BLADE-INFRA-OT Governance Node

Authority-Governed IT/OT Bridge for Cross-Boundary Operational-Technology Command Adjudication

A fail-closed, tier-gated governance appliance applying the AUTHREX pipeline at the IT/OT segmentation boundary

Burak Oktenli

Georgetown University - MPS Applied Intelligence | ORCID: 0009-0001-8573-1667

Version 1.0 | May 2026 | Zenodo Research Paper | DOI: 10.5281/zenodo.20342067

Keywords: authority-governed autonomy, IT/OT bridge, operational-technology security, zero-trust segmentation, Purdue model, ICS/SCADA governance, fail-closed consensus, linear provenance-trust scoring, SATA, HMAA, FLAME, CARA, IEC 62443, NIST SP 800-82, CISA/NSA OT principles, tamper-evident audit ledger

1. Zenodo Deposit Metadata

Field	Value
Title	BLADE-INFRA-OT Governance Node: Authority-Governed IT/OT Bridge for Cross-Boundary OT Command Adjudication
Author	Burak Oktenli | Georgetown University - MPS-AI | ORCID: 0009-0001-8573-1667
DOI	10.5281/zenodo.20342067 | License: CC BY 4.0 | Version: v1.0
Description	Hardware-oriented governance appliance operating as a bump-in-the-wire authority layer at the IT/OT segmentation boundary. Applies the AUTHREX SATA-ADARA-IFF-MAIVA-HMAA-TIMING-FLAME-ERAM-CARA pipeline to cross-boundary OT messages. 48 reference BOM line items, 35 electrical connections, 42 mechanical connections, ~$6,288 bare-parts / ~$14,410 typical-config reference cost. A seeded decision-logic simulator validates governance correctness; physical bring-up and hardware-in-the-loop pending. Hardware TRL 2-3; simulator TRL 3-4.
Hardware	48 BOM line items - 35 electrical - 42 mechanical - ~$6,288 bare-parts (~$14,410 typical config)
Website	burakoktenli.com
Project Page	burakoktenli.com/blade-infra-ot
Simulation	burakoktenli.com/blade-infra-ot-simulation
Related	SATA: zenodo.18936251 - HMAA: zenodo.18861653 - CARA: zenodo.18917790 - FLAME: zenodo.19015618 - BLADE-EDGE: zenodo.19177472 - BLADE-AV: zenodo.19232130 - BLADE-INFRA: zenodo.19277887 - BLADE-SPACE: zenodo.20183269

Table 1. Zenodo deposit fields.

2. Contents of This Deposit

File	Description
blade-infra-ot-zenodo-paper.pdf	This research paper (v1.0). Embedded tables, governance equations, simulation results, and the consolidated findings of nine independent modeling-and-simulation audits applied across five engine revisions.
blade-infra-ot-sim.html	Interactive governance simulator (engine v5.0): four OT scenarios (nominal operation, Monterrey-pattern IT-to-OT pivot, authorized vendor maintenance, multi-utility coordinated probe), seeded Monte Carlo, and external-dataset ingestion. Implements the nine-stage pipeline with a seed-deterministic tamper-evident SHA-256 ledger.
blade-infra-ot_bridge_PARTS.csv	48-line bill of materials with manufacturer part numbers, COTS sourcing, and reference cost.
blade-infra-ot_bridge_ELECTRICAL_CONNECTIONS.json	35 electrical connections (power and data) with net tagging.

File	Description
blade-infra-ot_bridge_MECHANICAL_CONNECTIONS.json	42 mechanical connections: chassis mounting, EMI isolation divider, thermal interfaces, harness routing.
ICD-INFRA-OT-001.pdf	Interface Control Document (Rev A): port map, signal definitions, mechanical envelope, full BOM.
ICD-INFRA-OT_Assembly_Guide.pdf	Assembly, Integration and Test plan: fabrication, wiring, bring-up, qualification with 17 checkpoints.
blade-infra-ot_bridge_SCHEMATIC.svg	Vector schematic of the full hardware architecture (35 electrical edges).
blade-infra-ot_bridge_CONFIG.json	Node and pin-array definitions, Blueprint.am-compatible.
SIMULATION_VnV.md	Verification and Validation record: audit-to-fix traceability and a formal V-001..V-012 test matrix.

Table 2. Deposit file inventory.

