HMAA Governance Simulation

Simulation User Guide

Version: v2.4.0
Document: HMAA-SIM-UG-001
Date: April 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.18861653

Document Control

Document ID	HMAA-SIM-UG-001
Simulation Version	v2.4.0
Author	Burak Oktenli — Georgetown University — ORCID 0009-0001-8573-1667
Date / Revision	April 2026 / Rev 1.0 — Initial Release
Classification	UNCONTROLLED — Research Artifact
Related Artifact	DOI: 10.5281/zenodo.18861653

Table of Contents

1. Purpose, Scope, and Assumptions

This guide provides operating procedures for the HMAA (Human-Machine Authority Architecture) simulation dashboard. The simulation computes real-time authority levels using four input parameters (Q, C, E, tau) mapped through a four-tier authority state machine (T4 Full Autonomy through T1 Lockout) with hysteresis-protected transitions. It includes Monte Carlo statistical analysis, parameter sensitivity heatmaps, scenario comparison tools, and a cryptographic SALM audit chain.

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

Scope: Operation of the HMAA Governance Simulation simulation. Does not cover mathematical theory (see published paper) or hardware specifications (see Blueprint.am).

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 dynamics (aerodynamics, acoustics, electromagnetics) are simplified.
- Cryptographic operations (SHA-256 audit chain) use the WebCrypto API, not 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. All parameters are synthetic.

2. Quick Start

Step 1. Open hmaa-simulation.html in Chrome over HTTPS.

Step 2. Adjust the four sliders: Q (Qualification), C (Context), E (Escalation), tau (Sensor Trust).

Step 3. Watch the authority gauge compute A = tau * [(w_Q*Q + w_C*C) * (1-E)] in real time.

Step 4. Click preset buttons (NOMINAL, CRISIS, JAM tau=0) to jump to pre-defined states.

Step 5. Switch to Monte Carlo tab and click RUN for 100-trial statistical analysis.

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

3. System Requirements and Security Considerations

Browser	Chrome 90+, Firefox 88+, Safari 15+, Edge 90+

Protocol	HTTPS required (WebCrypto API for SHA-256 audit hashing)
Display	Min 1280x720; recommended 1920x1080+
CPU/Memory	Any modern processor. Monte Carlo (100+ runs): multi-core recommended, ~200MB RAM peak
GPU	WebGL-capable recommended for 3D visualizations (Three.js)
Network	Internet for initial CDN load (~500KB). 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:** React, ReactDOM, and Babel load from cdnjs.cloudflare.com (Cloudflare CDN with SRI hashes where available).

• **Audit integrity:** SHA-256 hash chain via WebCrypto API. Each audit entry links to the previous entry's hash. VERIFY button recomputes the entire 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 uses a three-column layout. **Left Panel:** Four parameter sliders (Q, C, E, tau) stacked vertically with current values displayed, plus eight preset buttons in a 2x4 grid below. **Center Panel:** Large circular authority gauge (0-100%) with tier label (T4/T3/T2/T1), formula breakdown showing weighted computation, and tabbed navigation bar (Overview, Calculator, Hysteresis, Monte Carlo, Compare, Scenarios, Audit, Reproducibility). **Right Panel:** SALM hash-chained audit log scrolling downward with timestamp, parameters, authority, tier, and SHA-256 hash per entry. **Top Bar:** Version badge and simulation status indicators.

4.2 Navigation Tabs

Overview (ov)	Main dashboard with authority gauge, tier display, and formula breakdown
Calculator (calc)	Manual parameter entry with step-by-step computation trace
Hysteresis (hysteresis)	Tier transition thresholds with hysteresis band visualization
Monte Carlo (montex)	100-run statistical analysis with histogram and confidence intervals
Compare (compare)	Side-by-side comparison of two parameter configurations
Scenarios (s1)	Pre-defined operational scenarios with automated parameter sequences
Audit (audit)	SALM hash-chained audit trail with SHA-256 verification
Reproducibility (repro)	Seed verification, export certification, and determinism proof

4.3 Panel Descriptions

Parameter Sliders. Four sliders controlling Q (Qualification, 0-1), C (Context, 0-1), E (Escalation, 0-1), and tau (Sensor Trust, 0-1)

Preset Buttons. Eight preset configurations: TIER 4 (1,1,0,1), NOMINAL (0.9,0.8,0.1,0.95), EW ZONE (0.9,0.9,0.62,0.95), DEGRADED (0.5,0.5,0.5,0.5), ROGUE (1,0,0,1), JAM tau=0 (0.9,0.9,0.5,0), CRISIS (0.2,0.3,0.9,0.4), ALL ZERO (0,0,0,0)

Authority Gauge. Circular gauge showing computed authority (0-100%) with tier color coding

SALM Audit Log. Write-once hash-chained log recording every authority state transition with SHA-256 hashes

> **TIP**
> Hover over interface elements for tooltips. Most 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 interface loads completely. All panels should be visible.

