Refactoring at Mission Speed:
Multi-Agent AI Meshes for Modernizing Air and Space C2 Systems

Travis Steele
Chief Architect & Field CTO - Defense, Red Hat

Breakout Session // Track 1

Agenda

- The Modernization Bottleneck
- Agent Mesh Architecture & Discovery
- Security, Air-Gap & Adoption Path
- Programmatic Impact & Principles
- Q&A Discussion

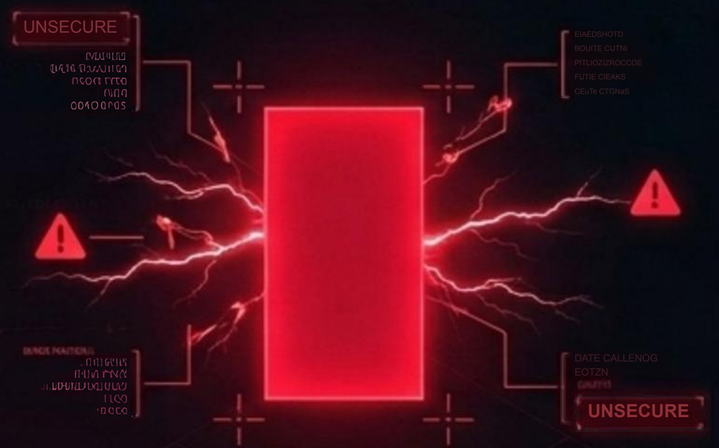


ENTERPRISE-TO-EDGE MODERNIZATION

MULTI-DOMAIN C3ISR,AIRBORNE,MARITIME,GROUND,SPACE

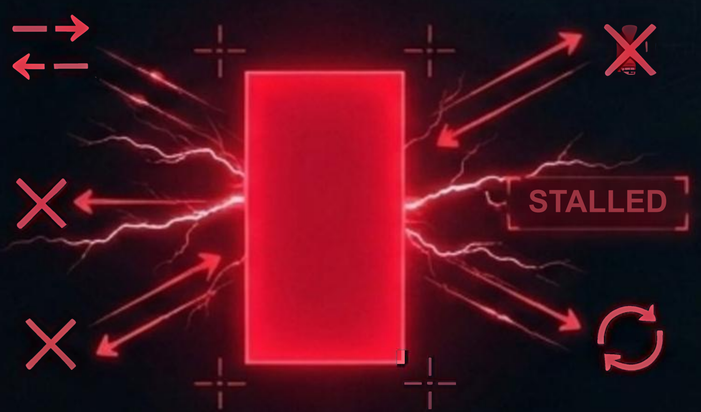
The Platform Dilemma: Technical Debt in Contested Environments

Compound Cyber Risk



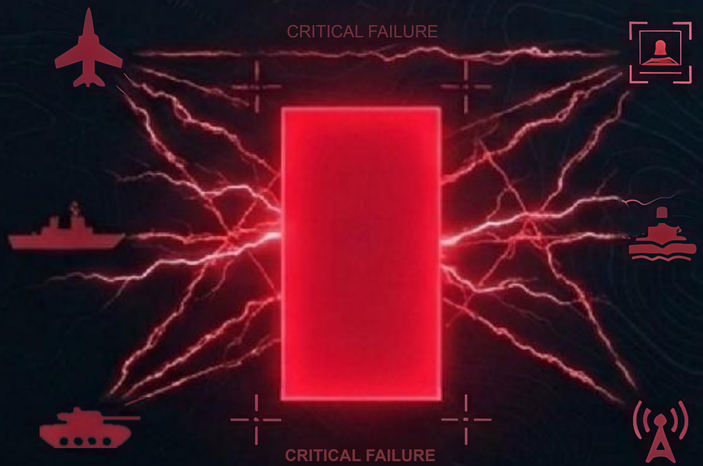
Monolithic legacy operating system baselines lock in unpatchable CVEs. High-risk, manual update processes create multi-month windows of cyber exposure across the kill web.

Operational Agility Failure



Rigid, paper-based requirements funnels stall warfighter feedback loops. Static software baselines cannot adapt against rapid, adaptive adversary threats.

Multi-Domain Reality



Technical debt compounds across air, sea, ground, and space C3ISR nodes, severely impairing decision dominance across the operational kill web.

