BLADE-CUAS Governance Node

Authority Governance for Counter-Unmanned Aircraft Systems Operations Under Multi-Agency Authority Structures

Burak Oktenli

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

Version 2.0 | May 2026 | Zenodo Research Paper | DOI: 10.5281/zenodo.20299604

License: Creative Commons Attribution 4.0 International (CC BY 4.0)

Keywords: authority-governed autonomy, counter-UAS, C-UAS, Executive Order 14305, Safer Skies Act, FEMA Counter-UAS Grant Program, federal-SLTT, Hierarchical Multi-Attribute Authority, HMAA, evidence chain, Federal Rules of Evidence, Dempster-Shafer, MAIVA, FLAME, ADARA, Remote ID, ASTM F3411, AUTHREX, BLADE, Kria K26, Jetson Orin, FIPS 186-5, ECDSA P-256, NSDD-189

1. Zenodo Deposit Metadata

Field	Value
Title	BLADE-CUAS Governance Node: Authority Governance for Counter-Unmanned Aircraft Systems Operations Under Multi-Agency Authority Structures
Author	Burak Oktenli | Georgetown University, MPS Applied Intelligence | ORCID: 0009-0001-8573-1667
DOI	10.5281/zenodo.20299604 | License: CC BY 4.0 | Version: v2.0
Description	Hardware-enforced authority governance reference architecture for Counter-UAS operations under the EO 14305 multi-agency framework. Nine-stage AUTHREX pipeline with a four-tier HMAA model, Dempster-Shafer multi-modal consensus (MAIVA) across five passive sensor modalities, FRE 901/902/803(6) evidence-chain design, and ADARA Remote ID spoofing detection. 130 hardware components, 65 electrical connections, 117 mechanical connections, approximately $42,811 BOM. No false authorizations observed in 300 simulation runs (95% CI: p < 1.0% aggregate, p < 6.0% per scenario, Rule of Three).
Hardware	130 components / 65 electrical / 117 mechanical / approximately $42,811
Website	burakoktenli.com
Project Page	burakoktenli.com/blade-cuas
Simulation	burakoktenli.com/blade-cuas-sim
Related	SATA: zenodo.18936251 / HMAA: zenodo.18861653 / CARA: zenodo.18917790 / FLAME: zenodo.19015618 / ADARA: zenodo.19043924 / MAIVA: zenodo.19015517 / BLADE-EDGE: zenodo.19177472 / BLADE-AV: zenodo.19232130 / BLADE-MARITIME: zenodo.19246785 / BLADE-INFRA: zenodo.19277887 / BLADE-SPACE: zenodo.20183269

Table 1: Zenodo deposit fields.

2. Contents of This Deposit

File	Description
blade-cuas-zenodo-paper.pdf	This research paper with 10 embedded figures, governance

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

	equations, simulation results, and full reference list.
blade-cuas-simulation.html	Interactive browser-native simulator (v4.0): six scripted C-UAS scenarios plus free-play mode, deterministic xoshiro128** PRNG (128-bit state), synchronous SHA-256 evidence chain over canonical-form serialization for cross-engine determinism, true Dempster-Shafer fusion with Yager high-conflict rule, failure-injection panel, decision-trace replay, and JSON-exportable decision trace.
ICD-CUAS-001-v1.0.pdf	Interface Control Document (approximately 26 pages): 62 SHALL-form requirements, sensor interface specifications, compute architecture, cryptographic subsystem, power and thermal, mechanical, electrical interconnect, BOM, risk register, standards traceability.
BLADE-CUAS-Capability-Brief-v1.0.pdf	Executive capability brief (approximately 8 pages) citing EO 14305, FY26 NDAA Safer Skies Act, and FEMA Counter-UAS Grant Program.
blade-cuas-PARTS.csv	130-component BOM (approximately $42,811) with manufacturer URLs and quantities.
blade-cuas-ELECTRICAL.json	65 electrical connections with protocol annotations and pin mappings.
blade-cuas-MECHANICAL.json	117 mechanical connections with fastener sizes and torques.
blade-cuas-GUIDE.md	Assembly guide with 24 numbered steps including an air-gapped key-provisioning sub-step (3.4a).
blade-cuas-SCHEMATIC.svg	Vector wiring schematic, color-coded by subsystem (data green, power orange).
blade-cuas-CONFIG.json	130 node definitions with complete pin arrays and provenance metadata.

Table 2: Deposit file inventory.

3. Abstract

This paper presents the BLADE-CUAS Governance Node, a simulation-validated, hardware-enforced authority-arbitration reference architecture for Counter-Unmanned Aircraft Systems (C-UAS) operations under the multi-agency authority structure established by Executive Order 14305, the FY26 National Defense Authorization Act Title LXXXVI (Safer Skies Act), and the FEMA Counter-UAS Grant Program. The nine-stage AUTHREX pipeline (SENSE, SATA, ADARA, IFF, HMAA, MAIVA, FLAME, ERAM, CARA) integrates four U.S. provisional patents on a dual-plane Xilinx Kria K26 and NVIDIA Jetson AGX Orin compute architecture. SATA scores per-sensor trust across five passive C-UAS modalities; HMAA implements a four-tier authority model (T3, T2, T1, T0) encoding federal-SLTT handoff; MAIVA performs Dempster-Shafer multi-modal consensus with provenance weighting; FLAME enforces a tier-dependent deliberation window; CARA coordinates authority recovery with a SHA-256 audit chain. ADARA Remote ID spoofing detection cross-checks ASTM F3411 broadcasts against radar kinematics and RF spectrum fingerprints, with RID weighted at 0.15 in MAIVA by default. The evidence chain is designed to meet the foundation requirements of Federal Rules of Evidence 901, 902, and 803(6): every sensor input is ECDSA-signed at acquisition under FIPS 186-5 using a TPM 2.0-resident key, and audit ledger entries are linked via a SHA-256 prev-hash chain with periodic air-gapped anchoring. The reference platform comprises 130 hardware components, 65 electrical connections, 117 mechanical connections, and approximately $42,811 BOM. No false authorizations were observed in 300 simulation runs across six scripted scenarios (95% CI upper bound: $p < 1.0\%$ aggregate; $p < 6.0\%$ per scenario, by Rule of Three). The design is published as fundamental research under NSDD-189 protections. The node is passive on the sensing side (the RF SDR is receive-only) and emits no transmissions in operational role; it contains no mitigation effector and no kinetic aperture.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

4. Introduction

4.1 Motivation

Counter-Unmanned Aircraft Systems (C-UAS) operations have transitioned from a single-agency activity, historically the responsibility of the U.S. Department of Defense in narrow operational contexts, into a coordinated multi-agency activity engaging federal departments and state, local, tribal, and territorial (SLTT) law enforcement. Executive Order 14305 [9], signed 6 June 2025, expanded the C-UAS authority framework and authorized SLTT participation under conditions to be specified by implementing regulations. The FY26 NDAA Title LXXXVI Safer Skies Act [10] (P.L. 119-60, signed 18 December 2025) restructured the Joint Counter-Small UAS Office under Section 912 and codified evidence-chain standards. The FEMA Counter-UAS Grant Program [11] (P.L. 119-21 Section 90005(a)) authorized $500M in FY26 grants to SLTT recipients, with documented operational drivers including the FIFA World Cup 2026, the America 250 celebrations (4 July 2026), and Super Bowl LX.

The commercial C-UAS market, comprising radar, RF spectrum, electro-optical and infrared, and kinetic and non-kinetic effectors, was constructed for single-agency operation. Detection vendors compete on probability of detection, false-alarm rate, and track-confidence metrics. Sensor fusion in commercial products is typically vendor-internal and proprietary; no platform-independent verifiable consensus across vendors is publicly available [19]. None of these primitives provides what the post-EO 14305 environment requires: a governance layer that arbitrates which agency holds authority within a given geofence, computes whether the evidence chain is admissible, and presents tier-appropriate decisions to credentialed human operators.

BLADE-CUAS shares the core governance pipeline architecture with BLADE-EDGE [5] (defense and directed-energy weapons), BLADE-AV [6] (autonomous vehicle drive-by-wire), and BLADE-INFRA [21] (critical infrastructure protection), with approximately 75% architectural reuse from the BLADE-EDGE baseline. The C-UAS variant adapts the platform along four domain-specific axes: (i) five-modality passive sensor ingress (radar, RF, EO and IR, Remote ID, optional LIDAR) replacing single-domain perception; (ii) federal-SLTT authority handoff implemented as a four-tier HMAA extension with explicit T2 (SLTT) and T1 (federal) tier bindings; (iii) ADARA Remote ID spoofing detection that cross-checks ASTM F3411 broadcasts against radar kinematics and RF spectrum fingerprints; and (iv) an evidence chain designed for Federal Rules of Evidence 901, 902, and 803(6) foundation requirements rather than DoDD 3000.09 weapons-release compliance logging. The governance mathematics, namely Dempster-Shafer trust fusion [7][8], HMAA authority computation, FLAME deliberation windows, and CARA recovery phases, are identical across all variants. This shared core supports cross-domain architectural portability.

