AUTHREX SYSTEMS

Simulation User Guide

ERAM Strategic Command

Master Escalation Risk Assessment — 5-Tab Analytical Suite

FIELD	VALUE
Document	Simulation User Guide
Version	1.0 — March 31, 2026
Filename	ERAM-Strategic-Command.html
File Size	86 KB
Dependencies	THREE.js r128 (CDN) — degrades gracefully without it
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). (2) Ensure internet connectivity for THREE.js CDN and Google Fonts (Oxanium). The core simulation engine works without CDN; only the LIVE DEMO 3D subplot requires it. (3) Open the HTML file directly in the browser. No server required. (4) Wait for the 3-second boot animation to complete before interacting. (5) For Monte Carlo tab: allow 10-15 seconds for 600-run computation.

2. QUICK START

Open the file in Chrome. Wait for the 3-second boot animation to complete. The main dashboard appears with 7 metrics across the top. Select a scenario from the left sidebar (default: first scenario). Click the green ▶ RUN button. Watch P(Escalation) climb in real-time. When it crosses critical thresholds, observe the ERAM pipeline banner react. Explore the 5 tabs: ESCALATION (main dashboard), MONTE CARLO (600-run campaign), ANALYSIS (formal verification + fuzz testing), AUDIT (hash chain), and LIVE DEMO (3D visualization).

3. STEP-BY-STEP WALKTHROUGH

Scenario: Run Any of 6 Threat Profiles

Step 1: Select scenario — Click any scenario in the sidebar: Flash War, AV Intersection, Maritime GPS Spoofing, Infrastructure Cascade, Cross-Domain, or HOTL Override

- ▶ **Observe:** Sidebar highlights selected scenario

Step 2: Click ▶ RUN — Starts the simulation. Tick counter begins incrementing.

- ▶ **Observe:** P(Escalation) starts rising from 0.000
- ▶ **Observe:** DCR compression ratio begins climbing
- ▶ **Observe:** Node trust values (tau) start decaying for attacked nodes

Step 3: Watch the attack inject — At the configured attack tick, adversarial pressure increases.

- ▶ **Observe:** P(Escalation) crosses 0.3 — pipeline turns AMBER
- ▶ **Observe:** ACI drops below 1.000 for compromised nodes
- ▶ **Observe:** STATUS changes from MONITOR to ALERT to CRITICAL

Step 4: Click ↺ RESET — Resets all state. You can select a different scenario.

- ▶ **Observe:** All metrics return to initial values
- ▶ **Observe:** Pipeline returns to green NOMINAL

Tab: ANALYSIS (Formal Verification + Fuzz)

Step 1: Click the ANALYSIS tab — Shows how changing parameters affects P(Escalation).

- ▶ **Observe:** Formal invariant results (5 checks), fuzz testing button (▶ FUZZ 50)
- ▶ **Observe:** Simplex Monitor shows safety boundaries and domain risk scores

Tab: AUDIT (Hash Chain Verification)

Step 1: Run a scenario first, then click the AUDIT tab — Shows 5 mathematical invariants and whether they held.

- ▶️ **Observe:** Escalation Bound: P(esc) stayed in [0,1] — should show PASS
- ▶️ **Observe:** HRW Safety, ACI Monotonicity, FLAME Hold, CRI Bound — all PASS
- ▶️ **Observe:** Audit chain integrity and Merkle root displayed

Tab: MONTE CARLO (600-Run Campaign)

Step 1: Click MONTE CARLO tab, then click ▶️ RUN 600 — Executes 600 independent simulation runs with randomized parameters.

- ▶️ **Observe:** Histogram of P(Escalation) distribution across 600 runs
- ▶️ **Observe:** Statistical summary: mean (μ), std dev (σ), min, max, P>0.6 percentage
- ▶️ **Observe:** Validates that governance bounds hold under random variation

Tab: LIVE DEMO (3D Visualization)

Step 1: Click the LIVE DEMO tab — Shows 3D wireframe visualization of the scenario network graph (requires THREE.js CDN).

- ▶️ **Observe:** 3D node graph with wireframe connections
- ▶️ **Observe:** Nodes colored by governance state
- ▶️ **Observe:** Visual representation of the scenario topology

Feature: Black Box Export

Step 1: Run a scenario, then click ⬇️ BLACK BOX button — Downloads a JSON file containing the full simulation record.

- ▶️ **Observe:** File contains: mission ID, Merkle root, all telemetry, invariant results
- ▶️ **Observe:** Signed with MurmurHash3 hash (non-cryptographic, labeled)
- ⚠️ *The Black Box uses MurmurHash3 (non-cryptographic) for integrity. This is labeled in the output.*

4. INTERFACE REFERENCE

4.1 Dashboard Metrics

METRIC	RANGE	MEANING
P(ESCALATION)	0.000 - 1.000	Composite probability that autonomous action exceeds authorized bounds. Green <0.3, amber 0.3-0.7, red >0.7
DCR	0 - 100+	Decision Compression Ratio: -10*log10(1-P(esc)). Logarithmic risk pressure scale.
CASCADE	0.000 - 1.000	Maximum Cascade Risk Index across all nodes. Shows worst-case domino effect.
HRW	0 - ∞	Human Recovery Window: time remaining before irreversible escalation. ∞ = safe.
ACI	0.000 - 1.000	Authority Confidence Index: composite trust * authority * fidelity. Below 0.25 = critical.
UNSAFE	0+	Count of formal invariant violations. Should always be 0 in normal operation.
STATUS	MONITOR/ALERT/ CRITICAL	Overall system state. MONITOR = nominal. CRITICAL = governance interlock active.

4.2 Controls

BUTTON	FUNCTION
▶️ RUN	Start simulation. Tick counter begins. Metrics update in real-time.
↺ RESET	Stop and reset all state. Select new scenario after reset.
⏭️ STEP	Advance simulation by one tick (manual stepping for analysis).
CSV	Export Monte Carlo results as CSV file.
JSON	Export configuration and formula definitions as JSON.
RPT	Export replay record for reproducibility analysis.
TLA+	Export formal TLA+ specification.
RPL	Export replay JSON with audit chain.
⬇️ BLACK BOX	Download complete signed Black Box record (JSON).
▶️ RUN 600	Execute 600-run Monte Carlo campaign (in MONTE CARLO tab).
▶️ FUZZ 50	Run 50-trial adversarial fuzz test (in ANALYSIS tab).

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	Node operating within authorized bounds. All governance checks passing.
COMPROMISED	Red	Node under adversarial pressure. Trust decaying. MAIVA voting in progress.
QUARANTINED	Red (dimmed)	CARA interlock fired. Authority=0. Isolated from mesh. Requires operator reset.

5. WHAT SUCCESS LOOKS LIKE

A successful demonstration shows: P(Escalation) rises under attack, the ERAM pipeline reacts in real-time (SATA turns red, MAIVA begins voting), CARA interlock fires when the threshold is crossed, P(Escalation) stabilizes after quarantine, all 5 formal invariants show PASS in the Verification tab, and the Monte Carlo campaign produces a bounded distribution with no outliers beyond [0,1].

The key takeaway for a reviewer: the governance mathematics provably bound autonomous behavior even under adversarial conditions. The simulation demonstrates this bound holds across 600+ randomized trials.

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.
Monte Carlo takes too long	600 runs is computationally intensive. Wait 10-15 seconds. Do not click during computation.
Boot animation stuck	Wait full 3 seconds. If stuck, reload page (Ctrl+R).
3D subplot blank but dashboard works	The 3D subplot uses THREE.js. Core simulation works without it.

END OF GUIDE