The Anatomy of Modernization Stalls: The Engineering Resource Trap

ENGINEERING RESOURCE TRAP DIAGNOSTIC

70%

Bandwidth Burn

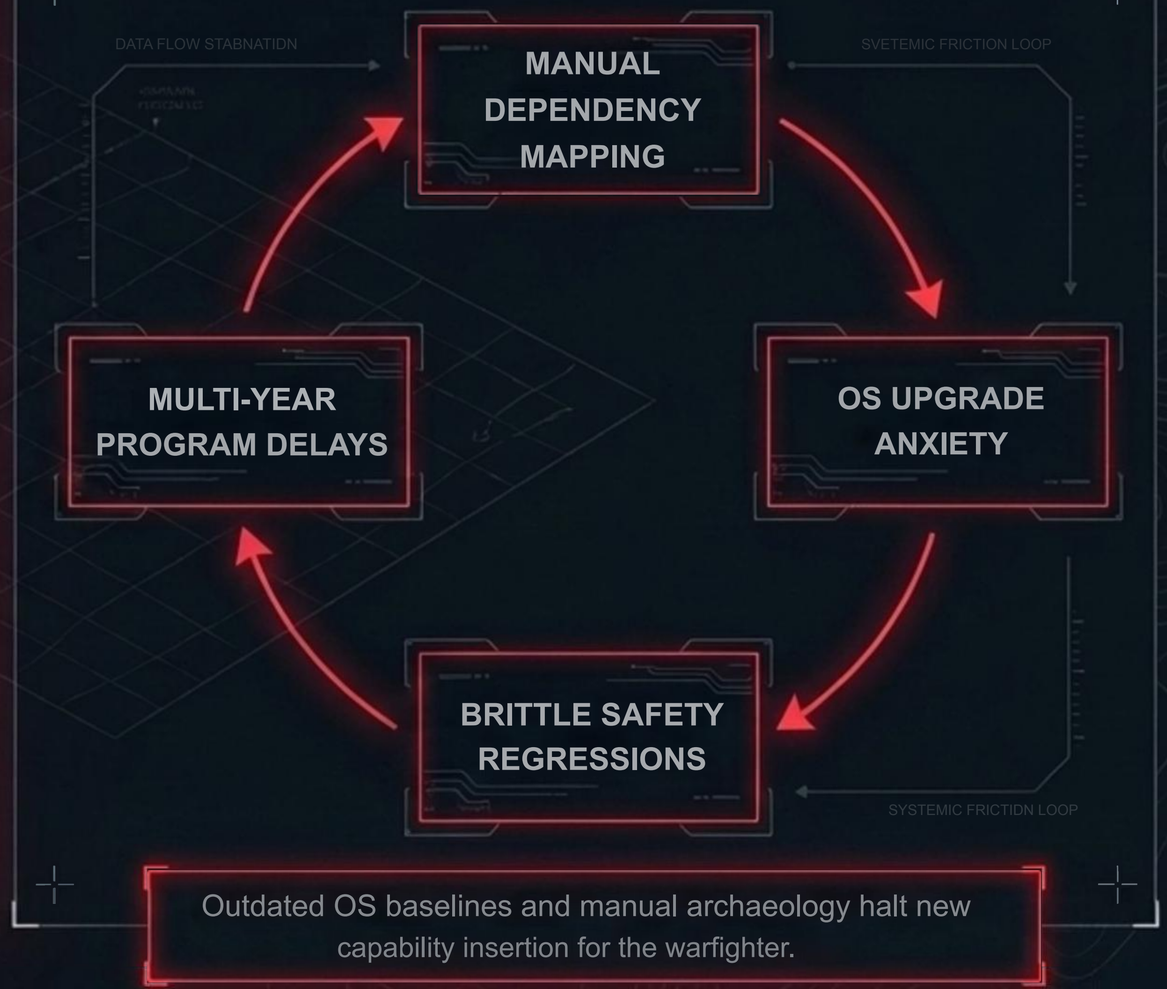
Senior engineering talent is consumed by manual code archaeology rather than building new front-line warfighting capabilities.

500

LOC/Week

The average manual refactoring throughput per developer when attempting to maintain safety-critical C2 baselines.

MODERNIZATION STALL CYCLE FLOW



Outdated OS baselines and manual archaeology halt new capability insertion for the warfighter.

