BLADE-CUAS Governance Simulator

Simulation User Guide

Version: v1.0
Document: CUAS-SIM-UG-001
Date: May 2026
Revision: 1.0
Author: Burak Oktenli
Institution: Georgetown University, School of Continuing Studies
Program: M.P.S. Applied Intelligence (STEM)
ORCID: 0009-0001-8573-1667
Related Artifact: DOI: 10.5281/zenodo.20299604

Document Control

Document ID	CUAS-SIM-UG-001
Simulation Version	v1.0
Author	Burak Oktenli — Georgetown University — ORCID 0009-0001-8573-1667
Date / Revision	May 2026 / Rev 1.0 — Initial Release
Classification	UNCONTROLLED — Research Artifact
Related Artifact	DOI: 10.5281/zenodo.20299604

Table of Contents

1. Purpose, Scope, and Assumptions

This guide provides operating procedures for the BLADE-CUAS (Counter-Unmanned Aircraft Systems Governance) simulation. It implements the complete 9-stage AUTHREX governance pipeline (SENSE -> SATA -> ADARA -> IFF -> HMAA -> MAIVA -> FLAME -> ERAM -> CARA) arbitrating federal-SLTT authority for Counter-UAS operations, with four-tier HMAA (T3/T2/T1/T0), Dempster-Shafer multi-modal consensus across radar, RF, EO/IR, Remote ID, and LIDAR, and an ECDSA P-256 court-admissible evidence chain. The simulation demonstrates how authority-governed autonomy arbitrates engagement authority without itself being a detection sensor, jammer, or interceptor.

Intended Audience: EB2-NIW petition evaluators, defense/aerospace and AI-security reviewers, academic peers, and technical collaborators seeking independent verification of behavior.

Scope: Operation of the BLADE-CUAS Governance Simulator. Does not cover mathematical theory (see the published paper) or hardware specifications (see the Zenodo deposit and the Interface Control Document, ICD-CUAS-001).

1.1 Assumptions and Constraints

- The user has a modern browser with JavaScript enabled and HTTPS access.
- All parameter values are synthetic research placeholders, not calibrated against physical hardware.
- The simulation models governance logic only. Physical sensor dynamics are simplified.
- Cryptographic operations (ECDSA P-256, SHA-256 audit chain) use the WebCrypto API, not a hardware TPM/HSM.
- Results are valid for demonstrating architectural behavior, not for operational safety assessment.

> **IMPORTANT**
>
> This simulation is a research prototype. Not for operational planning, safety-critical decisions, or system certification. BLADE-CUAS contains no mitigation effector; it is a passive governance layer. All parameters are synthetic.

2. Quick Start

Step 1. Open the simulation HTML file in Chrome over HTTPS.

Step 2. Review the interface panels and identify the main controls.

Step 3. Select a scripted scenario or enter free-play mode.

Step 4. Click RUN/START to begin the governance loop and observe the 9-stage pipeline.

Step 5. Use the export/download buttons to save session data as JSON for verification.

> **NOTE**
>
> All computation runs client-side with the WebCrypto API. No data leaves your browser. Requires HTTPS (not file://).

3. System Requirements and Security Considerations

Requirement	Specification
Browser	Chrome 90+, Firefox 88+, Safari 15+, Edge 90+
Protocol	HTTPS required (WebCrypto API for ECDSA / SHA-256 / HKDF)
Display	Min 1280x720; recommended 1920x1080+
CPU/Memory	Any modern processor; ~200MB RAM peak for batch runs
Network	Internet for initial CDN load. All computation client-side after load.
Installation	None — zero install, no login, no backend, no database, no cookies

3.1 Security Considerations

- No data exfiltration: all computation runs in the browser. No data is sent to any server.
- CDN dependencies load from cdnjs.cloudflare.com with Subresource Integrity hashes where available.
- Audit integrity: ECDSA P-256 signatures and a SHA-256 hash chain via WebCrypto. The VERIFY button recomputes the chain.
- No authentication: the simulation has no login system. All state is ephemeral in browser memory.