3. Abstract

Operational-technology (OT) networks increasingly receive automated and semi-automated commands that cross the information-technology (IT) boundary at timescales below the human supervisory loop. Recent threat reporting documents adversaries pivoting from compromised IT footholds toward OT actuation in critical-infrastructure environments. This paper presents the BLADE-INFRA-OT Governance Node, a fail-closed authority-gating appliance that sits as a bump-in-the-wire layer at the IT/OT segmentation boundary (Purdue level 3 to level 2/1) and computes, per cross-boundary message, how much authority an automated command should hold given current source trust, anomaly evidence, and operational posture. The nine-stage pipeline (SATA → ADARA → IFF → MAIVA → HMAA → TIMING → FLAME → ERAM → CARA, preceded by message ingest and five-feature extraction) reuses approximately 70 percent of the BLADE-INFRA parent design [7] and implements four provisionally patented governance modules: SATA (source-provenance trust allocation), HMAA (per-posture authority thresholds across four distinct tiers T3 to T0), FLAME (cascade prevention with bounded deliberation), and CARA (graduated recovery with a tamper-evident SHA-256 audit chain). The hardware reference comprises 48 BOM line items, 35 electrical connections, and 42 mechanical connections in a 1U fanless enclosure, with a Xilinx Kria K26 governance plane and an Intel Atom x6425E network plane, at a bare-parts reference cost of approximately $6,288 (typical configuration approximately $14,410). All quantitative results in this paper derive from a seeded, deterministic decision-logic simulator with explicit traffic generation, a computed research detector, and fault-injection models; no production deployment, captured OT corpus, or hardware-in-the-loop data is included. Within that simulator the full pipeline reports a system true-positive rate of 0.922 and false-positive rate of 0.026, with the anomaly detector evaluated separately (ADARA-only TPR 0.809, FPR 0.023) so that detector skill is never conflated with the source-roster rule, and an ADARA-only ROC AUC of 0.984 (all from a documented seed). An automated regression harness exercising 35 invariants passed 35 of 35 across three consecutive runs. The same SATA-HMAA-FLAME-CARA governance pipeline is shared across five published platforms (BLADE-EDGE, BLADE-AV, BLADE-INFRA, BLADE-SPACE, BLADE-INFRA-OT), demonstrating architectural portability across defense, automotive, critical-infrastructure, and orbital domains, now extended to the IT/OT bridge.

4. Introduction

4.1 Motivation

Cross-boundary OT command flows occupy a decision regime that conventional segmentation controls address only partially. Firewalls and data diodes at the IT/OT boundary enforce connectivity policy (which hosts may speak which protocols to which targets) but do not adjudicate, per message, whether a syntactically valid command should be permitted given the live trust state of its source and the current operational posture. A command that is policy-permitted can still be operationally illegitimate: issued from a compromised but rostered host, arriving in an anomalous burst, or requesting a high-consequence write while the bridge is operating under degraded trust.

BLADE-INFRA-OT addresses this adjudication gap as an authority layer, not a connectivity-policy replacement.

The case for a dedicated governance appliance, as opposed to interlocks embedded in the historian, PLC, or firewall, rests on three arguments. First, a bump-in-the-wire appliance decouples the safety-critical authority decision from the much larger trusted computing base of the surrounding IT and OT software; only the governance pipeline must be assured to a high standard. Second, a physically separate plane provides a fault-containment boundary: a compromised IT host cannot propagate a cross-boundary command unless the governance node grants authority. Third, the appliance produces a tamper-evident, seed-deterministic audit trail of every adjudication, independent of any single host that the adversary might compromise.

Recent critical-infrastructure threat reporting provides the operational backdrop. Public reporting on a 2025 water-utility incident describes an adversary attempting to pivot from an IT foothold toward OT actuation; the pivot was characterized as failing at the OT layer. BLADE-INFRA-OT is positioned for exactly this class of pivot: a rostered or spoofed-rostered IT source attempting cross-boundary writes that are individually policy-permitted but collectively anomalous. The architecture is anchored to the CISA/ASD-ACSC/NSA principles for OT security (2025) [11] and the Five-Eyes guidance on the careful adoption of agentic AI in OT contexts (2026) [12].

4.2 Scope and Contributions

- Position BLADE-INFRA-OT explicitly as an authority layer at the IT/OT boundary (Section 6.0), complementing rather than replacing firewalls, diodes, and segmentation policy.
- A nine-stage computed pipeline in which every stage gates the terminal decision; no decorative stages remain (Section 6.1).
- Four distinct authority regimes (Section 6.4): T3 autonomous, T2 supervised, T1 confirm, T0 manual-only, with a strictly increasing hold-rate verified in simulation.
- Fail-closed handling of malformed input: a command with missing or out-of-range features is isolated as a data fault, never scored as benign (Section 6.6).
- A decoupled metrics methodology that reports full-system and detector-only detection separately, plus the fraction of detections attributable to the source roster alone (Section 9).
- A seed-deterministic, tamper-evident SHA-256 audit ledger with a CAVP-style boot self-test, and replay-grade traffic export (Section 6.8, Section 9).
- Explicit treatment of governance-layer adversarial failure modes, including roster-spoofed pivots and Byzantine consensus nodes (Section 5.1).
- Four U.S. provisional patent applications shared with the BLADE family: SATA (64/002,453) [1], HMAA (63/999,105) [2], FLAME (64/005,607) [3], CARA (64/000,170) [4].
- Architectural portability evidenced by a shared implementation across five operational domains: defense (BLADE-EDGE [5]), automotive (BLADE-AV [6]), critical infrastructure (BLADE-INFRA [7]), orbital (BLADE-SPACE [8]), and the IT/OT bridge.