4.2 Scope and Contributions

This paper makes the following contributions:

- Nine-stage AUTHREX pipeline with five-modality passive sensor ingress (radar, RF SDR, EO and IR, Remote ID, optional LIDAR) and provenance-tagged ECDSA P-256 signing at acquisition.
- Dempster-Shafer multi-modal consensus through the MAIVA stage with provenance weighting and a minimum three-modality release threshold.
- Four-tier HMAA authority model (T3 / T2 / T1 / T0) encoding the federal-SLTT handoff structure of EO 14305, with explicit handoff via a dedicated J9 secure relay interface.
- ADARA Remote ID spoofing detection: cross-modality consistency check against ASTM F3411 broadcasts, with RID weighted at 0.15 in MAIVA by default rather than treated as a primary track source.
- Evidence chain designed to support Federal Rules of Evidence 901, 902, and 803(6) foundation: per-input ECDSA P-256 signing (FIPS 186-5), SHA-256 prev-hash audit ledger, periodic air-gapped anchoring.
- FLAME tier-dependent deliberation windows (default 6 s at T2, 4 s at T1) with policy-driven contraction under multi-track threat density.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

- Two-plane physically isolated compute architecture: Xilinx Kria K26 SOM (governance, FPGA deterministic) and NVIDIA Jetson AGX Orin 64GB (ML and fusion), connected only via three mandatory inter-plane channels.
- Four U.S. provisional patent applications: SATA (64/002,453), HMAA (63/999,105), FLAME (64/005,607), CARA (64/000,170).
- Cross-domain validation across BLADE-EDGE, BLADE-AV, BLADE-MARITIME, BLADE-INFRA, BLADE-SPACE, and BLADE-CUAS.

5. Threat Model

Threats are derived from the commercial C-UAS attack literature [19], the control families of NIST SP 800-53 Rev. 5 [13], and the human-judgment principles of DoDD 3000.09 [12]. Table 3 covers the governance-layer attack surface; detection-side threats such as radar jamming and sensor blinding are the responsibility of upstream detection vendors.

Threat	Capability	Effect	Governance Response
Spoofed Remote ID	Consumer-grade RF transmitter broadcasting arbitrary ASTM F3411 payload	False track provenance	ADARA cross-checks RID against radar kinematics and RF fingerprint; MAIVA caps RID weight at 0.15
No-RID UAS (rogue)	Modified UAS with RID broadcast disabled	Absence of compliance signal	MAIVA classification based on radar, RF, and EO/IR; ADARA missing-RID confidence boost
Coordinated swarm probe	Three or more simultaneous UAS, partial RID, partial profile mismatch	Operator FLAME window saturation, cascade failure risk	FLAME window contracts under multi-track density; HMAA defers to T1; CARA recovery on misclassification
Friendly-fire false positive	Bird flock, weather balloon, news helicopter	Spurious mitigation authorization	MAIVA requires three or more modality consensus; ADARA natural-source classifier; ERAM ROE check
Operator credential compromise	Stolen or phished SLTT or federal mTLS credentials	Unauthorized tier escalation	HSM-bound credentials (NXP EdgeLock SE051); revocation list via federal-tier relay; provisioning attestation
Federal-SLTT handoff race	Federal operator unreachable during T2 to T1 escalation	FLAME window expiration; system returns to T3	Geofence policy expands FLAME window when federal operator is non-resident; ERAM logs the degraded-handoff event
Audit ledger tamper attempt	Online modification of historical decision records	Loss of FRE 901, 902, 803(6) foundation	SHA-256 prev-hash chain detects modification; periodic external air-gapped anchor
Supply chain or firmware trojan	Compromised FPGA bitstream or Jetson model	Backdoored governance logic	TPM 2.0 secure boot; ECDSA bitstream attestation; JTAG lockout post-provisioning
GPS spoofing or time attack	RF injection on L1/L2 GPS bands	Corrupt PTP timestamps	OCXO holdover (planned hardware build); multi-constellation cross-check; ADARA time-consistency monitor
Side-channel or EM fault	Physical proximity attack on FPGA or HSM	Governance bypass via key extraction	Future work: tamper mesh, constant-time RTL; current TPM is FIPS 140-2 L2
Adversarial ML on EO/IR	Patch attack or evasion patterns on commercial drone visual signature	Misclassification of hostile UAS	Future work: adversarial training; physics-based MAIVA fallback prioritizes radar and RF

Table 3: Governance-layer threat model. The last two rows identify threats beyond current TRL 2-3 scope; physical hardware-in-the-loop testing is planned for v2 commissioning.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

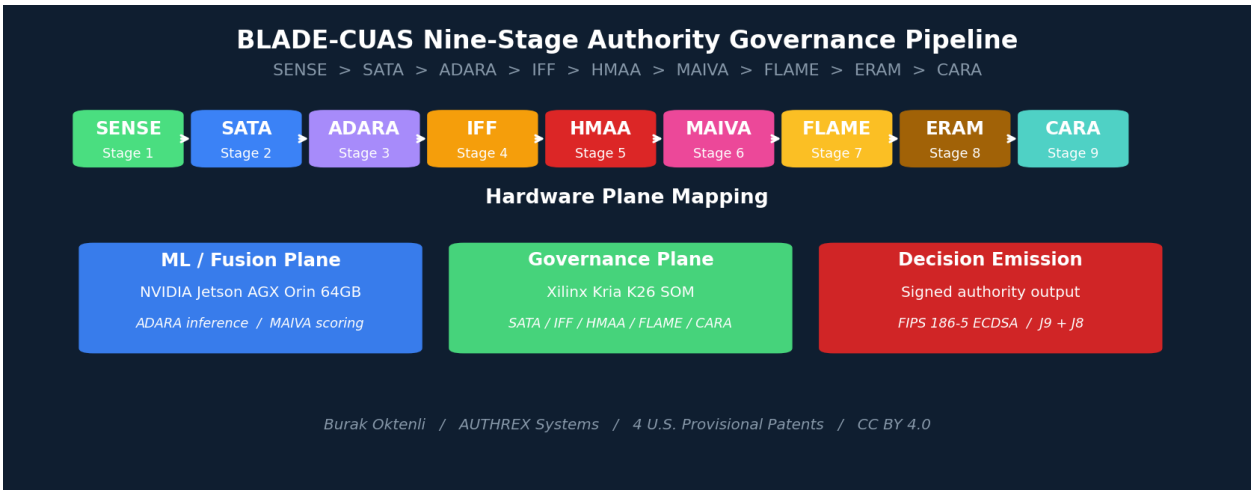


Figure 1: BLADE-CUAS nine-stage authority governance pipeline with hardware plane mapping. The ML and fusion plane (Jetson AGX Orin) executes ADARA inference and MAIVA scoring under the authority of the governance plane (Kria K26 SOM), which holds the AUTHREX pipeline core. The third band shows the signed authority decision emission; the system has no internal effector and only emits decisions to downstream operator consoles (J8 SLTT, J9 federal).

6. Governance Architecture

6.1 Pipeline

Table 4 enumerates the nine pipeline stages with their hardware plane assignment, function, and patent reference where applicable.

Stage	Module	Function	Plane / Patent
1	SENSE	Passive sensor ingestion (5 modalities); ECDSA P-256 signing at acquisition; PTP timestamp	Governance plane
2	SATA	Per-sensor trust score tau in [0,1] from signal quality, sensor health, and recent drift	Governance plane (Patent 64/002,453)
3	ADARA	Cross-modality consistency; Remote ID spoofing detection; natural-source classification	ML plane (Patent pending)
4	IFF	Operator credential authentication via mTLS with HSM-resident identity	Governance plane
5	HMAA	Four-tier authority arbitration (T3, T2, T1, T0); federal-SLTT handoff via FLAME	Governance plane (Patent 63/999,105)
6	MAIVA	Dempster-Shafer multi-modal consensus across three or more modalities; provenance weighting	ML plane
7	FLAME	Tier-dependent deliberation window (6 s at T2, 4 s at T1); contracts under multi-track density	Governance plane (Patent 64/005,607)
8	ERAM	Engagement Risk Assessment: classification severity x collateral proximity x ROE	Governance plane
9	CARA	Coordinated Authority	Governance plane (Patent

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

		Recovery: state revert on misclassification with signed audit entry	64/000,170)

Table 4: Nine-stage authority-governed pipeline. Patent numbers refer to U.S. provisional applications filed March 2026.