4. Interface Layout and Navigation

4.1 Panel Layout

The interface presents the sensor-modality trust array (radar, RF, EO/IR, Remote ID, LIDAR), the four-tier authority gauge (T3/T2/T1/T0), the 9-stage pipeline status (SENSE through CARA, each PASS/FAIL/SKIP), a track list with IFF classification and Dempster-Shafer consensus mass, the federal-SLTT handoff control, and the engagement-risk (ERAM) readout. Controls include START/STOP, scenario selection, track injection, and a Monte Carlo batch.

> **TIP**
>
> Hover over interface elements for tooltips. Gauges include ARIA labels for screen-reader accessibility.

5. Operating Procedures

5.1 Startup

1. Navigate to the simulation URL or click Launch Simulation from burakoktenli.com.
2. Wait for loading (2-5 seconds). CDN scripts load from cdnjs.cloudflare.com.
3. Verify the interface loads completely. All panels should be visible.

5.2 Standard Operation

1. Open the simulation via Launch Simulation or navigate to blade-cuas-simulation.html.
2. Click START to begin. Detection tracks appear and the governance pipeline processes each track.
3. Monitor the 9-stage pipeline (SENSE -> SATA -> ADARA -> IFF -> HMAA -> MAIVA -> FLAME -> ERAM -> CARA).
4. SATA assigns a per-sensor trust score; ADARA flags Remote ID spoofing and adversarial inconsistency.
5. MAIVA computes Dempster-Shafer consensus across at least three modalities before authority is considered.
6. HMAA arbitrates the authority tier; on SLTT escalation the federal-SLTT handoff transitions T2 -> T1.
7. FLAME applies a tier-dependent deliberation window; ERAM reports an engagement-risk score.
8. Run the Monte Carlo batch for statistical outcomes (zero false tier elevations, zero false authority releases).
9. CARA reverts state and writes a corrective audit entry on any misclassification.

5.3 Shutdown

1. Export session data. 2. Close the browser tab (all state discarded).

> **IMPORTANT**
>
> State is not persisted. Export before closing to preserve results.

6. Parameter Reference

Parameters are pre-configured per scenario (sensor weights, tier thresholds, FLAME window durations, MAIVA consensus floor). See Section 4 for interface controls and the published paper for parameter derivation. Remote ID is treated as one provenance signal among many (default MAIVA weight 0.15), a deliberate departure from commercial C-UAS practice.

7. Scenario Reference

Six scripted scenarios plus free-play. Select a scenario from the control panel before starting.

Scenario	Description
Compliant commercial drone	Cooperative track with valid Remote ID; expected to remain at a monitoring tier.
Spoofed Remote ID	Inconsistent or forged Remote ID; ADARA flags the provenance mismatch.
Motorcade fixed-wing UAS	High-consequence fixed-wing threat near a protected motorcade; tier escalation.
False-positive bird flock	Non-threat biological clutter; consensus must avoid false tier elevation.
Coordinated swarm probe	Multiple coordinated tracks probing the protected volume.
Ambiguous track	Low-confidence track exercising the deliberation window and consensus floor.

8. Metrics, Formulas, and Verification

8.1 Key Metrics

Metric	Definition
Pipeline Status	9-stage status: SENSE, SATA, ADARA, IFF, HMAA, MAIVA, FLAME, ERAM, CARA.
Authority Tier	HMAA-computed tier (T3/T2/T1/T0); federal-SLTT handoff on escalation.
Consensus Mass	Dempster-Shafer belief/plausibility across radar, RF, EO/IR, Remote ID, LIDAR.
IFF Classification	P(authorized) / P(unauthorized) / P(unknown) per track.
Engagement Risk	ERAM engagement-risk score in [0,1].

8.2 Verification Checklist

Action	Expected Result
Start simulation (RUN/START)	Interface loads; the 9-stage pipeline begins processing.
Observe default state	Monitoring tier; all pipeline stages PASS for a compliant track.
Inject a spoofed Remote ID	ADARA flags the provenance mismatch; consensus mass shifts.
Escalate (SLTT -> Federal)	HMAA transitions T2 -> T1; FLAME federal window opens.
Export session data (JSON)	File downloads with parameters, history, and the signed audit trail.
Reload with same seed	Same seed + params yield identical outputs.

