Onboard Authority Governance 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 onboard governance for orbital autonomy: sensor-trust scoring (SATA) gates spacecraft commands, and degraded or spoofed inputs drive a configured safe-hold response, so the spacecraft is protected from acting on untrustworthy data under the modeled conditions.

CONTROLS AND DISPLAY

- Orbit view shows the synthetic spacecraft and threat injections; the command queue shows gated actions.
- Inject spoofing, staleness, and link loss from the scenario panel; the seed reproduces runs.

READING THE VERDICTS

- EXECUTE / SAFE-HOLD / DENY per command; the trust trace shows the SATA scalar over time.
- The proposed governance layer is designed to reduce the risk of acting on spoofed or stale data; results apply to the modeled conditions only.

LIMITATIONS

Self-assessed TRL 2 to 3 concept demonstration mapped to the unbuilt BLADE-SPACE reference design; aligned conceptually with SPD-5.

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