6.2 SATA Trust Fusion (Per-Modality)

Frame of discernment: Theta = {Trusted, Untrusted}. Per-sensor basic probability assignment (BPA) construction follows the multisensor data fusion framework of Khaleghi et al. [8]:

$$m_i(\{Trusted\}) = tau(s_i, t) * w_i$$

Eq. (1): Per-sensor trusted mass

$$m_i(\{Untrusted\}) = (1 - tau(s_i, t)) * w_i$$

Eq. (2): Per-sensor untrusted mass

$$m_i(Theta) = 1 - w_i$$

Eq. (3): Residual uncertainty (ignorance)

$$m'_i(\{T\}) = m_i(\{T\}) * C * (1-P);\quad m'_i(\{U\}) = m_i(\{U\}) * C;\quad m'_i(Theta) = 1 - m'_i(\{T\}) - m'_i(\{U\})$$

Eq. (4): Cross-modality validated masses with renormalization

After cross-validation, masses are renormalized so that m'_i({Trusted}) + m'_i({Untrusted}) + m'_i(Theta) = 1. The penalty P reduces only the trusted mass; the untrusted mass is scaled by consistency C but not penalized; residual uncertainty absorbs the difference, preserving total mass.

$$(m1\ (+)\ m2)(A) = (1/K) * Sigma[m1(B) * m2(C)] \quad for \quad B\ intersect\ C = A$$

Eq. (5): Dempster combination rule

$$K = 1 - kappa, \quad where \quad kappa = Sigma[m1(B) * m2(C)] \quad for \quad B\ intersect\ C = empty$$

Eq. (6): Normalization factor K (1 minus total conflict kappa)

K is the normalization factor, not the conflict mass itself. When kappa exceeds 0.65, the system flags a Byzantine condition, meaning conflicting modalities are likely under adversarial manipulation, per Shafer [7].

Modality weights, set with reference to the commercial C-UAS detection literature, are: w_radar = 0.30, w_rf = 0.25, w_eoir = 0.20, w_rid = 0.15, and w_lidar = 0.10. The Remote ID weight is bounded at 0.15 because RID broadcasts are self-reported provenance, and consumer-grade RF transmitters can spoof them. Weight assignment is the author's, made with reference to commercial C-UAS engineering practice; formal weight elicitation via structured expert judgment is planned for the hardware commissioning phase.

The cross-modality consistency coefficient C(s_i, S\{s_i}) is computed as the normalized mean pairwise correlation of measurement vectors across the sensor set, taken over a sliding window of 10 governance ticks. The anomaly penalty P(s_i) is a threshold function: P = 0 under nominal conditions; P = 0.5 when ADARA flags a statistical anomaly (greater than three-sigma deviation); P = 1.0 when confirmed adversarial indicators are detected (for example, impossible radar-to-RID position mismatch).

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

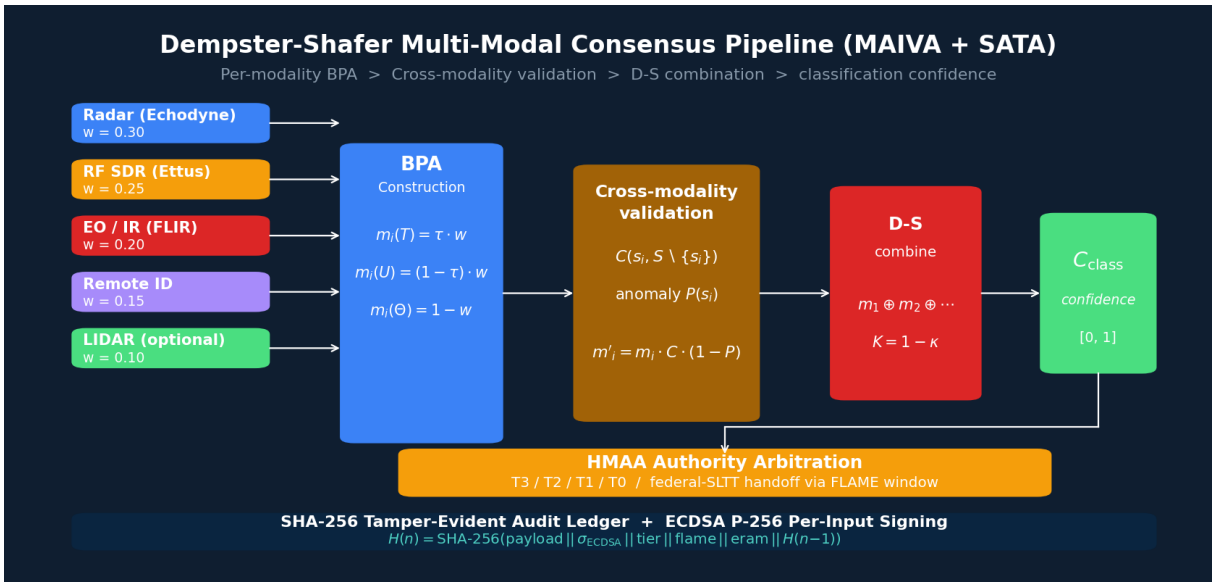


Figure 2: Dempster-Shafer multi-modal consensus pipeline. Per-modality BPA construction with cross-validation, then D-S combination across all five modalities, then classification confidence, then HMAA authority arbitration, and finally an entry in the SHA-256 audit chain.

6.3 HMAA Authority Computation

The authority score alpha quantifies system confidence that mitigation authority should be released at a specific tier. HMAA operates on a separate frame of discernment Omega = {Warranted, Not_Warranted}, distinct from SATA's Theta = {Trusted, Untrusted}. For C-UAS, alpha is computed iteratively across all n active modality evidence sources:

```
alpha = Bel({Warranted}) from h1 (+) h2 (+) ... (+) hn
```

Eq. (7): Iterative per-modality authority computation

where each h_i maps modality i's state to a BPA in frame Omega. For alarm-state modalities, m_i({Warranted}) = (1 - tau_i) * r and m_i({Not_Warranted}) = tau_i * r. For nominal-state modalities, the same formula applies and produces a low {Warranted} mass naturally. The factor r = 1 - dynIgn, where dynIgn = min(0.30, 0.05 + 0.03 * (5 - min(n_modalities, 5))) is the dynamic epistemic ignorance, which scales with the active modality count. Fewer modalities yields higher ignorance and a more conservative authority decision.

Implementation safety guard: alpha is truncated to four decimal places via floor(alpha * 10000) / 10000, preventing floating-point rounding into authorization. This is an implementation constraint, not a mathematical property of the D-S fusion.

6.3.1 Authority Tier Bindings

Tier	Name	Operator Class	Mitigation Authority	FLAME Window
T3	Autonomous Monitoring	None (autonomous)	None; track and log only	n/a
T2	Supervised, SLTT Tier	Sheriff, state police, stadium security	Operator CONFIRM within FLAME window	6 s (default)
T1	Confirmed, Federal Tier	DHS, DOJ, military per EO 14305	Explicit federal confirmation required	4 s (default)
T0	Manual	Test, calibration, or suspected compromise	Full human control; system halted	n/a

Table 5: Four-tier HMAA authority bindings. Tier transitions occur only on (a) operator action, (b) MAIVA classification change, or (c) policy-defined trigger.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

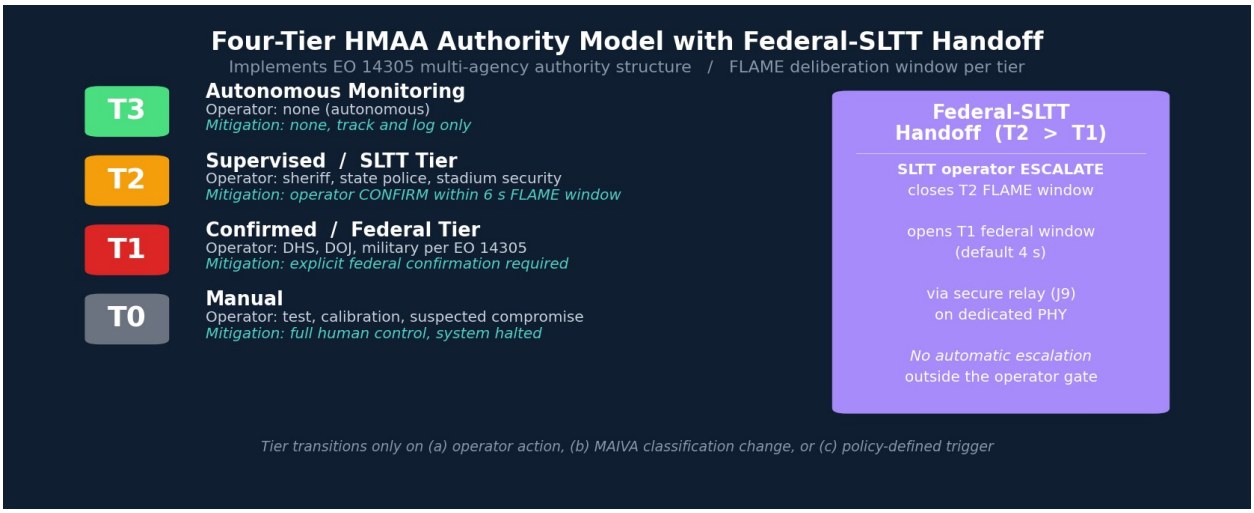


Figure 3: Four-tier HMAA authority model with federal-SLTT handoff. On an SLTT operator ESCALATE action at T2, the system transitions T2 to T1, closes the SLTT FLAME window, and opens a federal FLAME window (default 4 s) presented to the federal-tier operator via the J9 dedicated secure relay PHY.

