FLAME Deliberation Architecture Simulation

Simulation User Guide

Version: v5.11
Document: FLAME-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.19015618

Document Control

Document ID	FLAME-SIM-UG-001
Simulation Version	v5.11
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.19015618

Table of Contents

1. Purpose, Scope, and Assumptions 3
2. Quick Start (5-Step) 3
3. System Requirements and Security 4
4. Interface Layout and Navigation 4-5
5. Operating Procedures 5-6
6. Parameter Reference 6-7
7. Scenario Reference 7
8. Metrics, Formulas, and Verification 7-8
9. Data Export and Reproducibility 8-9
10. Limitations and Threat Considerations 9
11. Troubleshooting 9-10
12. Glossary and References 10

1. Purpose, Scope, and Assumptions

This guide provides operating procedures for the FLAME (Flash War Latency Architecture for Multi-Domain Escalation Control) simulation. FLAME implements a 5-state Circuit Breaker State Machine (NOMINAL, CAUTION, HOLD, FREEZE, LOCKOUT) with mandatory deliberation windows, Keep-Alive heartbeat monitoring, physical interlock requirements, and domain-specific delay calibration. It demonstrates how engineered latency preserves human decision authority in autonomous escalation loops.

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 FLAME Deliberation Architecture 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 flame-simulation.html in Chrome over HTTPS.

Step 2. Observe the Circuit Breaker State Machine starting in NOMINAL (green).

Step 3. Click ESCALATE STATE to move through CAUTION -> HOLD -> FREEZE.

Step 4. Click FORCE LOCKOUT to enter LOCKOUT state (requires physical interlock to exit).

Step 5. Click PHYSICAL INTERLOCK and enter the 6-digit code to reset to FREEZE.

> **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 is centered on the Circuit Breaker State Machine diagram. **Center Panel:** 5-state FSM visualization (NOMINAL green, CAUTION yellow, HOLD amber, FREEZE blue, LOCKOUT red) with animated transitions. Current state highlighted with sweep animation. **Top Controls:** ESCALATE STATE, DE-ESCALATE STATE, FORCE LOCKOUT buttons. **Bottom Panel:** Physical Interlock section with 6-digit code display and VERIFY button. Keep-Alive heartbeat monitor with pulse indicator. Deliberation window D(A) timer display. **Side Panel:** Escalation history timeline.

4.3 Panel Descriptions

Circuit Breaker State Machine. 5-state FSM visualization: NOMINAL (green), CAUTION (yellow), HOLD (amber), FREEZE (blue), LOCKOUT (red). Transitions animate in real time.

Escalation Controls. Buttons: ESCALATE STATE (increase escalation), DE-ESCALATE STATE (decrease), FORCE LOCKOUT (emergency), PHYSICAL INTERLOCK (hardware reset)

Deliberation Window. Dynamic delay D(A, tier, domain) computed from authority level, escalation tier, and operational domain

Keep-Alive Monitor. Heartbeat monitoring for human operator presence. Loss triggers automatic authority reduction.

Interlock Panel. 6-digit verification code entry for physical interlock reset. Required to exit LOCKOUT.

> **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 flame-simulation.html.

2. The simulation starts in NOMINAL state with the circuit breaker closed (green).

3. Click ESCALATE STATE to progressively increase escalation: NOMINAL -> CAUTION -> HOLD -> FREEZE.

4. Observe the deliberation window D(A) increase with each escalation level. Higher escalation = longer mandatory delay.

5. Click DE-ESCALATE STATE to reduce escalation. Note the asymmetric transitions: de-escalation requires deliberation too.

6. Click FORCE LOCKOUT to immediately enter LOCKOUT state. Note: software cannot exit LOCKOUT.

7. Click PHYSICAL INTERLOCK to initiate hardware reset. Enter the displayed 6-digit verification code to confirm human presence.

8. After successful interlock verification, the system resets to FREEZE state (not NOMINAL) requiring deliberate de-escalation.

9. Observe the Keep-Alive heartbeat indicator. If the heartbeat signal is lost, authority automatically reduces.

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

Parameters are pre-configured per scenario. See Section 4 for interface controls and the published paper for parameter derivation.

7. Scenario Reference

Continuous mode. Inject faults manually using controls in Section 5.

8. Metrics, Formulas, and Verification

8.1 Key Metrics

Circuit Breaker State

Current FSM state: NOMINAL (all actions permitted), CAUTION (advisory delays), HOLD (mandatory delays on critical actions), FREEZE (all autonomous actions suspended, human-only), LOCKOUT (all actions blocked, physical interlock required).

Deliberation Window D(A)

Computed delay in milliseconds before critical actions execute. D increases with escalation level and decreases with authority. Formula: D = base_delay * escalation_factor * (1 / authority).

Keep-Alive Status

Human operator heartbeat signal. Green = active, Yellow = warning (approaching timeout), Red = lost (triggers automatic authority reduction).

Interlock State

Physical interlock verification status. Required for LOCKOUT exit. 6-digit code ensures human physical presence at the control station.

Escalation History

Timeline of all escalation state transitions with timestamps and triggering conditions.

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 state machine. No hardware interlock validation.
No Physical Interlock Hardware	6-digit code is software-only. Production requires physical key/switch.
Simplified Delay Model	D(A) uses a parametric formula. Operational delays depend on hardware latency.
Single-Domain	Current simulation models one domain. Cross-domain FLAME interaction requires ERAM.
No Network Latency	Communication delays between nodes are not modeled in the state machine.

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

Cannot exit LOCKOUT	Software cannot de-escalate from LOCKOUT	Click PHYSICAL INTERLOCK and enter the displayed 6-digit code. Resets to FREEZE, not NOMINAL.
Interlock code rejected	Wrong code entered	Enter the exact code displayed on screen. Codes are case-sensitive.
Keep-Alive flashing red	Heartbeat timeout exceeded	Click the heartbeat button to send a pulse. Timeout is configurable.
State machine not animating	Simulation paused or no escalation	Click ESCALATE STATE to trigger a transition. Animation plays on state change.
Deliberation window shows 0ms	In NOMINAL state with low escalation	D(A) is minimal at low escalation. Increase escalation to see longer windows.

12. Glossary and References

12.1 Glossary

FLAME	Flash War Latency Architecture — deliberation window injection system
Circuit Breaker	5-state FSM: NOMINAL, CAUTION, HOLD, FREEZE, LOCKOUT
Deliberation Window	Mandatory delay D(A, tier, domain) before critical autonomous actions
Keep-Alive	Human operator heartbeat signal. Loss triggers authority reduction.
Physical Interlock	Hardware-verified human presence check. 6-digit code entry required.
Flash War	Conflict escalating from tactical to strategic faster than human intervention
Strategic Latency	Intentionally engineered delay to preserve human decision authority
FREEZE	All autonomous actions suspended. Human-only operation mode.

12.2 References

[1] Oktenli, B. (2026). FLAME: Flash War Latency Architecture v5.11. Zenodo. DOI: 10.5281/zenodo.19015618.

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

[3] Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. W.W. Norton.

[4] Altmann, J. & Sauer, F. (2017). Autonomous Weapon Systems and Strategic Stability. Survival, 59(5).

[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