5. Threat Model

Threats are identified by cross-referencing the MITRE ATT&CK; for ICS knowledge base [18] with documented OT incidents and the CISA/NSA OT-security principles. The table below covers the governance-layer attack surface at the IT/OT boundary; Section 5.1 addresses adversarial failure modes targeting the governance architecture itself.

Threat	Capability	Effect	Governance Response
IT-to-OT pivot	Rostered IT host compromised	Cross-boundary writes from a trusted source	SATA provenance trust collapses on anomalous gap; ADARA flags burst; HMAA gates high-stakes writes
Roster spoofing	Source impersonates a rostered host	IFF bypass attempt	IFF roster check plus SATA provenance gap; both must pass to propagate
Low-and-slow injection	Sub-threshold malicious writes spaced over time	Evasion of burst detectors	Overlapping benign/malicious feature distributions yield earned false negatives; posture-aware ERAM hold

Threat	Capability	Effect	Governance Response
Command burst / flooding	High-rate cross-boundary writes	Actuation faster than supervision	ADARA burst-rate feature; FLAME inter-event deliberation; TIMING stale-verdict hold
Malformed / fuzzed frames	Out-of-range or missing fields	Score-optimization or crash	Input validation; fail-closed DATA_FAULT isolation; no scoring on garbage
Consensus node compromise	Byzantine governance node	False propagate or false isolate (DoS)	Independent per-node observation; fail-closed on tie; 50% DoS modeled in FMEA
Clock desynchronization	IT/OT time skew	Stale or replayed authority	TIMING stage; time-dependent drift penalty to provenance; monotonic FLAME clock
Audit-chain tampering	Alter a prior adjudication record	Falsified forensic history	Seed-deterministic SHA-256 hash chain; out-of-process verifier; tamper produces a chain break

Table 3. Threat model cross-referenced with MITRE ATT&CK; for ICS and documented OT incidents.

5.1 Governance-Layer Adversarial Failure Modes

Failure Mode	Why It Threatens the Pipeline	Mitigation
Roster-spoofed pivot	A command from a rostered (or spoofed-rostered) IT host passes IFF; if its features sit near benign, it can reach OT.	SATA provenance gap and ADARA anomaly score are computed independently of roster membership; HMAA tier gates high-stakes writes regardless of source legitimacy; the roster-only detection fraction is surfaced so detector skill is never overstated.
Byzantine consensus DoS	A compromised MAIVA node votes to isolate benign traffic, immobilizing the bridge, or to propagate malicious traffic.	Each node forms an independent observation and recomputes its own score; consensus fails closed on a tie (votes x 2 >= nNodes); the Byzantine node is modeled with a 50 percent malicious-flag probability and the honest quorum still governs.
Malformed-input bypass	Missing or out-of-range fields could be coerced to values that imply perfect provenance and a low anomaly score.	validateFeatures flags any malformed field; the terminal decision treats input fault as an immediate isolation cause (DATA_FAULT) and the detector is never scored on coerced values.
Audit-chain corruption	An adversary alters a prior signed entry or splices an alternate chain to hide an adjudication.	Each entry is hash-chained to its predecessor from a seed-deterministic genesis; an out-of-process verifier recomputes the chain and any tampering produces a detectable break that cannot be silently reconciled.

Table 3a. Governance-layer adversarial failure modes with mechanism and mitigation.

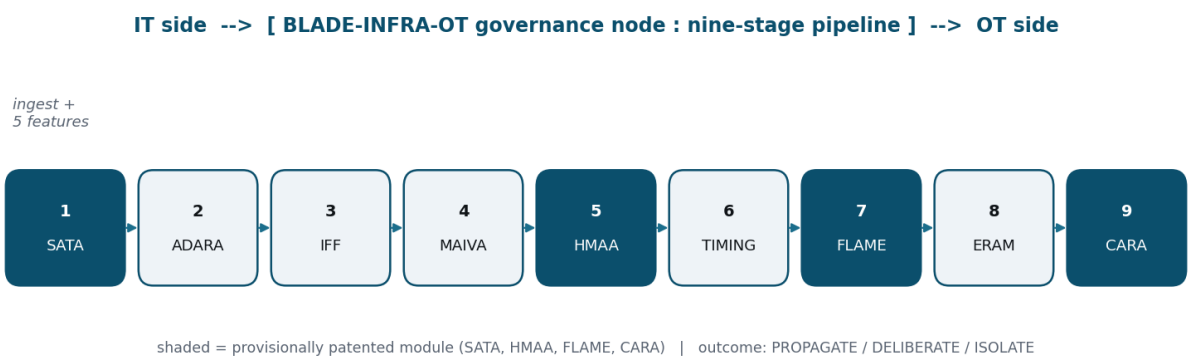

Figure 1. BLADE-INFRA-OT nine-stage governance pipeline at the IT/OT boundary. Shaded stages (SATA, HMAA, FLAME, CARA) are provisionally patented modules shared with BLADE-EDGE [5], BLADE-AV [6], BLADE-INFRA [7], and BLADE-SPACE [8]. Message ingest and five-feature extraction precede stage 1.