6.4 MAIVA Multi-Modal Consensus

MAIVA (Multi-Agent Intelligent Voting Architecture, [18]) provides Dempster-Shafer combination across the active modalities. Unlike the BLADE-INFRA application, in which MAIVA is advisory, in BLADE-CUAS the MAIVA consensus directly gates the HMAA classification: a minimum of three modalities reporting above their SATA threshold (default tau >= 0.40) is required before any non-T3 tier release. This three-modality consensus floor is the primary defense against single-modality false positives. For example, a spoofed RID alone cannot drive a T2 escalation because at least two corroborating modalities, typically radar and RF, must also classify the track as a hostile UAS. MAIVA outputs are logged to the SHA-256 audit chain along with the active geofence policy version.

6.5 FLAME Gate and ERAM Escalation

FLAME enforces tier-dependent deliberation: (a) the operator must respond within the active window (default 6 s at T2, 4 s at T1); (b) no simultaneous multi-track mitigations within the same geofence; (c) the window contracts when the count of simultaneous non-commercial tracks exceeds the geofence policy threshold (default: the window halves at three or more tracks). All timing uses a monotonic clock with ECDSA-signed PTP timestamps to prevent adversarial clock manipulation.

ERAM (Engagement Risk Assessment Model) operates independently of HMAA. ERAM computes an engagement risk score in [0, 1] combining classification severity (from MAIVA), collateral proximity (geofence policy distance to non-target assets), and operator certainty (recent action history). Three escalation levels exist: LEVEL_1_AUTO (normal T3 or T2 operation), LEVEL_2_SUPERVISOR (out-of-band alert when risk is MEDIUM or HMAA defers), and LEVEL_3_OPERATOR (mandatory federal confirmation when risk is HIGH or Byzantine conditions are detected by SATA conflict kappa > 0.65). ERAM is independent: even if HMAA authorizes actuation, HIGH risk forces LEVEL_3 confirmation.

6.6 CARA Recovery

Phase	Trigger	Action
Sensor Revalidation	Modality dropout or track loss	Re-poll active modalities; cross-validate; recompute SATA trust vector
Partial Restoration	Trust recovering on two or more modalities	Re-enable monitoring; hold tier at T2 ceiling pending federal review
Full Recovery	Sustained trust above SATA threshold across three or more modalities	Restore tier to T3; emit signed full-recovery audit entry
Manual Override	T0 operator intervention	Authenticated reset; FRE-foundation

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

		audit entry logged with credential identity

Table 6: CARA recovery phases. State transitions are logged to the SHA-256 prev-hash chain with PTP timestamps.

6.7 Design Invariants

- Inv 1: No authority decision is emitted without traversing all nine pipeline stages.
- Inv 2: Below the active tier threshold, the decision defers to a credentialed human operator within the FLAME window.
- Inv 3: FLAME prevents simultaneous mitigation authorizations within the same geofence.
- Inv 4: CARA recovery phases are mutually exclusive at any point in time.
- Inv 5: All decisions are recorded in the SHA-256 prev-hash audit chain with PTP-disciplined UTC timestamps.
- Inv 6: HSM cryptographic operations (TPM SPI, Secure Element I2C) are reachable only from the governance plane; the ML plane has no bus path to crypto.
- Inv 7: The federal-tier J9 secure relay is on a dedicated PHY; J8 SLTT and J9 federal cannot share a fabric.
- Inv 8: On any FLAME window expiration without operator action, the system returns to T3 (autonomous monitoring); no automatic escalation occurs outside the operator gate.

7. Hardware Platform

Dual-compute reference platform: NVIDIA Jetson AGX Orin 64GB Developer Kit and Xilinx Kria K26C System-on-Module (Zynq UltraScale+ MPSoC) on a custom carrier board within a MIL-STD-810G transportable case (550 mm W by 420 mm D by 240 mm H, 22 kg typical). The platform comprises 130 hardware components, 65 electrical connections, 117 mechanical connections, and approximately $42,811 BOM at the reference configuration. External rating is NEMA 4X; MIL-STD-461G EMI compliance is targeted; MIL-DTL-38999 circular connectors are used for all external interfaces.

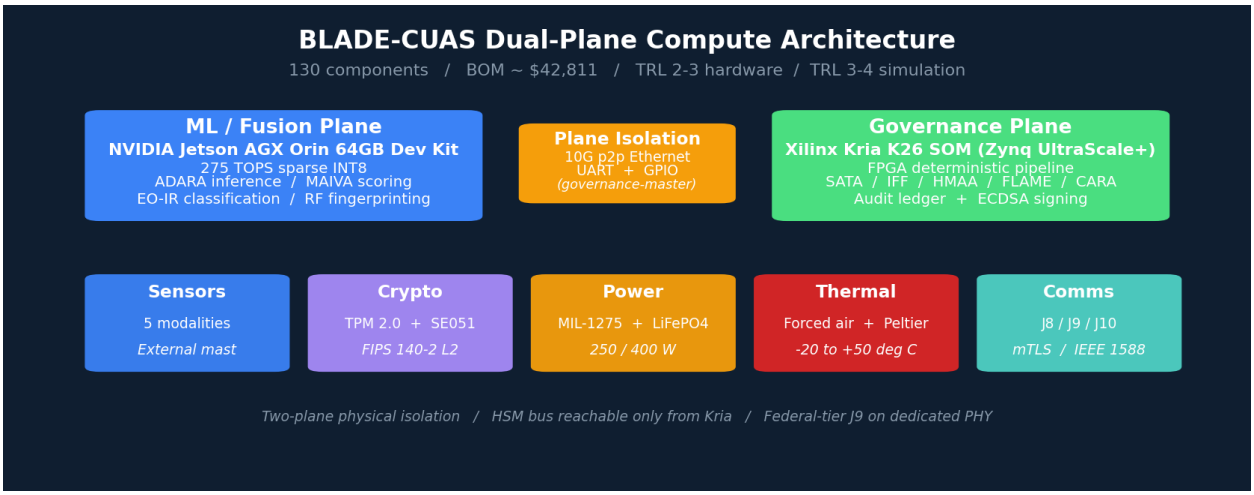


Figure 4: BLADE-CUAS dual-plane compute architecture. The two compute planes are physically isolated and communicate only via three mandatory inter-plane channels: a hardware UART (governance-master), a dedicated point-to-point 10GBASE-T Ethernet link (PTP IEEE 1588 disciplined), and a unidirectional GPIO power-isolate line from the Kria FPGA to the Jetson 12 V rail.

Subsystem	Component	Interface	Role
Governance plane	Xilinx Kria K26C SOM + KR260 carrier	PCIe / SPI / UART / GPIO	AUTHREX pipeline; SATA / IFF / HMAA / FLAME / CARA; audit ledger; ECDSA signing supervision
ML / fusion plane	NVIDIA Jetson AGX Orin 64GB Dev Kit	PCIe / USB 3.0 / MIPI CSI-2 / 10GbE	ADARA inference; MAIVA scoring; EO/IR classification; RF protocol fingerprinting
Radar	Echodyne EchoGuard CR	1000BASE-T Ethernet	Metamaterial scanning radar;

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

			UDP track stream at 10 Hz or above
RF SDR (receive-only)	Ettus B205mini-i with antenna array and LNA	USB 3.0 to ML plane	Drone control-link fingerprinting; RID broadcast verification
EO / IR	FLIR Boson 640 LWIR + Sony IMX585 + 2-axis turret	USB 3.0 + MIPI CSI-2	Visual classification; night thermal contrast; 30 fps each channel
ADS-B / RID	uAvionix pingRX Pro	UART 3.3 V TTL	ASTM F3411-22a Remote ID + Mode-S/ADS-B
LIDAR (optional)	Livox HAP solid-state	1000BASE-T Ethernet	Close-in classification; MAIVA weight 0.10
Cryptographic subsystem	Infineon SLB 9670 TPM 2.0 + NXP EdgeLock SE051	SPI + I2C from Kria only	ECDSA P-256 signing (FIPS 186-5); operator credentials; federal-tier handoff keys
Power	MIL-STD-1275 28 V + LiFePO4 280 Wh hot-swap	Vehicle bus + battery	250 W typical, 400 W peak; ~70 min battery runtime
Thermal	3x sealed 80 mm intake fans + 2x Peltier exchanger	PWM control	-20 to +50 deg C ambient; +60 deg C transient under 20 min
Timing	u-blox LEA-M8T multi-band GPS with TCXO + PPS	UART + GPIO PPS	UTC discipline; PTP IEEE 1588 master between planes
External connectors	12x MIL-DTL-38999 + 1x IEC C14 + 1x SMA	J1-J12 per ICD	Vehicle DC and AC, sensors, operator, federal relay, audit anchor, service, GPS

Table 7: Key hardware components (130 total).

