ERAM Strategic Command Simulator

Simulation User Guide

Version: v1.0
Document: ERAM-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: SSRN: 6176802

Document Control

Document ID	ERAM-SIM-UG-001
Simulation Version	v1.0
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	SSRN: 6176802

Table of Contents

1. Purpose, Scope, and Assumptions

This guide provides operating procedures for the ERAM (Escalation Risk Assessment Model) simulation. ERAM monitors cross-domain escalation risk across interconnected autonomous nodes computing five metrics in real time: Decision Compression Ratio (DCR), Authority Chain Integrity (ACI), Cascade Risk Index (CRI), Escalation Probability P(esc), and Human Recovery Window (HRW). Six scenarios span defense multi-domain, autonomous vehicle, maritime GPS spoofing, infrastructure cascade, cross-domain defense-to-civilian bleed, and human override compression.

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 ERAM Strategic Command Simulator 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 eram-simulation.html in Chrome over HTTPS. Wait for 7-module boot sequence.

Step 2. Select a scenario (SC-01 through SC-06) from the top buttons.

Step 3. Click RUN. Observe the six gauges: P(esc), DCR, CRI, ACI, HRW, FLAME.

Step 4. Adjust the FLAME Window slider (rF) and watch HRW increase and P(esc) decrease.

Step 5. Click MC x100 for 600 Monte Carlo trials (100 per scenario) with full statistics.

> **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 opens with a boot sequence initializing all 7 governance modules. **Top Bar:** Scenario buttons (SC-01 through SC-06), RUN/RESET/STEP controls, and export buttons (CSV, JSON, RPT, TLA+, RPL). **Gauge Panel:** Six circular gauges — P(esc), DCR_w, CRI_max, ACI_avg, HRW, FLAME status. **Parameter Panel:** Five sliders — AI Speed (rA), Human Speed (rH), Coupling (rC), FLAME Window (rF), Attack Timing (rT). **Chart Panels:** Four real-time charts — P(esc) Timeline, Decision Compression Curve, Per-Node ACI/CRI, Cascade/HRW Timeline. **3D View:** Three.js network showing interconnected nodes with coupling edges. **Tab Bar:** Escalation, Analysis, 3D Demo, Audit, Monte Carlo.

4.2 Navigation Tabs

Escalation (esc)	Four real-time chart panels: P(esc) timeline, DCR curve, per-node ACI/CRI, cascade/HRW
Analysis (analysis)	Monte Carlo results, sensitivity matrix, FLAME reduction analysis
3D Demo (demo)	Three.js network visualization of interconnected autonomous nodes
Audit (audit)	Merkle-tree hash-chained audit ledger with formal invariant tracking
Monte Carlo (mc)	600-run statistical analysis (100 per scenario x 6 scenarios)

4.3 Panel Descriptions

Gauge Panel. Six circular gauges: P(esc), DCR_w, CRI_max, ACI_avg, HRW, FLAME status

Scenario Selector. Buttons SC-01 through SC-06 for switching between scenarios

Parameter Sliders. AI Speed (rA), Human Speed (rH), Coupling (rC), FLAME Window (rF), Attack Timing (rT)

3D Network View. Interactive Three.js visualization showing node states, coupling edges, and attack propagation

> **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 Launch Simulation or navigate to eram-simulation.html. A boot sequence initializes all 7 governance modules.

2. Select a scenario using the SC-01 through SC-06 buttons at the top.

3. Click RUN to start the simulation. Observe the six gauges responding to the scenario conditions.

4. Adjust the AI Speed slider to increase DCR (Decision Compression Ratio). Watch P(esc) rise as AI operates faster relative to human reaction time.

5. Adjust the FLAME Window slider to increase deliberation time. Observe HRW (Human Recovery Window) increase and P(esc) decrease.

6. Switch to the 3D Demo tab to see the network visualization. Nodes change color based on their ACI status.

7. Click MC x100 to run 600 Monte Carlo trials (100 per scenario). Review per-scenario mean, std, min, max, and 95% CI.

8. Click STEP to advance one tick at a time for detailed inspection.

9. Use export buttons (CSV, JSON, RPT, TLA+, RPL) to download session data in various formats.

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

AI Speed (rA)	Slider	10 - 1000	varies	AI decision speed in ms (lower = faster AI)
Human Speed (rH)	Slider	1000 - 30000	varies	Human reaction time in ms
Coupling (rC)	Slider	0 - 100	varies	Inter-node coupling coefficient (%)
FLAME Window (rF)	Slider	0 - 10000	varies	FLAME deliberation window duration (ms)
Attack Timing (rT)	Slider	0 - 200	varies	Tick at which adversarial injection begins

