

Operational-Technology Authority Gate Console

authrex.systems · browser simulation · seeded PRNG · synthetic data only · client-side execution

Scope. Everything in this document describes independent research artifacts: browser simulations, formal models, and unbuilt hardware reference designs. Maturity is self-assessed. Nothing here is a certification, an Authorization to Operate, a government endorsement, or evidence of a fielded system. Model-checking results apply to the stated finite model and assumptions, not to physical implementations.

PURPOSE

Simulates AUTHREX sitting between AI proposals and OT actuators: a safety floor prevents any AI write to a Safety-Instrumented Function, deterministic bounds checking clamps or denies out-of-envelope writes, and FLAME latency slows high-consequence actions for human confirmation.

CONTROLS AND DISPLAY

- The asset map shows synthetic OT assets; the proposal feed shows AI write requests.
- Scenario and seed reproduce runs; the V&V panel reruns packaged assertions.
- Within the stated configuration, high-consequence actions slow down for human confirmation and remain reversible.

READING THE VERDICTS

- AUTHORIZE / CLAMP / DENY per proposal; the floor-and-bound status bar tracks the two structural properties within this simulation.

LIMITATIONS

Self-assessed TRL 3 to 4 reference architecture demonstration aligned with NIST SP 800-82 and ISA/IEC 62443 concepts.

CANONICAL TERMINOLOGY

SATA: Sensor & Actor Trust Assessment · HMAA: Human-Machine Authority Allocation · ADARA: Adversarial Deception-Aware Reasoning · MAIVA: Multi-Agent Integrity Voting · FLAME: Forced Latency for Authority-Managed Escalation · CARA: Controlled Authority Recovery Architecture · ERAM: Escalation Risk Assessment Model