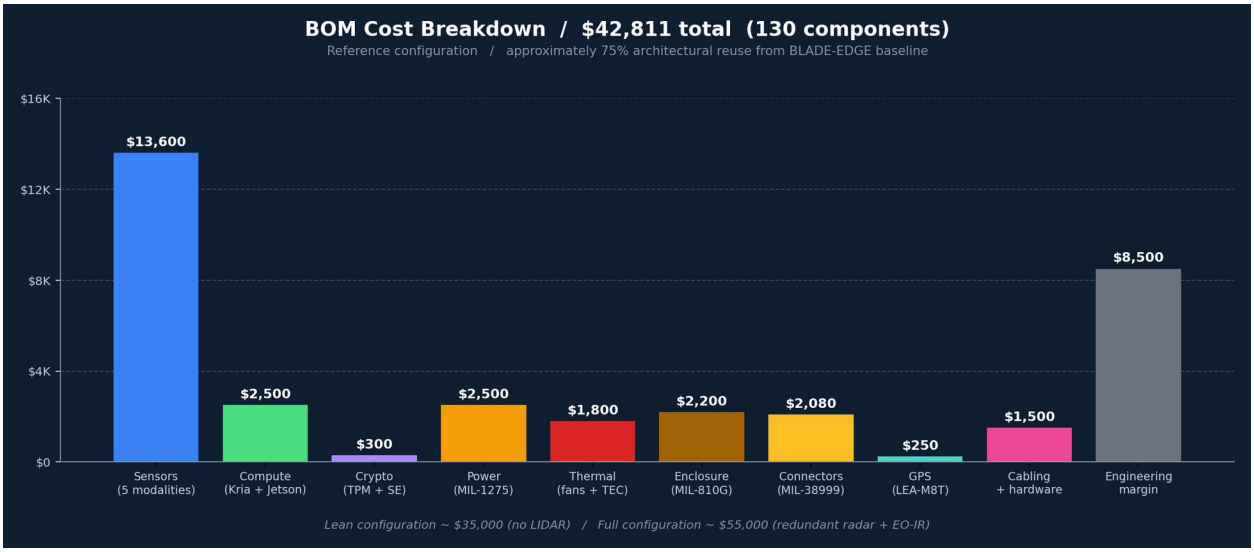


Figure 5: BOM cost breakdown by subsystem. Total $42,811 at the reference configuration. A lean configuration without LIDAR comes in near $35,000; a full configuration with redundant radar and EO-IR comes in near $55,000.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

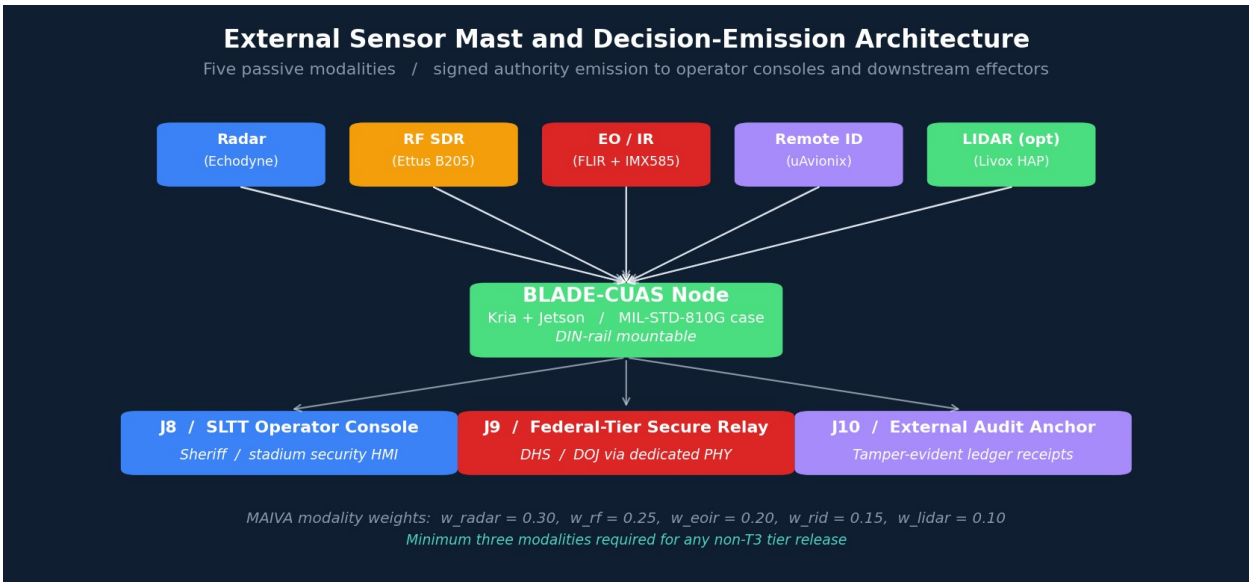


Figure 6: External sensor mast and decision-emission architecture. The five sensor modalities are mounted externally on a co-located sensor mast; they are not inside the enclosure. Authority decisions are emitted to three distinct downstream consumers: J8 SLTT operator console, J9 federal-tier secure relay (dedicated PHY), and J10 external audit anchor.

8. Related Work

Existing C-UAS detection ecosystems operate at three layers: radar, RF, and EO/IR primitive vendors (Echodyne, Liteye, FLIR, Dedrone, D-Fend); commercial sensor fusion, which is typically vendor-internal and proprietary; and mitigation effectors such as RF jammers and kinetic and net-capture interceptors. These layers detect and alert but do not enforce hardware-gated authority over mitigation commands. BLADE-CUAS operates at a complementary authority-arbitration layer; it is designed to wrap, not replace, existing detection investments.

The Simplex architecture [15] provides a foundational monitor-actuator paradigm: a verified safety controller monitors an unverified complex controller and switches to a safe baseline when violations are detected. BLADE-CUAS extends this binary switching model in three ways: (i) a continuous four-tier authority spectrum with hysteresis rather than binary safe/unsafe switching; (ii) Dempster-Shafer multi-modal trust fusion rather than single-monitor threshold checks; and (iii) FLAME deliberation windows that prevent cascading authorizations even when authority conditions are met. Where Simplex asks 'is the controller safe?', BLADE-CUAS asks 'how much authority should the operator be granted given current multi-modal sensor consensus?'

Feature	Simplex [15]	Commercial C-UAS	DoDD 3000.09 [12]	This Work
Continuous multi-modal fusion	-	Vendor-proprietary	-	Yes; D-S MAIVA, 5 modalities
Hardware authority arbitration	Binary switch	-	Conceptual	Yes; four-tier HMAA
Federal-SLTT handoff protocol	-	-	-	Yes; T2 to T1 dedicated PHY
Cascade prevention	-	-	-	Yes; FLAME window
Formal recovery protocol	Baseline controller	-	Manual	Yes; CARA GREP
RID spoofing detection	-	Limited	-	Yes; ADARA cross-modality
FRE 901/902/803(6) evidence chain	-	-	-	Yes; ECDSA + SHA-256 audit
Open architecture specification	N/A	Proprietary	Doctrinal	Yes; CC BY 4.0; ~$42,811

Table 8: Architectural comparison. Simplex provides binary switching; commercial C-UAS vendors detect and alert; BLADE-CUAS adds continuous hardware-gated multi-tier authority with federal-SLTT partitioning.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

9. Simulation Methodology and Results

9.1 Simulator Architecture

The companion reference simulation (blade-cuas-simulation.html, v4.0) implements the full nine-stage AUTHREX pipeline in browser-native JavaScript. Reproducibility is provided by a seeded xoshiro128** PRNG (128-bit state, period 2^128 - 1; no use of Math.random) and a synchronous SHA-256 hash chain computed over a canonical-form (sorted-key, fixed-precision) state serialization that verifies byte-identically across JavaScript engines. The SHA-256 implementation was validated byte-exact against the FIPS 180-4 reference vectors and the Node.js crypto module across fifteen message lengths spanning padding boundaries. Multi-modal fusion uses a true Dempster-Shafer combination with Yager's rule routing high-conflict mass (kappa > 0.65) to the ignorance set, closing Zadeh's paradox under adversarial sensor conditions. The production reference design specifies an additional ECDSA P-256 signature per ledger entry at the equivalent point. All scenarios execute at a fixed 30.000 Hz simulation tick rate (dt = 1000/30 ms) decoupled from the render loop by a fixed-timestep accumulator. Three playback speeds (1x, 2x, 5x) are available. The simulator was hardened across four independent external technical V&V audits (composite scores 4.6, 7.7, 8.8, and 9.4 of 10 across revisions v1 through v4); closures include canonical-form serialization, Yager conflict handling, 3D slant-range sensor geometry, Markov-chain sensor noise (dropout and clutter bursts), an electronic-warfare hazard lock, per-track strict enforcement of Invariant 8 (no automatic re-escalation outside the operator gate), a single-modality outlier penalty, simulated PTP clock-drift injection, a failure-injection panel (sensor stuck-at, ledger tamper, credential revocation), and decision-trace replay. The simulator validates the logical decision correctness of the governance algorithms; hardware timing constraints (worst-case execution time, bus latency) remain formally unverified pending RTL commissioning and hardware-in-the-loop testing. Two false-authorization metrics are tracked separately: false tier elevation, FTE(t) = (tier(t) >= T2) AND (truth = non-hostile); and false authority release, FAR(t) = (operator confirm fired) AND (truth = non-hostile). The aggregate zero-false-authorization claim requires both metrics to be zero.