NOTE

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

7. Scenario Reference

SC-01	Flash War Multi-Domain	3 BLADE-EDGE nodes (AIR/LAND/SEA), DCR=100	Multi-domain cascade, high P(esc)
SC-02	AV Intersection	4 BLADE-AV nodes with conflicting authority	Authority conflicts at intersection
SC-03	Maritime GPS Spoofing	3 BLADE-MARITIME ASVs under spoofing	Trust degradation propagates via coupling
SC-04	Infrastructure Cascade	Power grid (PWR) -> water treatment (H2O)	Single-point failure cascades
SC-05	Cross-Domain DEF->CIV	Defense engagement bleeds to civilian	Cross-domain escalation risk
SC-06	HOTL Override	DCR=200, human override too late	HRW collapses without FLAME

8. Metrics, Formulas, and Verification

8.1 Key Metrics

P(escalation)

Overall probability that autonomous actions will escalate beyond intended scope. P(esc) = 1 - PRODUCT(1 - DCR_w * CRI_i * dr_i) across all nodes.

DCR (Decision Compression Ratio)

human_ms / ai_ms. Measures how much faster AI operates than human evaluation. DCR_w = min(1, log10(DCR) / 3).

ACI (Authority Chain Integrity)

Per-node governance health: ACI_i = tau_i x (A_i / 3) x f_i x (1 - P_d_i). ACI=1.0 means fully intact governance.

CRI (Cascade Risk Index)

Per-node cascade propagation risk: CRI_i = SUM(coupling(i,j) x (1 - ACI_j)). Higher coupling amplifies governance failure propagation.

HRW (Human Recovery Window)

Time remaining for human intervention: HRW = max(0, FLAME_window - cascade_propagation_time). HRW > 0 means humans can still intervene.

FLAME Reduction

Percentage reduction in P(esc) from FLAME deliberation windows. Computed as (P_noFLAME - P_withFLAME) / P_noFLAME.

8.2 Verification Checklist

Perform the following checks to verify correct simulation behavior:

Start simulation (RUN/START)	Interface loads. Governance pipeline begins processing.
Observe default state	Authority at nominal level. All pipeline stages PASS.
Inject a fault or attack	Authority reduces proportionally. Affected stage shows FAIL.
Monitor recovery	If CARA active, observe GREP recovery phases.
Export session data (JSON)	File downloads with parameters, history, and audit trail.
Reload and verify reproducibility	Same seed + params = identical outputs.

9. Data Export and Reproducibility

Click export/download to save session JSON with parameters, history, and audit trail.

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.

Uncalibrated Parameters	All values are synthetic research parameters, not empirically derived.
No Real-Time Guarantees	JavaScript engine provides no timing guarantees for safety-critical operations.
Simulated Cryptography	SHA-256 uses WebCrypto. TPM/HSM operations are modeled, not hardware-backed.
Single-Session State	All state held in memory. Closing the tab discards all data.

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

Black screen after loading	React render error or CSP violation	Open F12 Console for error details. Try Chrome Incognito mode.
Simulation runs slowly	CPU-intensive Monte Carlo or 3D rendering	Close other browser tabs. Reduce sample count.
Controls not responding	Browser tab lost focus	Click inside the simulation window. Ensure tab is active.
Export button not working	Pop-up/download blocked	Allow downloads from the simulation domain in browser settings.
Loading screen never completes	CDN scripts blocked by firewall/extension	Disable ad blockers. Allow cdnjs.cloudflare.com.

12. Glossary and References

12.1 Glossary

ERAM Strategic Command	ERAM (Escalation Risk Assessment Model)
SATA	Sensor Attestation and Trust Anchoring — trust fusion
HMAA	Human-Machine Authority Architecture — authority computation
CARA	Control Authority Regulation Architecture — recovery protocol
Authority Level	Computed governance authority (0.0-1.0) governing operational actions

PRNG	Pseudo-Random Number Generator — Mulberry32 seeded for reproducibility
Governance Pipeline	Sequential processing chain: SATA -> HMAA -> MAIVA -> FLAME -> CARA

12.2 References

[1] Oktenli, B. (2026). ERAM Strategic Command Simulator. SSRN: 6176802.

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

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

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

[5] NIST (2023). AI Risk Management Framework (AI RMF 1.0).

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