

30-Day Production Soak

The flagship endurance record: full adversarial injection across the longest continuous window.

FINAL VERDICT
PASS

Internal adversarial soak testing. Independent third-party security audit remains pending.

SYSTEM	WINDOW	RUN	SOURCE
R-Series core - frozen tag audit-tob-v1.1.0 (697f339)	30 days continuous - closed Jul 2026	Final closing run	Machine-generated closing snapshot

Closing metrics

518,336 CYCLES 30-day window	0 CYCLE FAILURES failure rate 0	29/29 FAULTS SURVIVED 100% recovery	99.99% UPTIME continuous
3 ms LATENCY P95 full window	4 classes FAULT COVERAGE kill/drop/corrupt/partition	0 UNRECOVERED HALTS none recorded	PASS WINDOW CLOSE all gates earned

WHAT THIS RUN DEMONSTRATES

Thirty consecutive days on the frozen audit tree established long-window endurance and recovery across process kill, message drop, data corruption and network partition events. Every injected fault was survived, no cycle failed and latency remained stable.

EVIDENCE STATUS

Final internal test verdict: PASS. This is the headline sustained-operation record for audit scoping. It does not assert external audit completion, certification or flight qualification.

30-Day Production Soak

Technical results

Metric / gate	Closing result	State
Cycles completed	518,336	PASS
Cycles failed / failure rate	0 / 0	PASS
Faults injected / survived	29 / 29	PASS
Fault classes	process kill; message drop; data corruption; network partition	PASS
Recovery rate	100%	PASS
Uptime	99.99%	PASS
Latency P95	3 ms	PASS
Run status	PASS at window close	PASS
System-level anomalies	None recorded	PASS

Method and controls

- The exact frozen source tree submitted for audit remained under test for the full window.
- Fault events were scheduled across four production-relevant classes.
- Vacuum-pass prevention and null-until-earned verdicts governed closure.
- Closing results were machine-generated; no hand-retyped metrics were used.

ANOMALIES, LIMITS AND DISCLOSURES

No system-level anomaly was recorded during the 30-day window. Harness verdict disciplines were hardened in the parallel 72-hour campaign and govern the interpretation of this record.

RAW RECORD AND AUDIT SCOPE

Reference: closing JSON snapshot, full 30-day logs, fault-injection schedule, per-event recovery receipts and frozen source tree. Raw records are retained by DCS Labs. Internal evidence shortens, but does not replace, independent security audit.