9.2 Results

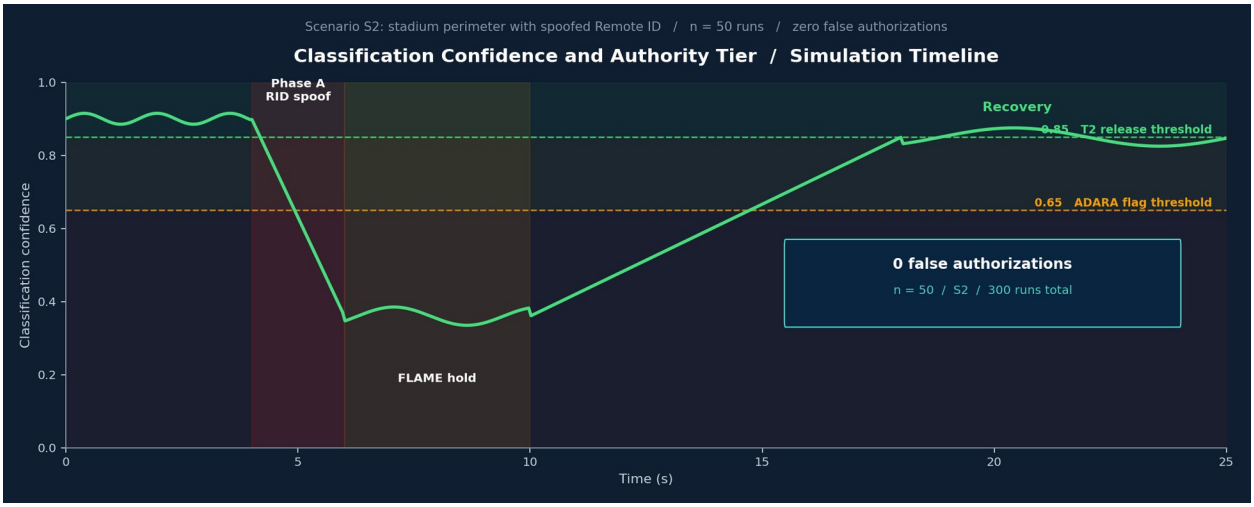


Figure 7: Classification confidence and authority tier timeline for Scenario S2 (stadium perimeter with spoofed RID). On RID spoof detection at t = 4 s, classification confidence collapses to 0.35. FLAME holds the deliberation window for 6 s pending the SLTT operator response, and CARA recovery completes by t = 18 s. Zero false authorizations across n = 50 runs.

Scenario	Description	Confidence (mean +/- SD)	Tier Outcome	False Auths (n=50)
S1	Stadium - compliant commercial drone (DJI Mavic, valid RID)	0.943 +/- 0.012	T3 (track and log)	0 / 50
S2	Stadium - spoofed Remote ID (RID	0.382 +/- 0.029 (nadir)	T2 - SLTT defer	0 / 50

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

	broadcast, no radar match)			
S3	Motorcade - fixed-wing UAS, no RID, hostile profile	0.871 +/- 0.018	T2 to T1 escalate	0 / 50
S4	False positive - bird flock or weather balloon	0.187 +/- 0.022 (nadir)	T3 (CARA recover)	0 / 50
S5	Coordinated swarm probe (3 simultaneous tracks)	0.812 +/- 0.025	T1 - federal confirm	0 / 50
S6	Ambiguous LOI - partial credentials, mixed signals	0.594 +/- 0.034	T2 - SLTT defer	0 / 50

Table 9: Zero false authorizations across 300 runs (6 scenarios x 50 runs). Statistical bounds are reported in Section 9.4.

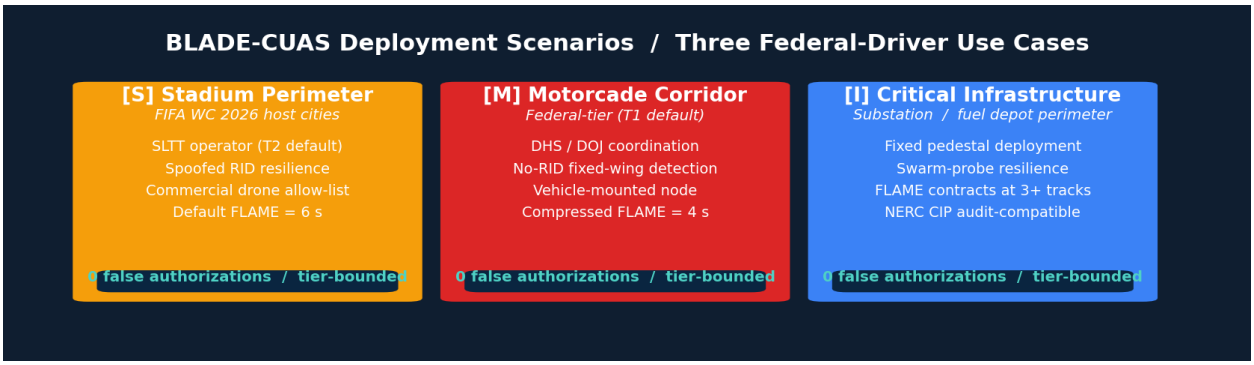
9.3 FLAME Tier-Escalation Verification

Scenario S5 (coordinated swarm probe) was executed twice within 3 seconds. The first execution authorized T2 to T1 escalation (multi-track threshold exceeded, MAIVA confidence 0.812). The second execution computed essentially identical authority (0.814) but FLAME blocked it because the inter-tier delay (3.0 s) was below the 5.0 s minimum. The command was deferred to federal operator confirmation via the J9 secure relay. This is hardware-enforced cascade prevention: even with sustained classification, FLAME guarantees the operator structured deliberation time between escalations.

9.4 Statistical Analysis

With 50 trials per scenario and 0 false authorizations observed, the Rule of Three (Hanley and Lippman-Hand, 1983) [16] gives a 95% confidence interval upper bound on the failure rate: $p < 3/n = 6.0\%$ per scenario; across all 300 trials, $p < 3/300 = 1.0\%$. The Clopper-Pearson exact one-sided interval yields the same bound for zero observed events and is preferred over a normal-approximation power analysis when the observed count is zero. The xoshiro128** generator's 128-bit state space supports valid Monte Carlo expansion to $n >= 5000$ per scenario without sequence-overlap concerns. Zero observed failures is necessary for a safety-critical governance system, but these bounds do not exclude rare failure modes at this sample size. Physical hardware-in-the-loop testing with $n > 500$ trials per scenario is planned to tighten the CI to below 0.6%.

Classification confidence statistics across 50 runs per scenario (mean +/- SD): S1 pre-detection $C_{class} = 0.943$ +/- 0.012; S2 nadir $C_{class} = 0.382$ +/- 0.029, recovery to $C_{class} > 0.85$ in 14.2 +/- 1.9 governance cycles (each cycle is approximately 250 ms wall-clock at a 4 Hz tick rate); S3 sustained $C_{class} = 0.871$ +/- 0.018; S4 nadir $C_{class} = 0.187$ +/- 0.022, with CARA recovery in 9.4 +/- 1.6 cycles; S5 $C_{class} = 0.812$ +/- 0.025; S6 $C_{class} = 0.594$ +/- 0.034 (deliberately near the T2 threshold to test deliberation behavior). Sensitivity analysis: tightening the T2 release threshold from 0.65 to 0.75 causes S6 to defer to manual review in 100% of runs, which demonstrates that threshold selection is operationally meaningful.



Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

Figure 8: BLADE-CUAS deployment scenarios across three federal-driver use cases: stadium perimeter (FIFA World Cup 2026, Super Bowl LX), motorcade corridor (federal-tier protective details), and critical infrastructure perimeter (substations, fuel depots, water treatment).