6. Governance Architecture

6.0 Position Within the IT/OT Boundary

BLADE-INFRA-OT is an authority layer, not a connectivity-policy replacement. The surrounding security architecture continues to perform its functions: the boundary firewall or data diode enforces which hosts may communicate which protocols; the historian and engineering workstations operate normally; and conventional intrusion detection monitors the segment. BLADE-INFRA-OT intercepts at the message level on the cross-boundary path: for each command crossing from IT toward OT, the pipeline computes an authority decision from current evidence and either propagates the command, holds it for deliberation, or isolates it. Held commands are buffered through the FLAME inter-event window rather than dropped, preserving the operational intent while preventing cascades.

6.1 Pipeline

Stage	Module	Function
1	SATA	Source-provenance trust allocation; trust collapses on anomalous provenance gap (Eq. 1)
2	ADARA	Computed research anomaly detector (logistic model) over the five-feature vector; physics-free, calibration-pending (Eq. 2)
3	IFF	Source-roster authentication; off-roster sources are blocked
4	MAIVA	Independent per-node advisory consensus; fail-closed on a tie
5	HMAA	Authority computation across four posture tiers (T3/T2/T1/T0)
6	TIMING	Inter-plane latency and stale-verdict gate; bus-latency fault inflates verdict age
7	FLAME	Cascade prevention with bounded inter-event deliberation
8	ERAM	Risk escalation; holds elevated-risk traffic under tightened posture
9	CARA	Graduated recovery and tamper-evident SHA-256 audit-chain entry

Table 4. Nine-stage authority-governed pipeline (engine v5.0 order). Message ingest and five-feature extraction precede stage 1 as a pre-pipeline step.

6.2 SATA Source-Provenance Trust

SATA assigns each cross-boundary source a trust score that attenuates as the provenance gap and role mismatch grow. The reference construction (Eq. 1) is monotone and bounded; it is intentionally simple so that the governance decision remains auditable rather than opaque.

$$\tau(s) = \mathrm{clamp}_{[0,1]}\left(1 - 0.7 \cdot \mathrm{provenanceGap} - 0.2 \cdot \mathrm{roleMismatch} - 0.05\right)$$

Eq. (1): SATA provenance trust. A source with tau below 0.60 is treated as untrusted and its commands are isolated.

Under the clock-drift fault, the provenance gap accrues a time-dependent penalty min(1, simTime · 0.00015), so a long-running desynchronization progressively degrades SATA trust rather than applying a single static offset.

6.3 ADARA Computed Detector

ADARA [9] is a logistic model over the five-feature vector. It is explicitly a computed research detector, not a field-validated industrial classifier; its weights are hand-specified and its absolute rates illustrate the architecture rather than field performance (Section 10).

$$z = 2.5\,b + 2.0\,h + 1.8\,r + 2.2\,p + 0.8\,o - 3.2 \;; \quad \mathrm{ADARA} = \sigma(z)$$

Eq. (2): ADARA anomaly score over burst rate b, function-code entropy h, role mismatch r, provenance gap p, off-hours o.

6.4 HMAA Authority Tiers

HMAA gates the terminal decision through four distinct posture regimes. The tiers shape the hold-rate, not the classifier: detection rates are tier-invariant by design, while the fraction of traffic held for human confirmation rises monotonically as posture tightens. This separation is deliberate and is disclosed in the simulator UI.

Tier	Posture	Behavior	Hold-rate (5000-msg batch)
T3	Autonomous	High-stakes clean writes propagate	118
T2	Supervised	High-stakes writes enter deliberation	1767
T1	Confirm	High-stakes plus elevated-risk writes held for confirmation	2123
T0	Manual-only	All operations held for human authority	3752

Table 5. HMAA authority tiers. Hold-rate strictly increases T3 < T2 < T1 < T0 (fixed-tier batch, seed 12345, n=5000).

6.5 MAIVA Consensus and 6.6 Fail-Closed Handling

MAIVA [10] runs an advisory consensus across independent nodes, each forming its own noisy observation of the feature vector and recomputing its own score. Consensus is fail-closed: a tie isolates (votes x 2 >= nNodes). A Byzantine node is modeled with a 50 percent probability of voting to flag benign traffic, exercising the denial-of-service case; the honest quorum still governs the outcome. Malformed input is handled fail-closed: any missing or out-of-range feature flags an input fault, and the terminal decision isolates the message with cause DATA_FAULT before the detector is consulted, closing the score-optimization bypass.

6.7 FLAME, ERAM, and 6.8 CARA Audit Chain

FLAME enforces cascade prevention through a monotonic inter-event delay and a bounded deliberation window; monotonic-clock regression blocks authorized actions until the delay expires. ERAM provides risk escalation that holds elevated-risk traffic under tightened posture. CARA records every adjudication to a seed-deterministic, tamper-evident SHA-256 hash chain whose genesis is derived from the run seed, so a full run replays exactly and any record alteration produces a detectable chain break. The SHA-256 implementation is validated against CAVP-style vectors at boot.