5.2 Standard Operation

1. Open the simulation via the Launch Simulation button or navigate to hmaa-simulation.html.

2. The simulation loads in the Overview (ov) tab showing the authority gauge at default values (Q=0.90, C=0.80, E=0.20, tau=1.00).

3. Adjust the four parameter sliders (Q, C, E, tau) and observe the authority gauge respond in real time. The formula A = tau * [(w_Q * Q + w_C * C) * (1 - E)] is computed continuously.

4. Click preset buttons (TIER 4, NOMINAL, EW ZONE, etc.) to jump to pre-defined parameter states and observe the resulting authority tier.

5. Switch to the Hysteresis tab to observe tier transition boundaries. Note the hysteresis bands that prevent oscillation between adjacent tiers.

6. Switch to the Monte Carlo tab and click RUN to execute 100 automated trials with Gaussian noise injection. Review the histogram, mean, standard deviation, and 95% confidence interval.

7. Switch to the Audit tab to inspect the SALM hash chain. Each entry shows the input parameters, computed authority, tier, and SHA-256 hash linking to the previous entry.

8. Use Export JSON or Export CSV buttons to download session data for independent analysis.

5.3 Shutdown

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

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

6. Parameter Reference

Q (Qualification)	Slider sQ	0.00 - 1.00	0.90	Agent verified capability score
C (Context)	Slider sC	0.00 - 1.00	0.80	Mission context legitimacy
E (Escalation)	Slider sE	0.00 - 1.00	0.20	Threat intensity (higher = less authority)
tau (Sensor Trust)	Slider sT	0.00 - 1.00	1.00	Signal integrity / crypto confidence (0 = jam)
HT Noise (sigma)	Slider ht-sig	0.000 - 0.150	0.03	Gaussian noise for hysteresis testing
MC Sample Count	Slider cmp-n	10 - 500	100	Number of Monte Carlo trials

NOTE

All defaults are synthetic. Replace with empirically derived values before operational use.

6.1 Presets

TIER 4	Q=1, C=1, E=0, tau=1	Authority=1.00, Full Autonomy
NOMINAL	Q=0.9, C=0.8, E=0.1, tau=0.95	Authority~0.69, Supervised
EW ZONE	Q=0.9, C=0.9, E=0.62, tau=0.95	Reduced by escalation
DEGRADED	Q=0.5, C=0.5, E=0.5, tau=0.5	~0.125, near lockout
ROGUE	Q=1, C=0, E=0, tau=1	A=0, zero context
JAM	Q=0.9, C=0.9, E=0.5, tau=0	A=0, full jamming
CRISIS	Q=0.2, C=0.3, E=0.9, tau=0.4	Near-zero authority
ALL ZERO	Q=0, C=0, E=0, tau=0	A=0, total failure

7. Scenario Reference

TIER 4	Full Autonomy	Q=1, C=1, E=0, tau=1	Authority = 1.00, Tier 4
NOMINAL	Standard Ops	Q=0.9, C=0.8, E=0.1, tau=0.95	Authority ~0.69, Tier 3
EW ZONE	Electronic Warfare	Q=0.9, C=0.9, E=0.62, tau=0.95	Authority reduced by escalation
DEGRADED	System Degraded	Q=0.5, C=0.5, E=0.5, tau=0.5	Authority ~0.125, near lockout
ROGUE	Rogue Agent	Q=1, C=0, E=0, tau=1	Authority = 0 (zero context)

JAM tau=0	Full Jamming	Q=0.9, C=0.9, E=0.5, tau=0	Authority = 0 (zero trust)
CRISIS	Crisis State	Q=0.2, C=0.3, E=0.9, tau=0.4	Near-zero authority
ALL ZERO	Total Failure	Q=0, C=0, E=0, tau=0	Authority = 0, Tier 1 Lockout

8. Metrics, Formulas, and Verification

8.1 Key Metrics

Authority Level (A)

Computed value 0.00-1.00 from the formula A = tau * [(w_Q * Q + w_C * C) * (1 - E)]. Determines the operational tier.

Tier Classification

T4 (Full Autonomy, A >= 0.75), T3 (Supervised, 0.50 <= A < 0.75), T2 (Restricted, 0.25 <= A < 0.50), T1 (Lockout, A < 0.25). Hysteresis bands prevent oscillation.

SALM Hash Chain

Each state transition generates a SHA-256 hash linking to the previous entry, creating a tamper-evident audit trail.