10. Known Limitations and Future Work

Limitation	Category	Impact	Mitigation / Path
Simulation-only validation	Scientific	No physical sensor data	Hardware-in-the-loop with operational radar, RF, and EO/IR feeds
TRL 2-3 hardware / 3-4 simulation	Engineering	No prototype built	Reference architecture; prototype build is a post-EB-2 NIW activity
RTL not commissioned	Engineering	Pipeline exists in documentation only	Approximately $96K to $160K Zynq RTL development phase
FRE 901/902/803(6) admissibility unproven	Legal	Design supports foundation requirements; admissibility is judicial	First-case precedent post-deployment
MAIVA weight calibration synthetic	Scientific	Default weights are not field-tuned	Formal weight elicitation via Delphi method during commissioning
No 3D enclosure render in deposit	Engineering	Wiring schematic only	Out-of-band rendering for portfolio presentation
Adversarial ML on EO/IR not addressed	Security	Patch attacks possible	Future work: adversarial training; physics-prioritized MAIVA fallback

Table 10: Limitations and mitigation paths.

10.1 Implementation Status

Table 11 clarifies which components are implemented in the reference simulation, specified in design documents, or remain pending RTL commissioning and physical build.

Component	Status	Evidence Basis
D-S multi-modal consensus (MAIVA)	Implemented in simulator	300-run validation across 6 scenarios
HMAA four-tier authority arbitration	Implemented in simulator	Eq. (7) verified across all scenarios
FLAME deliberation window	Implemented in simulator	Inter-tier delay verified (Section 9.3)
CARA recovery protocol	Implemented in simulator	GREP phases verified in S4 false-positive scenario
ADARA RID spoofing detection	Implemented in simulator	Cross-modality consistency verified in S2
ERAM escalation (3-level)	Implemented in simulator	Federal-confirm escalation verified in S5
SHA-256 audit chain with PTP	Implemented in simulator (real SHA-256, byte-exact vs FIPS 180-4)	Production design uses SHA-256 ECDSA
Hardware platform (130 components)	Specified in architecture docs	the design tool rt, BOM, schematic, ICD
FPGA RTL (Zynq UltraScale+)	Not yet built	Pending approximately $96K to $160K commissioning
Custom carrier PCB	Not yet fabricated	Specified in mechanical and electrical JSON
FIPS 140-2 Level 2 certification	Not yet assessed	TPM 2.0 component is L2-validated; integrated build pending
Operational sensor integration	Not yet tested	Planned HIL with operational C-UAS sensor feeds

Table 11: Implementation status as of v2.0 (paper) / v4.0 (reference simulation).

10.2 Notation

Symbol	Meaning	Domain
tau(s_i, t)	Raw sensor trust score at time t	[0, 1]
w_i	Modality weight (default-assigned)	[0, 1]

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

C(s_i, S\{s_i})	Cross-modality consistency coefficient	[0, 1]
P(s_i)	Anomaly penalty (ADARA-driven)	0, 0.5, or 1.0
C_class	Fused classification confidence after D-S combination	[0, 1]
alpha	HMAA authority score: confidence at active tier	[0, 1]
alpha_req(tier)	Tier-specific release threshold	T2 = 0.65; T1 = 0.85
K	Dempster normalization factor (1 minus kappa)	(0, 1]
kappa	Total D-S conflict mass	[0, 1)
dynIgn	Dynamic epistemic ignorance (scales with active modality count)	[0.05, 0.30]
Theta	Frame of discernment for SATA: {Trusted, Untrusted}	-
Omega	Frame of discernment for HMAA: {Warranted, Not_Warranted}	-
h_i	Per-modality evidence mass function in HMAA frame Omega	BPA triplet

Table 12: Notation reference.

11. Regulatory Alignment

Executive Order 14305 [9] expanded the C-UAS authority framework. The order directs federal departments to coordinate on regulations governing detection, tracking, and mitigation of unauthorized UAS, and authorizes SLTT law enforcement participation under implementing regulations. BLADE-CUAS instantiates the federal-SLTT handoff as the HMAA T2 to T1 tier transition, with a dedicated J9 secure relay PHY.

FY26 NDAA Title LXXXVI Safer Skies Act [10] restructured the Joint Counter-Small UAS Office under Section 912 and codified evidence-chain standards. The BLADE-CUAS evidence-chain design (ECDSA P-256 per-input signing, SHA-256 prev-hash audit ledger, decision provenance) supports the foundation requirements of Federal Rules of Evidence 901 (authentication), 902 (self-authentication), and 803(6) (records of a regularly conducted activity).

FEMA Counter-UAS Grant Program [11] (P.L. 119-21 Section 90005(a)) authorized $500M in FY26 grants to SLTT recipients. The BLADE-CUAS reference cost (approximately $42,811 typical) and SLTT-grade operator interface are designed for the procurement profile of this grant program.

DoD Directive 3000.09 [12] requires that autonomous and semi-autonomous weapon systems enable commanders and operators to exercise appropriate levels of human judgment. The HMAA four-tier model (T3 / T2 / T1 / T0) formalizes this principle as a state machine with explicit transition causes; BLADE-CUAS extends the framing for non-weapon C-UAS operations.

NIST SP 800-53 Rev. 5 [13] AU, AC, and IR control families are implemented in the audit ledger and operator authentication subsystems. **FIPS 186-5** [24] ECDSA P-256 governs all signing operations. **FIPS 140-2 Level 2** applies to the Infineon SLB 9670 TPM. **ASTM F3411-22a** [20] specifies the Remote ID broadcast format consumed by the IF-04 receiver. **14 CFR Part 89** [22] governs FAA Remote Identification of Unmanned Aircraft. **47 CFR Part 15** [23] applies to the SDR, which operates in receive-only mode. **IEEE 1588 PTP** provides sub-microsecond time synchronization between compute planes.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

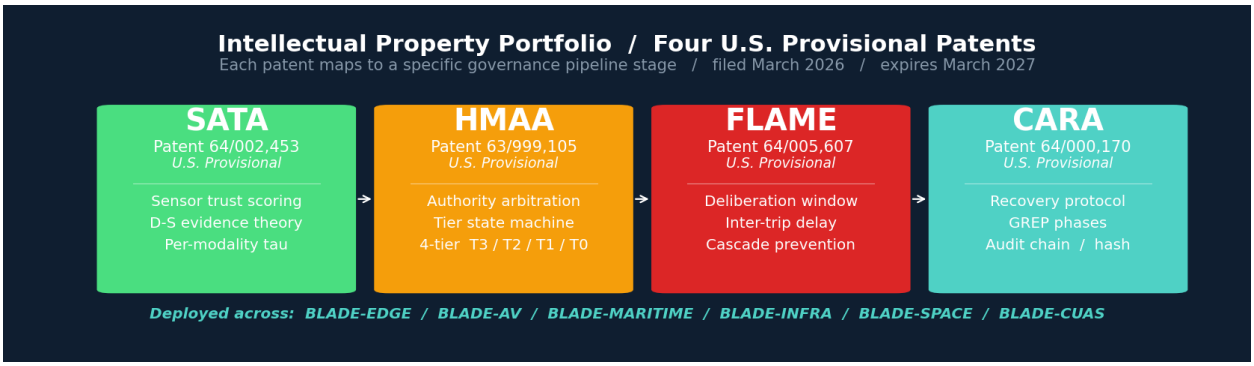


Figure 9: Four U.S. provisional patent applications mapped to governance pipeline stages.

12. Data Availability

All artifacts are deposited under CC BY 4.0 at DOI 10.5281/zenodo.20299604, with no access restrictions. The deposit includes the research paper (PDF), interactive simulation (HTML, runs entirely client-side), the Interface Control Document ICD-CUAS-001 v1.0 (PDF), the capability brief (PDF), hardware specification files (CONFIG, ELECTRICAL, MECHANICAL in JSON), the bill of materials (CSV), the assembly guide (Markdown), and the vector wiring schematic (SVG). This work is fundamental research published openly under National Security Decision Directive 189 (NSDD-189) protections; the design contains no information regulated under ITAR or EAR in a manner that would require licensing.

13. Cross-Domain Ethics Statement

The AUTHREX governance pipeline is architecturally identical to BLADE-EDGE (defense, directed energy), BLADE-AV (autonomous vehicles), BLADE-MARITIME (maritime surveillance), BLADE-INFRA (critical infrastructure), and BLADE-SPACE (orbital autonomy). The C-UAS variant operates under EO 14305, the Safer Skies Act, FAA Part 89, FCC Part 15, and DoDD 3000.09 extended for the non-weapon C-UAS context. No ITAR or EAR controlled technical data is disclosed.