6.9 Design Invariants

- Inv 1: No cross-boundary command propagates without traversing the full nine-stage pipeline.
- Inv 2: Malformed input isolates as DATA_FAULT and is never scored as benign.
- Inv 3: MAIVA consensus fails closed on a tie.
- Inv 4: Authority tiers shape hold-rate with a strictly increasing order T3 < T2 < T1 < T0.
- Inv 5: Every adjudication is recorded to the seed-deterministic tamper-evident SHA-256 chain.
- Inv 6: Detector-only metrics are reported separately from the source-roster rule.
- Inv 7: Traffic export is replay-grade (seed, fault state, threshold, node count, per-message tier before and after).

7. Hardware Platform

BLADE-INFRA-OT is a 1U fanless rack appliance (DIN-rail-adaptable) built entirely from commercial off-the-shelf parts. A Xilinx Kria K26 Industrial system-on-module hosts the governance plane; an AAEON GENE-EHL5 single-board computer (Intel Atom x6425E) hosts the network plane; a Marvell 88E6390X managed switch fabric carries four monitored gigabit paths (IT-IN, OT-OUT, IT-MON, OT-MON). Hardware roots of trust are an Infineon SLB 9670 TPM 2.0 and a Microchip ATECC608B secure element, with an ASPEED AST2500 BMC for out-of-band management. The reference comprises 48 BOM line items, 35 electrical connections, and 42 mechanical connections. Hardware maturity is TRL 2-3; the design is specified to ICD and assembly-guide level and has not been fabricated.

Subsystem	Component	Role
Governance plane	Xilinx Kria K26 Industrial SOM	AUTHREX pipeline fabric (SATA, HMAA, FLAME, CARA)
Network plane	AAEON GENE-EHL5 (Intel Atom x6425E)	Ingest, ADARA, IFF, audit-chain software
Switch fabric	Marvell LinkStreet 88E6390X	Four monitored GbE paths; span/mirror to monitor ports

Subsystem	Component	Role
TPM	Infineon SLB 9670 VQ2.0	TPM 2.0; secure boot measurement
Secure element	Microchip ATECC608B-TFLXTLS	Hardware root of trust; key storage
BMC	ASPEED AST2500	Out-of-band management and health
Primary power	TDK-Lambda CUS100ME-12	AC/DC front end
Secondary power	Vicor DCM3623 (24 VDC in)	Isolated DC bus
Network ports	Amphenol RJ-45 x4 + Bourns PT61018 magnetics	IT-IN / OT-OUT / IT-MON / OT-MON
Point-of-load	TI LM25085 / TPS5450 / TPS5430; ADI LTC3633 / LTC7130	12V / 5V / 3.3V / 1.8V / 1.0V rails
Enclosure	Penn Elcom 1U rack + EMI isolation divider	Fanless 1U; DIN-rail adapter

Table 6. Key hardware components (48 BOM line items total).

7.1 BOM Cost Position

The bare-parts reference cost is approximately $6,288 across the 48 line items; a typical built configuration including the two custom four-layer ENIG printed circuit boards (network motherboard and governance mezzanine), assembly, and test is approximately $14,410. Cost is dominated by the two compute modules (Kria K26 at approximately $3,000 and the Atom SBC at approximately $1,800), which together account for more than three-quarters of the bare-parts total. All line items are COTS and the BOM contains no export-controlled parts.

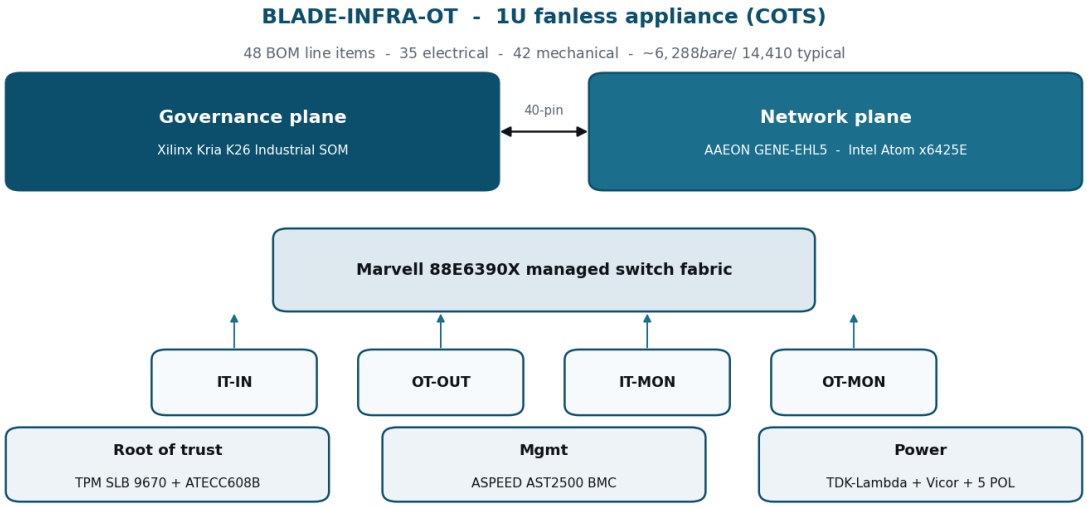

Figure 2. 1U fanless appliance: Kria K26 governance plane and Intel Atom x6425E network plane over a Marvell 88E6390X switch fabric with four monitored GbE paths, hardware roots of trust, BMC, and power. 48 BOM line items.