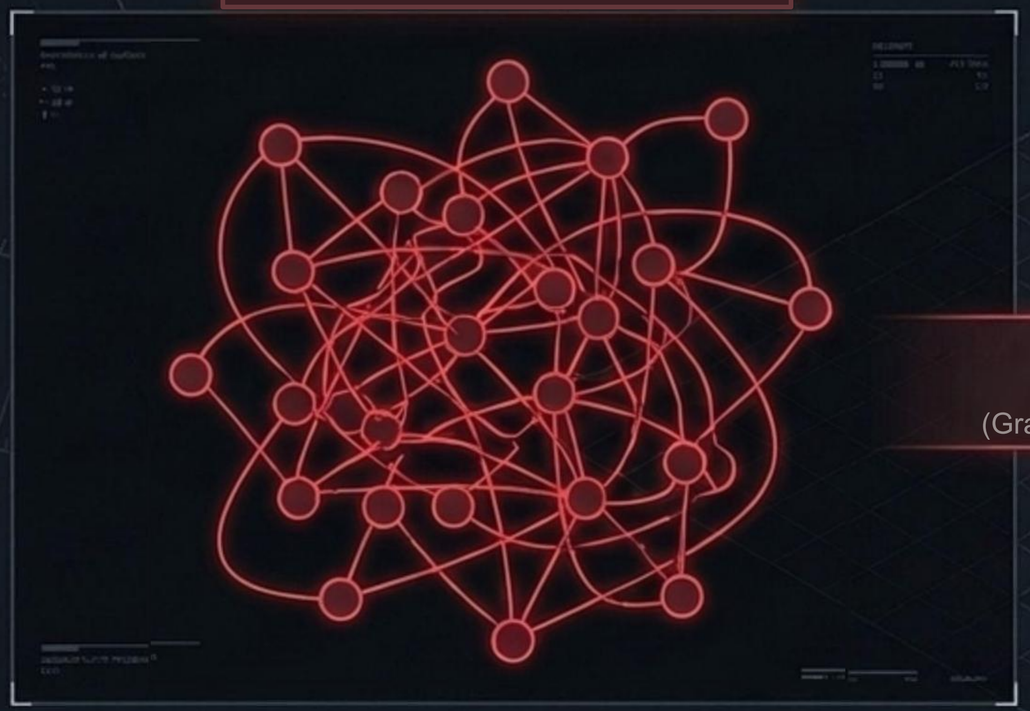
Operational Architecture: Programmatically Governed Agent Mesh



Engineers and Authorizing Officials retain final approval. Everything upstream of that gate is automated.

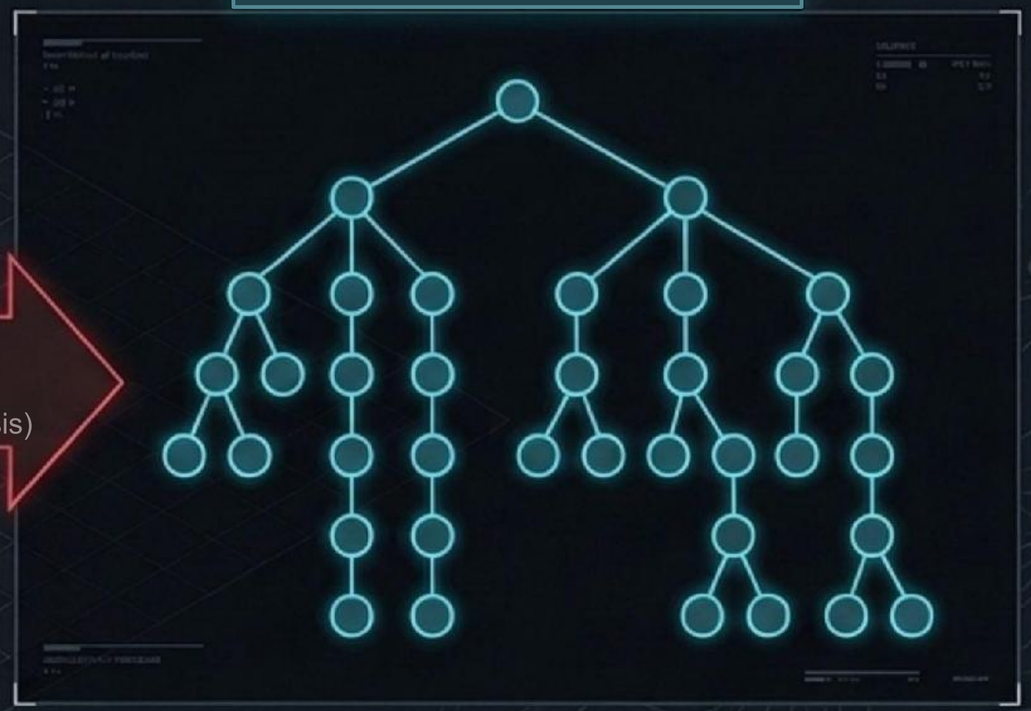
Automated Discovery via Semantic Graph Knowledge Mapping

Opaque Codebase



Semantic Graph
Knowledge Mapping
(GraphRAG + AST analysis)