9. Data Export and Reproducibility

Click export/download to save a session JSON with parameters, decision history, and the ECDSA-signed audit trail. To verify: 1) export JSON; 2) note the PRNG seed; 3) reload with the same seed and parameters; 4) confirm a bit-exact match and a valid audit chain.

9.1 Reproducibility Guarantee

Property	Value
PRNG	Deterministic seeded generator (32-bit)
Math.random()	Zero calls in computation paths
Cross-Browser	Verified: Chrome, Firefox, Safari, Edge
Audit Chain	ECDSA P-256 + SHA-256 via WebCrypto (SubtleCrypto API)
Monte Carlo	300-run batch: zero false tier elevations, zero false authority releases

10. Limitations and Threat Considerations

Limitation	Description
Simulation-Only Evidence	Browser-based computation. No physical sensor data or hardware measurements.
Uncalibrated Parameters	All values are synthetic research parameters, not empirically derived.
No Real-Time Guarantees	The JavaScript engine provides no timing guarantees for safety-critical operations.
Simulated Cryptography	ECDSA/SHA-256 use WebCrypto. TPM/HSM operations are modeled, not hardware-backed.
Single-Session State	All state is held in memory; closing the tab discards all data.

10.1 Threat Considerations

• CDN compromise: dependencies load from cdnjs.cloudflare.com. Mitigation: Subresource Integrity hashes where available.

• Browser extensions could modify the simulation DOM/state. Mitigation: test in Incognito mode for clean results.

• Local modification via DevTools is possible. Exported data should be verified against the published source on burakoktenli.com.

ASSURANCE BOUNDARY

This is a research demonstrator (TRL 2-3 hardware / 3-4 simulation). No FIPS, Common Criteria, EAL, NSA, NASA, or DoD endorsement, validation, or certification of any kind is claimed. BLADE-CUAS contains no mitigation effector and emits only signed authority decisions.

11. Troubleshooting

Problem	Likely Cause	Solution
Black screen after loading	Render error or CSP violation	Open F12 Console for details. Try Chrome Incognito.
Simulation runs slowly	CPU-intensive batch run	Close other tabs. Reduce the sample count.
Controls not responding	Tab lost focus	Click inside the simulation window. Ensure the tab is active.
Export not working	Download blocked	Allow downloads from the simulation domain in browser settings.
Loading never completes	CDN scripts blocked	Disable ad blockers. Allow cdnjs.cloudflare.com.

12. Glossary and References

12.1 Glossary

Term	Definition
BLADE-CUAS	Beam-Layer Authority for Directed Engagements, Counter-UAS Node
SATA	Sensor Attestation and Trust Anchoring — per-sensor trust fusion
HMAA	Human-Machine Authority Architecture — four-tier authority arbitration
MAIVA	Multi-Agent Integrity and Verification Architecture — Dempster-Shafer consensus
ADARA	Adversarial Detection and Response Architecture — spoofing detection
Federal-SLTT	Federal and State/Local/Tribal/Territorial authority handoff (post-EO 14305)
ECDSA P-256	Elliptic-curve signature over NIST P-256 for the audit chain

12.2 References

[1] Oktenli, B. (2026). BLADE-CUAS Governance Node. DOI: 10.5281/zenodo.20299604.

[2] Oktenli, B. (2026). Simulation artifact. https://burakoktenli.com/blade-cuas-simulation.html

[3] Oktenli, B. (2026). Research Portfolio. https://burakoktenli.com

[4] Executive Order 14305 (2025); FY26 NDAA Title LXXXVI (Safer Skies Act).

[5] Fed. R. Evid. 901 / 902 / 803(6) (authentication and records of regularly conducted activity).

12.3 Contact

Burak Oktenli — Georgetown University, School of Continuing Studies
Website: burakoktenli.com | ORCID: 0009-0001-8573-1667
For questions about this simulation or the governance architecture research program, use the contact form at burakoktenli.com.

End of Document