8. Related Work

Existing IT/OT boundary controls operate at three layers: connectivity policy (firewalls, unidirectional gateways and data diodes), passive monitoring (OT-aware intrusion detection and asset inventory), and protocol enforcement (deep-packet inspection of industrial protocols). These approaches authenticate and constrain connectivity but do not adjudicate, per message, whether a policy-permitted command should hold authority given live source trust. BLADE-INFRA-OT operates at a complementary authority layer. The Simplex monitor-actuator paradigm [17] provides the foundational pattern of a verified safety controller supervising an unverified complex one; BLADE-INFRA-OT extends this with a continuous authority spectrum across four tiers, decoupled detector and roster metrics, fail-closed consensus, and a tamper-evident audit chain, while remaining a research prototype rather than a validated industrial control.

Property	Conventional OT boundary	BLADE-INFRA-OT
Adjudication granularity	Connectivity policy	Per-message authority decision
Authority model	Allow / deny	Four-tier continuous hold-rate (T3-T0)
Detector accountability	Single alert stream	System and detector-only metrics, plus roster-only fraction
Consensus	None / single sensor	Independent per-node, fail-closed on tie
Malformed input	Often dropped or passed	Fail-closed DATA_FAULT isolation
Audit	Telemetry log	Seed-deterministic tamper-evident SHA-256 chain
Portability	Domain-specific	Shared pipeline across five BLADE platforms

Table 7. Differentiation from conventional IT/OT boundary controls. BLADE-INFRA-OT complements, not replaces, these controls.

9. Simulation Methodology and Results

9.1 Simulator Architecture

The BLADE-INFRA-OT simulator (engine v5.0) is a seeded, deterministic decision-logic validator implementing the full nine-stage pipeline. It validates governance correctness; hardware timing and physical behavior are out of scope. Traffic is generated by a seeded mulberry32 stream decoupled from a separate pipeline-noise stream, so changing node counts does not perturb the baseline traffic sequence. Benign and malicious feature distributions deliberately overlap (65 percent bursty, 35 percent low-and-slow) to produce earned false positives and false negatives rather than staged accuracy. All metrics in Section 9.3 derive from a single documented seed (12345) so a reader can reproduce them against the deposited engine.

9.2 Unsafe-Action Definitions

Scenario	Definition of Unsafe Action
S1 Nominal operation	Any benign cross-boundary write isolated without cause (false isolation of legitimate operations).
S2 Monterrey-pattern pivot	A malicious burst write from a rostered-but-compromised source propagates to OT (false propagate).
S3 Authorized maintenance	A legitimate high-stakes vendor write is auto-propagated at T0/T1 without deliberation.
S4 Coordinated probe	An off-roster or bad-provenance probe propagates; or FLAME permits two automated writes within the inter-event window.

Table 8. Per-scenario operational definition of an unsafe action.

9.3 Results

Experiment	System TPR	System FPR	ADARA-only TPR / FPR	AUC	Outcome
S1 Nominal	-	-	-	-	All PROPAGATE at T3
S2 Monterrey pivot	-	-	-	-	Bursts ISOLATE (cause SATA); tier collapses T3 → T0
S3 Maintenance	-	-	-	-	Vendor writes DELIBERATE (FLAME window)
S4 Coordinated probe	-	-	-	-	Probes ISOLATE (cause SATA / IFF)
Monte Carlo (seed 12345, n=5000, thr 0.50, 3 nodes)	0.922	0.026	0.809 / 0.023	0.984	non-ADARA share of detections ~12%

Table 9. Scenario narratives and seeded Monte Carlo metrics. Detector-only rates are reported separately so detector skill is never conflated with the roster rule.

9.4 Verification Harness

An automated Node regression harness exercises 35 invariants spanning the SHA-256 boot self-test, same-seed determinism, tier-causal gating, decoupled detector metrics, fail-closed consensus, fail-closed malformed input, time-dependent clock drift, operator-clearance Time-in-System, Byzantine denial-of-service, and traffic/noise PRNG decoupling. The harness passed 35 of 35 across three consecutive runs. The verification-and-validation record (SIMULATION_VnV.md) contains the full V-001 through V-012 test matrix and the audit-to-fix traceability for the nine independent audits applied across five engine revisions.

