different layers (optical ↔ IP ↔ application ↔ service) to identify a common root cause.

Decision Dominance — The operational state in which one's OODA cycle is consistently faster and better-informed than the adversary's, forcing them into reactive postures.

Digital Twin — A continuously synchronized virtual representation of the network that allows "what-if" simulation of proposed changes before they are committed to the live system.

Evidence Pack — A structured archive of telemetry, decisions, actions, and verification data captured during an incident, used for governance, AAR, and continuous improvement.

gNMI / NETCONF — Modern model-driven network management protocols used to stream telemetry (gNMI) or configure devices (NETCONF) using YANG data models.

Human-in-the-Loop — A control pattern in which human approval is required at defined gates before the AI is permitted to execute consequential actions; the policy mechanism that preserves accountability.

Impact Prognosis — The forward-looking assessment of how a current event or proposed change will affect mission services, expressed in mission terms rather than purely technical metrics.

ISR (Intelligence, Surveillance, Reconnaissance) — The integrated activity of collecting, processing, and disseminating information to support military operations.

Mission-Tailored Information — Operational data presented in a form aligned to a specific commander's intent, mission phase, and rules of engagement.

MTTD / MTTR (Mean Time to Detect / Mean Time to Repair) — Two of the most common operational KPIs measuring detection latency and resolution latency; both are directly reduced by AIOps.

Network-in-a-Box (NiB) — A compact, pre-integrated transport-and-services bundle deployable in hours, used for disaster recovery, expeditionary operations, and forward command posts.

OKG (Operational Knowledge Graph) — The unified, time-aligned graph of telemetry, topology, SRGs, services, configuration, and policy that serves as the source of truth for AIOps decision-making.

OODA Loop — Observe → Orient → Decide → Act; John Boyd's decision-making cycle. The OODA model emphasizes that the "loop" is in fact a series of interacting loops continuously executed during engagement (ooda.de).

Orient — The second and, in Boyd's view, the most important step of the OODA Loop. Orient is where raw observation becomes understanding through the combination of culture, history, prior experience, and new analysis. In AIOps, Orient maps to cross-layer correlation, mission-context interpretation, and root-cause hypothesis generation.

Palantir Gotham — A defense and intelligence analysis platform that fuses network-truth (from AIOps) with mission context to deliver global operational picture, threat detection, real-time decision support, and mission analysis.

Policy-Controlled Execution — An execution pattern in which all actions are governed by explicit, machine-readable policy describing who may approve what, under which conditions, and with what evidence requirements.

QoE (Quality of Experience) — A user-perceived metric of service quality (e.g., MOS for voice, video MOS, application response times), used to verify that mitigations achieved their intended effect.

Ranked Options — A prioritized list of mitigation alternatives produced by AIOps, each with associated risk, benefit, confidence, and policy-gate requirements.

RCA (Root-Cause Analysis) — The process of identifying the underlying cause of an observed symptom; in AIOps, RCA is automated through cross-layer correlation and hypothesis ranking.

SIGINT (Signals Intelligence) — Intelligence derived from intercepted communications and electronic signals.

SRG / SRLG (Shared-Risk Group / Shared-Risk Link Group) — A set of network elements that share a common failure mode (e.g., same fiber duct, same power feed, same site); awareness of SRGs is essential for choosing valid mitigations.

SR / SR-TE (Segment Routing / SR Traffic Engineering) — A source-routing forwarding paradigm in IP/MPLS networks (RFC 8660) that encodes the path as an ordered list of segments at the ingress; SR-TE programs the data plane along an intent.

Super-OODA Loop — A term introduced by Michael Raska (RSIS) describing future AI-driven, highly autonomous OODA cycles that operate near machine speed, requiring robust ethical and policy frameworks for responsible deployment.

Telemetry, Time-Aligned — Telemetry data normalized onto a common timebase so that events across optical, IP, service, and management planes can be correlated.

VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) — A German national protective marking equivalent to "Restricted"; commonly applicable to Bundeswehr network and information systems.

Abbreviations

AAR	After-Action Review
AI	Artificial Intelligence
AIOps	AI for IT/Network Operations
BGP-LS	Border Gateway Protocol – Link State
C2	Command and Control
ECMP	Equal-Cost Multipath
FMN	Federated Mission Networking
FMV	Full-Motion Video
gNMI	gRPC Network Management Interface
IGP	Interior Gateway Protocol
INT	Intelligence
IP	Internet Protocol
ISR	Intelligence, Surveillance, Reconnaissance
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
MTTD	Mean Time To Detect
MTTR	Mean Time To Repair
NATO	North Atlantic Treaty Organization
NETCONF	Network Configuration Protocol
NiaB	Network-in-a-Box
OKG	Operational Knowledge Graph
OODA	Observe–Orient–Decide–Act
OTN	Optical Transport Network
QoE	Quality of Experience
RCA	Root-Cause Analysis
RSIS	S. Rajaratnam School of International Studies
SIGINT	Signals Intelligence
SLA	Service-Level Agreement
SNMP	Simple Network Management Protocol
SR	Segment Routing
SR-TE	Segment Routing – Traffic Engineering
SRG/SRLG	Shared-Risk Group / Shared-Risk Link Group
VS-NfD	Verschlusssache – Nur für den Dienstgebrauch
WDM	Wavelength-Division Multiplexing

Contact Us Contact us for more information on Ribbon AIOps and Assured ISR Networks

About Ribbon

Ribbon Communications (Nasdaq: RBBN) is a global provider of voice communications software, IP routing, and optical networking to mobile and wireline service providers, enterprises, critical infrastructure and defense sectors. We support our customers' Path to Autonomous Networks by leveraging the latest AIOps automation platforms and Agentic AI technologies, helping them deliver better customer experiences, reduce operational costs, and achieve sustainable growth. To learn more about Ribbon visit rbbn.com.