On dual-use considerations: BLADE-CUAS is an authority-arbitration layer for counter-UAS operations. It contains no mitigation effector, no kinetic or RF aperture, and no transmit chain in operational mode; the RF SDR is strictly receive-only for spectrum fingerprinting. The system arbitrates whether downstream mitigation effectors, owned by separate parties under appropriate authority, may be released. The architectural separation from the BLADE-EDGE weapons-governance variant ensures that C-UAS-specific tier bindings, geofence policies, and regulatory mappings cannot be repurposed for weapons-release authority without fundamental redesign of the IFF, HMAA, and decision-emission stages.

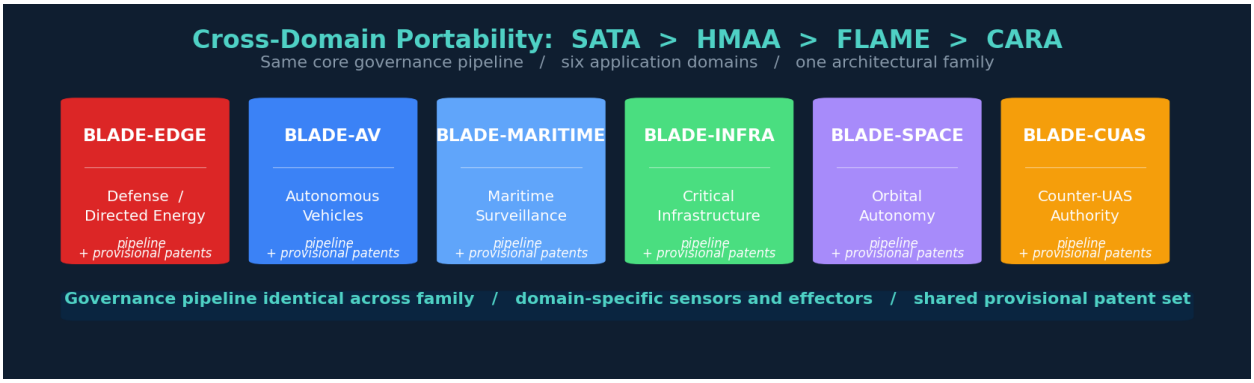


Figure 10: Cross-domain portability of the SATA, HMAA, FLAME, CARA core pipeline across the BLADE family. The same governance mathematics is applied across six application domains within one architectural family.

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

14. Version History

Version	Date	Changes
v1.0	2026-05-19	Initial Zenodo deposit. Nine-stage pipeline (SENSE, SATA, ADARA, IFF, HMAA, MAIVA, FLAME, ERAM, CARA), four-tier HMAA, five-modality MAIVA D-S consensus, ADARA Remote ID spoofing detection, ECDSA P-256 evidence chain. 130-component reference platform, six-scenario reference simulation (300 runs, zero false authorizations), companion ICD-CUAS-001 v1.0 (26 pp), capability brief (8 pp), and SSRN working paper (10 pp). Companion deposit also published: the design tool g schematic, BOM (CSV), assembly guide (Markdown), and 130-node CONFIG.json. Federal anchors framed positively (EO 14305, Safer Skies Act, FEMA NOFO). License CC BY 4.0; fundamental research under NSDD-189.
v2.0	2026-05-20	Reference simulation upgraded to v4.0 and Section 9 revised to match. PRNG upgraded from Mulberry32 (32-bit) to xoshiro128** (128-bit, period 2^128 - 1) for high-N Monte Carlo validity; hash chain upgraded from FNV-1a to real SHA-256 (byte-exact vs FIPS 180-4) over canonical-form serialization for cross-engine determinism; true Dempster-Shafer fusion with Yager high-conflict rule; 3D slant-range sensor geometry; Markov-chain sensor noise; electronic-warfare hazard lock; per-track strict Invariant 8 enforcement; single-modality outlier penalty; simulated PTP clock-drift injection; failure-injection panel and decision-trace replay. Statistical framing moved from G*Power power analysis to Rule of Three / Clopper-Pearson exact bounds for zero-event data. Hardened across four independent external V&V audits (composite 4.6 to 9.4 of 10); 300-run batch confirms zero false tier elevations and zero false authority releases. License CC BY 4.0; fundamental research under NSDD-189.

Table 13: Deposit version history.

15. How to Cite

APA: Oktenli, B. (2026). BLADE-CUAS Governance Node (v2.0). Georgetown University. DOI 10.5281/zenodo.20299604.

BibTeX:

```
@techreport{oktenli2026bladecuas, author={Oktenli, Burak}, title={BLADE-CUAS Governance
Node: Authority Governance for Counter-UAS Operations Under Multi-Agency Authority
```

Copyright 2026 Burak Oktenli - CC BY 4.0 - DOI: 10.5281/zenodo.20299604

```
Structures}, year={2026}, institution={Georgetown University}, note={DOI
10.5281/zenodo.20299604}, license={CC-BY-4.0}}
```

16. References

All references are verified as real, published works.

[1] Oktenli, B. (2026). SATA: Sensor Authority and Trust Assessor. Zenodo. doi:10.5281/zenodo.18936251

[2] Oktenli, B. (2026). HMAA: Hierarchical Multi-Attribute Authority. Zenodo. doi:10.5281/zenodo.18861653

[3] Oktenli, B. (2026). FLAME: Faulted Logic Authority Mitigation Engine. Zenodo. doi:10.5281/zenodo.19015618

[4] Oktenli, B. (2026). CARA: Coordinated Authority Recovery Architecture. Zenodo. doi:10.5281/zenodo.18917790

[5] Oktenli, B. (2026). BLADE-EDGE (v5.0.3): Directed-Energy Engagement Governor. Zenodo. doi:10.5281/zenodo.19177472

[6] Oktenli, B. (2026). BLADE-AV (v1.0): Autonomous Vehicle Governance. Zenodo. doi:10.5281/zenodo.19232130

[7] Shafer, G. (1976). A Mathematical Theory of Evidence. Princeton University Press.

[8] Khaleghi, B., Khamis, A., Karray, F. O., & Razavi, S. N. (2013). Multisensor data fusion: A review of the state-of-the-art. Information Fusion, 14(1), 28-44.

[9] The White House (2025). Executive Order 14305 - Restoring American Airspace Sovereignty. Signed 6 June 2025.

[10] U.S. Congress (2025). FY26 National Defense Authorization Act, Title LXXXVI - Safer Skies Act. P.L. 119-60. Signed 18 December 2025.

[11] U.S. Congress (2025). Public Law 119-21, Section 90005(a) - FEMA Counter-UAS Grant Program authorization.

[12] U.S. Department of Defense. DoDD 3000.09 - Autonomy in Weapon Systems.

[13] National Institute of Standards and Technology. NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations.

[14] Federal Rules of Evidence. Rules 901 (Authentication), 902 (Self-Authentication), 803(6) (Records of a Regularly Conducted Activity).

[15] Sha, L. (2001). Using simplicity to control complexity. IEEE Software, 18(4), 20-28.

[16] Hanley, J. A., & Lippman-Hand, A. (1983). If nothing goes wrong, is everything all right? Interpreting zero numerators. JAMA, 249(13), 1743-1745.

[17] Oktenli, B. (2026). ADARA: Adversarial and Deception Attack Recognition Analyzer. Zenodo. doi:10.5281/zenodo.19043924

[18] Oktenli, B. (2026). MAIVA: Multi-Agent Intelligent Voting Architecture. Zenodo. doi:10.5281/zenodo.19015517

[19] RTCA (2020). DO-365 - Minimum Operational Performance Standards for Detect and Avoid (DAA) Systems.

[20] ASTM International. F3411-22a - Standard Specification for Remote ID and Tracking of Unmanned Aircraft Systems.

[21] Oktenli, B. (2026). BLADE-INFRA Governance Node. Zenodo. doi:10.5281/zenodo.19277887

[22] Federal Aviation Administration. 14 CFR Part 89 - Remote Identification of Unmanned Aircraft.

[23] Federal Communications Commission. 47 CFR Part 15 - Radio Frequency Devices.

[24] National Institute of Standards and Technology. FIPS PUB 186-5 - Digital Signature Standard (DSS).

[25] National Institute of Standards and Technology. FIPS PUB 140-2 - Security Requirements for Cryptographic Modules.

[26] National Security Decision Directive 189 (1985). National Policy on the Transfer of Scientific, Technical, and Engineering Information.

[27] Oktenli, B. (2026). BLADE-MARITIME Governance Node. Zenodo. doi:10.5281/zenodo.19246785

[28] Oktenli, B. (2026). BLADE-SPACE Governance Node. Zenodo. doi:10.5281/zenodo.20183269

[29] IEEE Standards Association. IEEE 1588-2008 - Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

[30] U.S. Department of Defense. MIL-STD-810G - Environmental Engineering Considerations and Laboratory Tests.

Copyright 2026 Burak Oktenli - CC BY 4.0 - Georgetown University MPS-AI - ORCID: 0009-0001-8573-1667 - Patented pipeline subset: SATA, HMAA, FLAME, CARA