

# BLADE-INFRA Governance Simulator

## Simulation User Guide

Version: v6.0

Document: INFRA-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.19277887](https://doi.org/10.5281/zenodo.19277887)

# Document Control

<b>Document ID</b>	INFRA-SIM-UG-001
<b>Simulation Version</b>	v6.0
<b>Author</b>	Burak Oktenli — Georgetown University — ORCID 0009-0001-8573-1667
<b>Date / Revision</b>	April 2026 / Rev 1.0 — Initial Release
<b>Classification</b>	UNCONTROLLED — Research Artifact
<b>Related Artifact</b>	DOI: 10.5281/zenodo.19277887

## 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 BLADE-INFRA simulation implementing governance for ICS/SCADA critical infrastructure systems. Three scenarios cover power grid (138kV transformer with ADE9000 THD analysis), water treatment (chlorine pump overdose), and pipeline leak detection (48-inch steel pipeline with H2S alarm). The simulation features a vintage CRT terminal live mode, 11-stage governance pipeline including ERAM escalation authority, Sensitivity Analysis, Fault Tree Analysis, and MITRE ATT&CK; for ICS mapping.

**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 BLADE-INFRA Governance 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 the simulation HTML file in Chrome over HTTPS.

**Step 2.** Review the interface panels and identify the main controls.

**Step 3.** Click RUN or START to begin the simulation loop.

**Step 4.** Observe the governance pipeline processing sensor inputs through all modules.

**Step 5.** Use export/download buttons to save session data as JSON for verification.

### 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 visualizes critical infrastructure scenarios with ASCII art. **Top Panel:** Scenario selector (Power Grid, Water Treatment, Pipeline, Cyber Attack) with ASCII art representation of the active ICS topology. **Center Panel:** Sensor array with real-time readings (CT, PT, THD, RTD, Flow, pH, Cl2, Pressure, H2S) showing values, nominals, and trust scores. 11-stage governance pipeline (SENSORS through EFFECTOR including ERAM). Authority gauge with actuator action status. **CRT Mode:** Vintage terminal display for real-time telemetry. **Tab Bar:** Main View, Sensitivity Analysis, Fault Tree Analysis, MITRE ATT&CK; for ICS.

### 4.2 Navigation Tabs

Main View	ICS scenario visualization with sensor readings, pipeline status, and authority gauge
Sensitivity Analysis	Parameter sensitivity visualization showing authority response to sensor variations
Fault Tree Analysis	Root cause analysis mapping failure modes to contributing factors and probabilities
MITRE ATT&CK; for ICS	Attack technique mapping showing which ICS-specific attacks are detected by the governance pipeline

### 4.3 Panel Descriptions

**ICS Scenario Panel.** ASCII art visualization of the active scenario (power grid, water treatment, or pipeline)

**Sensor Array.** ICS-specific sensors with real-time readings, nominal values, and trust scores

**11-Stage Pipeline.** SENSORS -> ADARA -> SATA -> IFF -> HMAA -> MAIVA -> FLAME -> ERAM -> CARA -> BDA -> EFFECTOR

**CRT Terminal.** Vintage terminal interface showing real-time governance pipeline telemetry

**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 blade-infra-simulation.html.
2. The simulation initializes with the Power Grid scenario showing a 138kV transformer with Phase B overcurrent (340%).
3. Observe the sensor array: CT-A, CT-B (alarm), CT-C, PT-A, PT-B (warning), THD (alarm), RTD (warning) show real-time values.
4. Watch the 11-stage governance pipeline process the sensor data. Note ERAM (Escalation Authority) between FLAME and CARA.
5. Switch scenarios using the scenario selector: Power Grid (breaker trip), Water Treatment (pump shutoff), Pipeline Leak (valve shutoff).
6. Switch to the Sensitivity Analysis tab to see how authority changes as individual sensor values are varied.
7. Switch to the Fault Tree Analysis tab to see root cause diagrams for each failure scenario.
8. Switch to the MITRE ATT&CK; for ICS tab to see which attack techniques (T0800-series) map to governance pipeline detections.
9. Enable CRT Terminal mode for a vintage terminal display of real-time pipeline telemetry.

### 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

POWER	Power Grid Fault	Phase B 340% overcurrent on 138kV transformer	BREAKER TRIP action, authority drops
WATER	Water Treatment	Chlorine pump 280% overdose	PUMP SHUTOFF action, pH/Cl2 alarms
PIPE	Pipeline Leak	Flow differential + H2S alarm on 48-inch steel pipeline	VALVE SHUTOFF action, pressure anomaly
CYBER	Cyber Attack	SCADA network intrusion	ADARA detects anomalous commands

## 8. Metrics, Formulas, and Verification

### 8.1 Key Metrics

#### ICS Authority

Operational authority for the critical infrastructure controller. Governs actuator commands (breaker trips, pump shutoffs, valve closures).

#### Sensor Trust Array

ICS-specific sensors with weighted trust: Current Transformers (CT), Potential Transformers (PT), THD analyzer (ADE9000), RTD temperature, flow meters, pH sensors, Cl2 analyzers, pressure gauges, H2S detectors.

#### 11-Stage Pipeline

Complete governance pipeline with ERAM escalation authority: SENSORS -> ADARA -> SATA -> IFF -> HMAA -> MAIVA -> FLAME -> ERAM -> CARA -> BDA -> EFFECTOR.

#### SIL 3 Compliance

IEC 61508 Safety Integrity Level 3 monitoring. PFH (Probability of Failure on demand per Hour) tracked for safety functions.

#### NERC CIP Status

Critical infrastructure protection compliance: CIP-002 through CIP-014 requirement mapping.

#### MITRE ATT&CK; Coverage

ICS attack technique detection coverage: percentage of T0800-series techniques detectable by the governance pipeline.

### 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

BLADE-INFRA	BLADE-INFRA
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). BLADE-INFRA Governance Simulator. DOI: 10.5281/zenodo.19277887.
- [2] Oktenli, B. (2026). Simulation artifact. <https://burakoktenli.com/blade-infra-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](https://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](https://burakoktenli.com).

---

End of Document