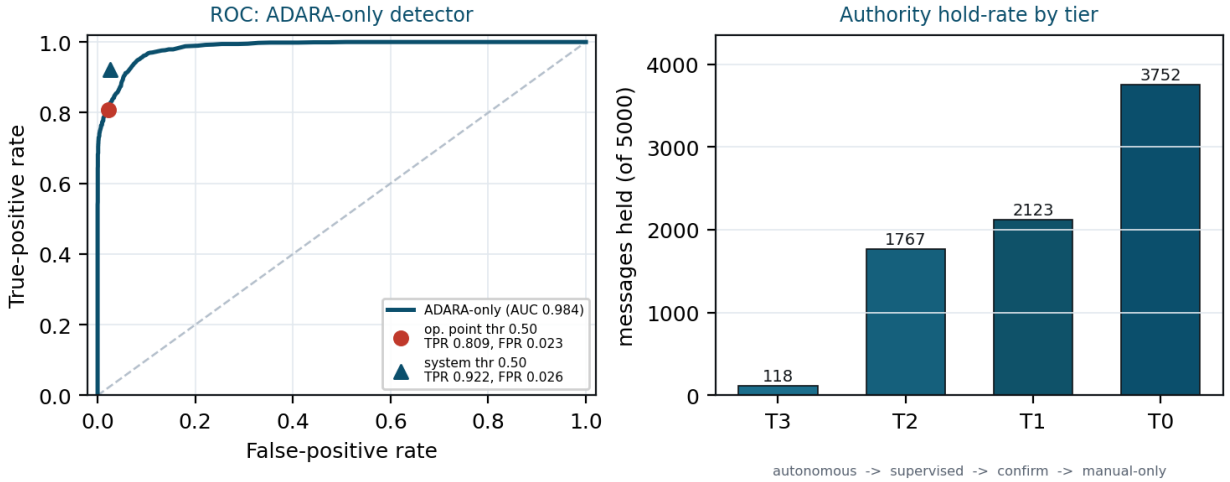

Figure 3. Left: ADARA-only ROC from the deposited engine (AUC 0.984); the circle marks the detector operating point (TPR 0.809, FPR 0.023) and the triangle the full-system point (TPR 0.922, FPR 0.026) at threshold 0.50. Right: authority hold-rate per posture tier, strictly increasing T3 to T0. Seed 12345, n=5000.

10. Known Limitations and Future Work

Limitation	Category	Impact	Path
Simulation-only validation	Scientific	No production OT telemetry	HIL bench with captured OT traffic
Hand-specified detector weights	Scientific	Absolute rates illustrative, not field-calibrated	Calibrate on a cited OT corpus via external-dataset mode
No real protocol-frame parsing	Scientific	Five-feature abstraction only	Add protocol decoders (Modbus/DNP3/OPC UA)
No plant-physics / consequence model	Scientific	Governs decisions, not effects	Add process-state and mission-impact layer
Hardware not fabricated	Engineering	ICD/assembly level only (TRL 2-3)	Fabricate the two four-layer PCBs; bring-up
Ledger tamper-evident, not anchored	Security	Local integrity only	External anchoring / signed bundles
Tiers shape hold-rate, not classifier	Math (disclosed)	TPR/FPR tier-invariant by design	Documented, not a defect

Table 10. Limitations and mitigation paths.

10.1 Implementation Status

Component	Status	Evidence Basis
SATA / HMAA / FLAME / CARA logic	Implemented in simulator	35-invariant harness; 3-run stability
Decoupled detector metrics	Implemented in simulator	System and ADARA-only confusion matrices
Fail-closed malformed handling	Implemented in simulator	DATA_FAULT isolation verified (V-008)
Four distinct authority tiers	Implemented in simulator	Hold-rate T3<T2<T1<T0 verified (V-009)
Tamper-evident audit chain	Implemented in simulator	Seed-deterministic genesis; CAVP boot self-test

Component	Status	Evidence Basis
Hardware platform (48 line items)	Specified in architecture docs	BOM, ICD Rev A, assembly guide, schematic
Custom four-layer PCBs	Not yet fabricated	Specified in electrical/mechanical JSON
IEC 62443 / SIL self-assessment	Not yet assessed	Pending bring-up phase

Table 11. Implementation status as of v1.0.

11. Standards Alignment

The BLADE-INFRA-OT design references the following operational-technology security and engineering frameworks: the CISA/ASD-ACSC/NSA principles for OT security (2025) [11]; the Five-Eyes guidance on careful adoption of agentic AI in OT (2026) [12]; IEC 62443 (industrial automation and control system security) [13]; NIST SP 800-82 (guide to OT security) [14]; the Purdue Enterprise Reference Architecture / ISA-95 zone-and-conduit model [15]; and NIST FIPS 180-4 (SHA-256, validated against CAVP-style vectors at boot) [16]. All BOM line items are commercial off-the-shelf; the deposit contains only architectural and reference-design information and no export-controlled detail.

12. Data Availability

All artifacts are deposited under CC BY 4.0 with DOI 10.5281/zenodo.20342067 (placeholder; final DOI assigned at Zenodo deposit). The deposit includes this research paper (PDF), the interactive simulator (HTML, client-side), the hardware specification files (CONFIG / ELECTRICAL / MECHANICAL JSON, BOM CSV, vector schematic), the Interface Control Document and assembly guide (PDF), and the verification-and-validation record (Markdown).