Structured Intelligence



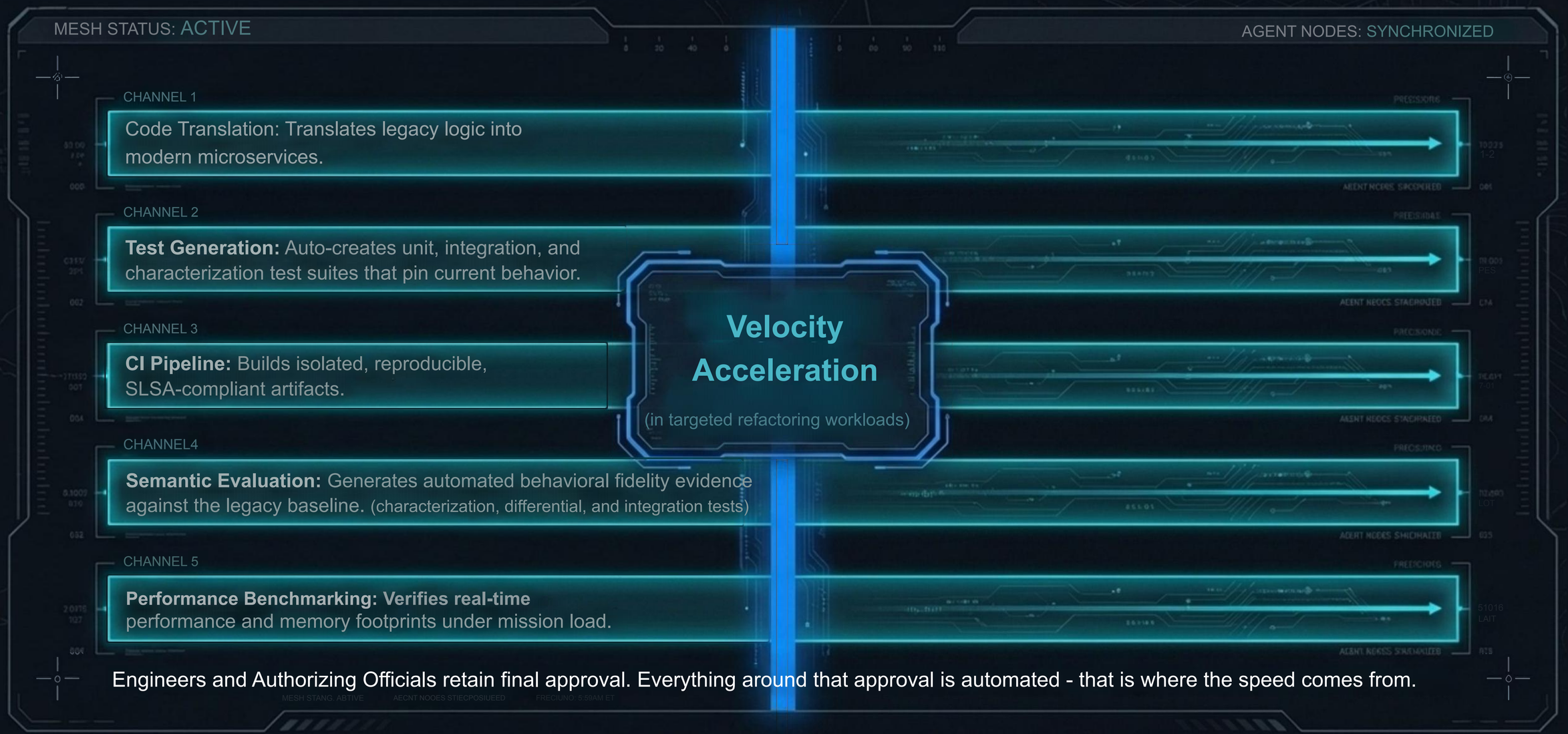
Ingesting legacy C, C++, Ada, COBOL, and Java source trees lacking manual documentation. Hidden call trees and circular dependencies obscure business logic.