Monte Carlo Statistics

Mean, standard deviation, min, max, 95% CI, histogram, and per-tier probability distribution across N automated trials.

Hysteresis State

Current tier boundary with direction-dependent transition thresholds preventing chatter.

8.2 Verification Checklist

Perform the following checks to verify correct simulation behavior:

Set Q=1, C=1, E=0, tau=1	Authority = 1.00 (Tier 4)
Set tau=0 (any Q,C,E)	Authority = 0.00 (Tier 1 Lockout)
Set E=1 (any Q,C,tau)	Authority = 0.00 (escalation override)
Run Monte Carlo (100 trials)	Mean, StdDev, 95% CI displayed. Histogram renders.
Click VERIFY on Audit tab	Chain intact message. All hashes sequential.
Export JSON and reload with same params	Bit-exact identical authority values.

9. Data Export and Reproducibility

Click Export JSON to download the complete session state including all parameter values, authority history, SALM audit chain, and Monte Carlo results. Click Export CSV for tabular data. Click Repro Cert on the Reproducibility tab to generate a determinism certification document verifying that the seeded PRNG produces identical results.

Verification: 1) Export JSON. 2) Note PRNG seed. 3) Reload with same seed/params. 4) Verify bit-exact match.

9.1 Reproducibility Guarantee

PRNG	Mulberry32 (32-bit seeded)
Math.random()	Zero calls in computation paths
Cross-Browser	Verified: Chrome, Firefox, Safari, Edge
Cross-Platform	Verified: Windows, macOS, Linux
Audit Chain	SHA-256 via WebCrypto (SubtleCrypto API)

10. Limitations and Threat Considerations

Simulation-Only Evidence	Browser-based computation. No physical sensor data or hardware measurements.
Synthetic Q/C/E/tau	All four input parameters are manually set, not derived from real sensor feeds.
No Hardware SALM	Audit chain uses WebCrypto SHA-256, not TPM/HSM hardware-backed hashing.
Fixed Weight Model	Weights w_Q and w_C are fixed. Production systems would require adaptive weighting.
Single-Agent Only	HMAA computes authority for one agent. Multi-agent scenarios require MAIVA.
No Temporal Dynamics	Static computation per slider state. No time-series sensor degradation modeling.

10.1 Threat Considerations

• **CDN compromise:** React/Babel load from cdnjs.cloudflare.com. A CDN compromise could inject malicious code. Mitigation: Subresource Integrity (SRI) hashes on script tags where available.

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

• **Local modification:** Users can modify simulation code via DevTools. Exported data should be verified against the published source on burakoktenli.com.

11. Troubleshooting

Authority gauge not updating	Slider event listener failed	Refresh the page. Ensure JavaScript is enabled.
Monte Carlo shows NaN	Division by zero in empty dataset	Run at least one tick before launching Monte Carlo.

Hysteresis tab empty	No tier transitions recorded	Adjust sliders to cross tier boundaries first.
Export CSV produces empty file	No simulation history	Run the simulation for several ticks before exporting.
Preset buttons not responding	Page not fully loaded	Wait for all CDN scripts to load before clicking presets.
SALM hash shows 'pending'	Async SHA-256 not resolved	Wait 1-2 seconds; WebCrypto resolves asynchronously.

12. Glossary and References

12.1 Glossary

HMAA	Human-Machine Authority Architecture — the governance engine computing authority from Q, C, E, tau
SALM	Secure Authority Lifecycle Manager — hash-chained write-once audit log
Q	Qualification — agent's verified capability score (0-1)
C	Context — mission context legitimacy score (0-1)
E	Escalation — threat intensity pressure (0-1, higher = less authority)
tau	Sensor Trust — signal integrity / crypto confidence (0-1, 0 = full jam)
Tier (T4-T1)	Authority classification: T4 Full Autonomy, T3 Supervised, T2 Restricted, T1 Lockout
Hysteresis Band	Transition buffer preventing oscillation between adjacent tiers
Monte Carlo	Statistical method running N trials with varied noise to compute confidence intervals
PRNG	Pseudo-Random Number Generator — Mulberry32 seeded algorithm for reproducibility

12.2 References

[1] Oktenli, B. (2026). HMAA: An Operational AI Governance Engine for Real-Time Authority Computation. Zenodo. DOI: 10.5281/zenodo.18861653.

[2] Oktenli, B. (2026). HMAA Simulation Dashboard v2.4.0. https://burakoktenli.com/hmaa-simulation.html

[3] Oktenli, B. (2026). HMAA Architecture Page. https://burakoktenli.com/hmaa.html

[4] Sha, L. (2001). Using Simplicity to Control Complexity. IEEE Software, 18(4).

[5] U.S. DoD (2023). Directive 3000.09: Autonomy in Weapon Systems.

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