13. Cross-Domain Ethics Statement

The governance pipeline is architecturally shared with BLADE-EDGE (defense), BLADE-AV (autonomous vehicles), BLADE-INFRA (critical infrastructure), and BLADE-SPACE (orbital). The IT/OT-bridge variant is designed exclusively for protective adjudication of cross-boundary operational commands and contains no offensive capability. Its scenarios are framed as civilian critical-infrastructure protection. The architecture is published as a research prototype to invite scrutiny; the authors make no claim of field validation, regulatory certification, or operational deployment readiness.

14. Version History

Version	Date	Changes
v1.0	2026-05	Initial Zenodo deposit. Nine-stage governance pipeline retargeted to the IT/OT boundary from the BLADE-INFRA parent (~70% reuse). 48-line hardware reference. Four OT scenarios plus seeded Monte Carlo and external-dataset modes. Simulator engine matured across five revisions (v1 through v5) under nine independent NASA/DoD-style M&S; audits: tier-causal gating, decoupled detector metrics, fail-closed consensus and malformed-input handling, four distinct authority tiers, time-dependent clock drift, operator-clearance Time-in-System, replay-grade export, and a CAVP-validated tamper-evident audit chain. Verification harness 35/35 across three runs.

Table 12. Deposit version history.

15. How to Cite

APA: Oktenli, B. (2026). BLADE-INFRA-OT Governance Node (v1.0). Georgetown University. DOI 10.5281/zenodo.20342067.

BibTeX: @techreport{oktenli2026bladeinfraot, author={Oktenli, Burak}, title={BLADE-INFRA-OT Governance Node}, year={2026}, institution={Georgetown University}, version={v1.0}, note={DOI 10.5281/zenodo.20342067}, license={CC-BY-4.0}}

16. References

[1] Oktenli, B. (2026). SATA. Zenodo. doi:10.5281/zenodo.18936251
[2] Oktenli, B. (2026). HMAA. Zenodo. doi:10.5281/zenodo.18861653
[3] Oktenli, B. (2026). FLAME. Zenodo. doi:10.5281/zenodo.19015618
[4] Oktenli, B. (2026). CARA. Zenodo. doi:10.5281/zenodo.18917790
[5] Oktenli, B. (2026). BLADE-EDGE (v5.0.3). Zenodo. doi:10.5281/zenodo.19177472
[6] Oktenli, B. (2026). BLADE-AV (v1.0). Zenodo. doi:10.5281/zenodo.19232130
[7] Oktenli, B. (2026). BLADE-INFRA (v2.0). Zenodo. doi:10.5281/zenodo.19277887
[8] Oktenli, B. (2026). BLADE-SPACE Governance Node (v2.0). Zenodo. doi:10.5281/zenodo.20183269
[9] Oktenli, B. (2026). ADARA. Zenodo. doi:10.5281/zenodo.19043924
[10] Oktenli, B. (2026). MAIVA. Zenodo. doi:10.5281/zenodo.19015517
[11] CISA, ASD ACSC, NSA, et al. (2025). Principles of Operational Technology Cyber Security.
[12] CISA, NSA, FBI, and international partners. (2026). Careful Adoption of Agentic AI in Operational Technology.
[13] International Electrotechnical Commission. IEC 62443: Security for Industrial Automation and Control Systems.
[14] Stouffer, K. et al. (2023). NIST SP 800-82 Rev. 3: Guide to Operational Technology Security. NIST.
[15] International Society of Automation. ANSI/ISA-95 (IEC 62264): Enterprise-Control System Integration (Purdue model).
[16] National Institute of Standards and Technology. (2015). FIPS 180-4: Secure Hash Standard (SHS).
[17] Sha, L. et al. (2001). Using Simplicity to Control Complexity. IEEE Software, 18(4), 20-28.
[18] MITRE. ATT&CK; for ICS Knowledge Base.

Appendix A. Acronym Index

Acronym	Expansion
ADARA	Adversarial Detection and Risk Assessment (anomaly-correlation stage)
AUTHREX	Authority Regulation and Execution (governance framework root)
BLADE	Bayesian Layered Authority for Defensive Engagements (platform family)
CARA	Compositional Autonomy Recovery Architecture (Patent 64/000,170)
CISA	Cybersecurity and Infrastructure Security Agency
DATA_FAULT	Isolation cause assigned to malformed or out-of-range input
ERAM	Escalation and Response Authority Manager
FLAME	Fault-Limited Authority Modulation Engine (Patent 64/005,607)
FMEA	Failure Modes and Effects Analysis
HMAA	Hierarchical Multi-Authority Adjudication (Patent 63/999,105)
IFF	Identification, Friend or Foe (source-roster authentication)
IT / OT	Information Technology / Operational Technology
MAIVA	Multi-Agent Intelligent Voting Architecture
ROC / AUC	Receiver Operating Characteristic / Area Under Curve
SATA	Source/Sensor Authority Trust Allocation (Patent 64/002,453)
TPR / FPR	True-Positive Rate / False-Positive Rate
TRL	Technology Readiness Level