AUTHREX SYSTEMS

Simulation User Guide

AUTHREX Master OS

Unified Operating System — 6-Node Distributed Actor Mesh

FIELD	VALUE
Document	Simulation User Guide
Version	1.0 — March 31, 2026
Filename	authrex-master-os.html
File Size	25 KB
Dependencies	THREE.js r128 (CDN), Web Workers, WebCrypto API
Browser	Chrome 90+ / Edge 90+ (WebGL + WebCrypto required)
Author	Burak Oktenli — Georgetown University
ORCID	0009-0001-8573-1667
License	CC BY 4.0 International

1. PREREQUISITES

Before opening this simulation: (1) Use Chrome 90+ or Edge 90+ (recommended). Firefox and Safari may have WebGL differences. (2) Ensure internet connectivity — this simulation loads THREE.js from a CDN. Without internet, the 3D visualization will show a fallback message but the governance engine continues. (3) Open the HTML file directly in the browser (double-click the file or drag into Chrome). No web server is required. (4) Allow the page to fully load before interacting with controls.

2. QUICK START

Open in Chrome. A unified dashboard loads with 3 tabs: 3D COP (kinematic Common Operating Picture), ERAM Charts (real-time probability graphs), and Provenance (SHA-256 audit table). 6 Web Workers spawn as distributed nodes. Select a scenario and click INJECT to begin.

3. STEP-BY-STEP WALKTHROUGH

Scenario: EW Spoof UCAV-1

The Master OS has two attack buttons (not a scenario selector). Each button spoofs a specific UCAV.

Step 1: Click '⚡ EW SPOOF UCAV-1' — Injects EW compromise into the first UCAV node.

- ▶️ **Observe:** UCAV-1 wireframe turns RED in TACTICAL COP tab
- ▶️ **Observe:** Telemetry table shows UCAV-1 status: COMPROMISED
- ▶️ **Observe:** P(Escalation) begins rising
- ▶️ **Observe:** SHA-256 hashes appear in AUDIT LEDGER tab

Step 2: Switch to ERAM TELEMETRY tab — Shows real-time P(Escalation) chart.

- ▶️ **Observe:** P(Escalation) line graph rising
- ▶️ **Observe:** Per-node trust history updating

Step 3: Switch to AUDIT LEDGER tab — Shows SHA-256 provenance entries.

- ▶️ **Observe:** Audit entries with SHA-256 hashes
- ▶️ **Observe:** Entries appear every 8 ticks
- ▶️ **Observe:** Newest entries at top (prepended)

Step 4: Watch for PBFT auto-trigger — If >66% of nodes report escalation, CARA fires automatically.

- ▶️ **Observe:** If triggered: compromised node quarantined automatically
- ▶️ **Observe:** If not triggered: node continues in COMPROMISED state until more nodes affected

Scenario: EW Spoof UCAV-2 (Cascade)

Click the second spoof button to compromise a second node, testing multi-node cascade dynamics.

Step 1: Click '⚡ EW SPOOF UCAV-2' — Compromises a second UCAV — now 2/6 nodes are affected.

- ▶️ **Observe:** Second UCAV wireframe turns RED
- ▶️ **Observe:** P(Escalation) rises more steeply with 2 compromised nodes

- ▶️ **Observe:** PBFT evaluation: 2/6 escalated — still below 2/3 threshold
- ▶️ **Observe:** Pipeline: MAIVA → QUORUM approaching

Step 2: Watch PBFT threshold — With 2/6 nodes compromised, the system is stressed but PBFT has not breached 2/3.

- ▶️ **Observe:** ESC/TOT shows 2/6 or higher as trust spreads
- ▶️ **Observe:** If other nodes' ACI drops below threshold, they may also vote escalation
- ▶️ **Observe:** Auto-CARA triggers if/when >4/6 nodes register escalation

Full Reset

Step 1: Click '↺ RESET' — Terminates all 6 Web Workers, clears state, respawns nodes.

- ▶️ **Observe:** All nodes return to green NOMINAL
- ▶️ **Observe:** P(Escalation) returns to 0.000
- ▶️ **Observe:** Audit ledger clears
- ▶️ **Observe:** Web Workers terminated and recreated

4. INTERFACE REFERENCE

4.1 Dashboard Metrics

METRIC	RANGE	MEANING
P(esc)	0.000 - 1.000	Composite escalation probability
MSG/s	Counter	DDS messages per second across the mesh (totalMsg * 20Hz)
Merkle	SHA-256 hex	Current audit ledger hash (updates every 8 ticks)
PBFT	>0.66 triggers	Proportion of escalated nodes. Auto-triggers CARA at 2/3.

4.2 Controls

BUTTON	FUNCTION
⚡ EW SPOOF UCAV-1	Compromise the first UCAV node via EW injection
⚡ EW SPOOF UCAV-2	Compromise the second UCAV node via EW injection
↺ RESET	Terminate all 6 Web Workers. Clear state. Respawn.
TACTICAL COP / ERAM TELEMETRY / AUDIT LEDGER	Three tab views: 3D wireframe COP, real-time P(esc) charts, SHA-256 audit table

4.3 ERAM Pipeline Indicators

The pipeline banner at the top of the screen shows 6 BLADE governance modules. Each indicator changes color based on simulation state:

COLOR	STATE	MODULES	MEANING
Green	NOMINAL	All modules	System operating within normal bounds
Amber	WARNING	MAIVA, ADARA	Anomaly detected, monitoring escalation
Red	CRITICAL	SATA, HMAA, CARA, FLAME	Compromise detected or interlock active

4.4 Node States

STATE	COLOR	MEANING
NOMINAL	Green	Normal operation
COMPROMISED	Red	Under attack
QUARANTINED	Grey	CARA interlock active

5. WHAT SUCCESS LOOKS LIKE

This simulation demonstrates the Master OS integrating all BLADE capabilities: distributed Workers, SHA-256 provenance, PBFT consensus, CARA interlock, and real-time ERAM charting in a single unified interface.

Key point: the 13 cumulative architectural fixes (setTimeout death spiral removed, O(N²) DDS batched to 20Hz, async closure capture, GPU dispose) make this the most thoroughly hardened simulation in the portfolio.

6. TROUBLESHOOTING

PROBLEM	SOLUTION
Black screen / no 3D	Requires internet for THREE.js CDN. Use Chrome with WebGL enabled.
Buttons don't respond	Buttons enable in sequence (phase guards). Select scenario first, then EXECUTE/INJECT.
Hash shows N/A	WebCrypto requires HTTPS or localhost. Open via file:// in Chrome.
Pipeline banner missing	Scroll to top. Banner is fixed-position. Check if boot animation is still playing.
Page feels slow	Close DevTools. Reduce browser tabs. Ensure GPU acceleration is enabled in browser settings.

END OF GUIDE