Transforms the codebase into a queryable graph' Auto-generates prioritized user stories, interface definitions, and mission-linked engineering backlogs in hours instead of months

Acceleration Callout

Assessment time reduced from months to hours.
High automated structural coverage of parsed sources

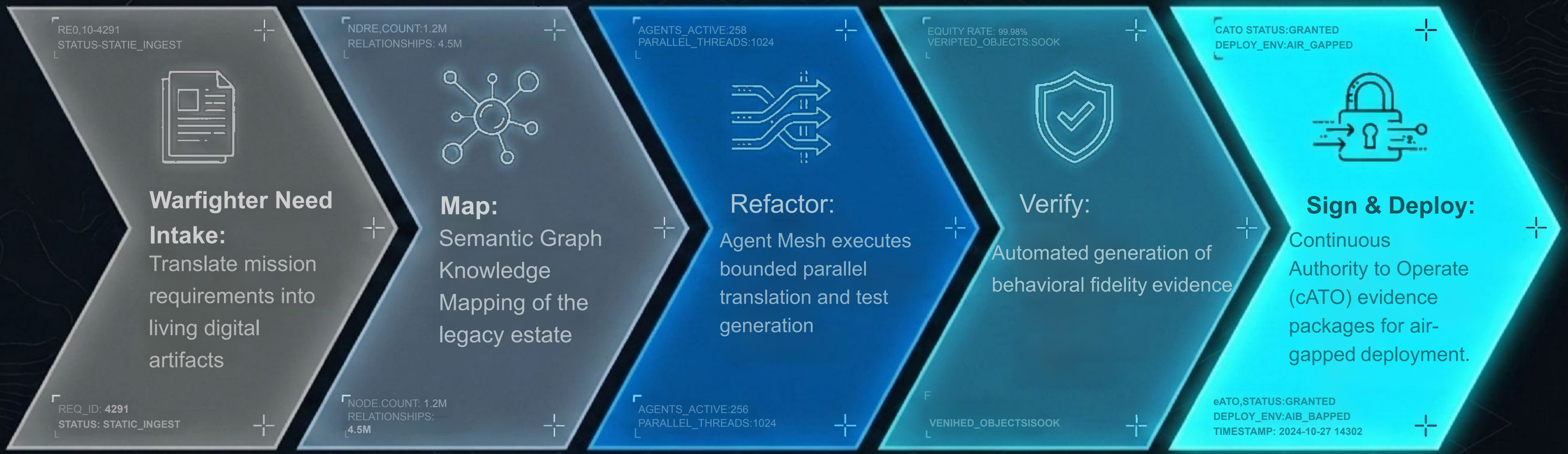
The Software Engineering Agent Mesh: Bounded Parallel Agents



Engineers and Authorizing Officials retain final approval. Everything around that approval is automated - that is where the speed comes from.

SY5ID:SE-AM-003

Technical Flow: End-to-End Capability Pipeline

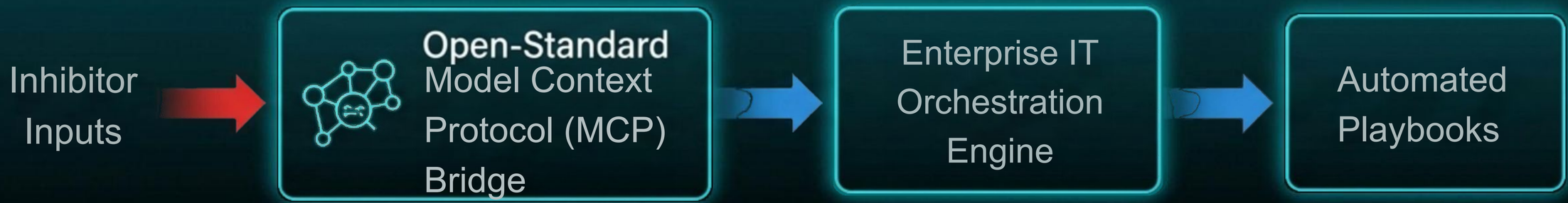


Machine-readable compliance artifacts are generated concurrently with the code; reducing human regression bottlenecks.

Platform Modernization: Autonomous Operating System Remediation

The Challenge: Systems locked on vulnerable legacy OS releases due to ~60 - 70% manual upgrade success rates.

Diagnostic Remediation Flowchart



- MCP Bridge diagnoses pre-upgrade inhibitors programmatically
- Precise remediation playbooks are generated and executed
- Complete, human-readable audit trails are produced
- Targeting 95%+ first-pass upgrade success
- Upgrade time reduced by ~90%



Disconnected & Air-Gapped Operations (DDIL)

Constraint: Forward-deployed assets must operate in Disconnected, Denied, Intermittent, and Limited environments.



Central Command Node





Forward-Deployed Edge Node

Edge Topology Diagram

- Unidirectional cross-domain transfer of cryptographically signed, immutable content bundles.
- High-Performance Optimized Inference Engine serves quantized models natively at the edge.
- Zero reliance on external APIs or enterprise cloud reachback for sustained operations.
- Operates fully under DDIL conditions while preserving enclave security

Supply Chain Security and AI Safety



SLSA Level 3 Build Isolation

Hardened environments with Hardware Security Module (HSM) signing, complete SBOMs, and attestations.

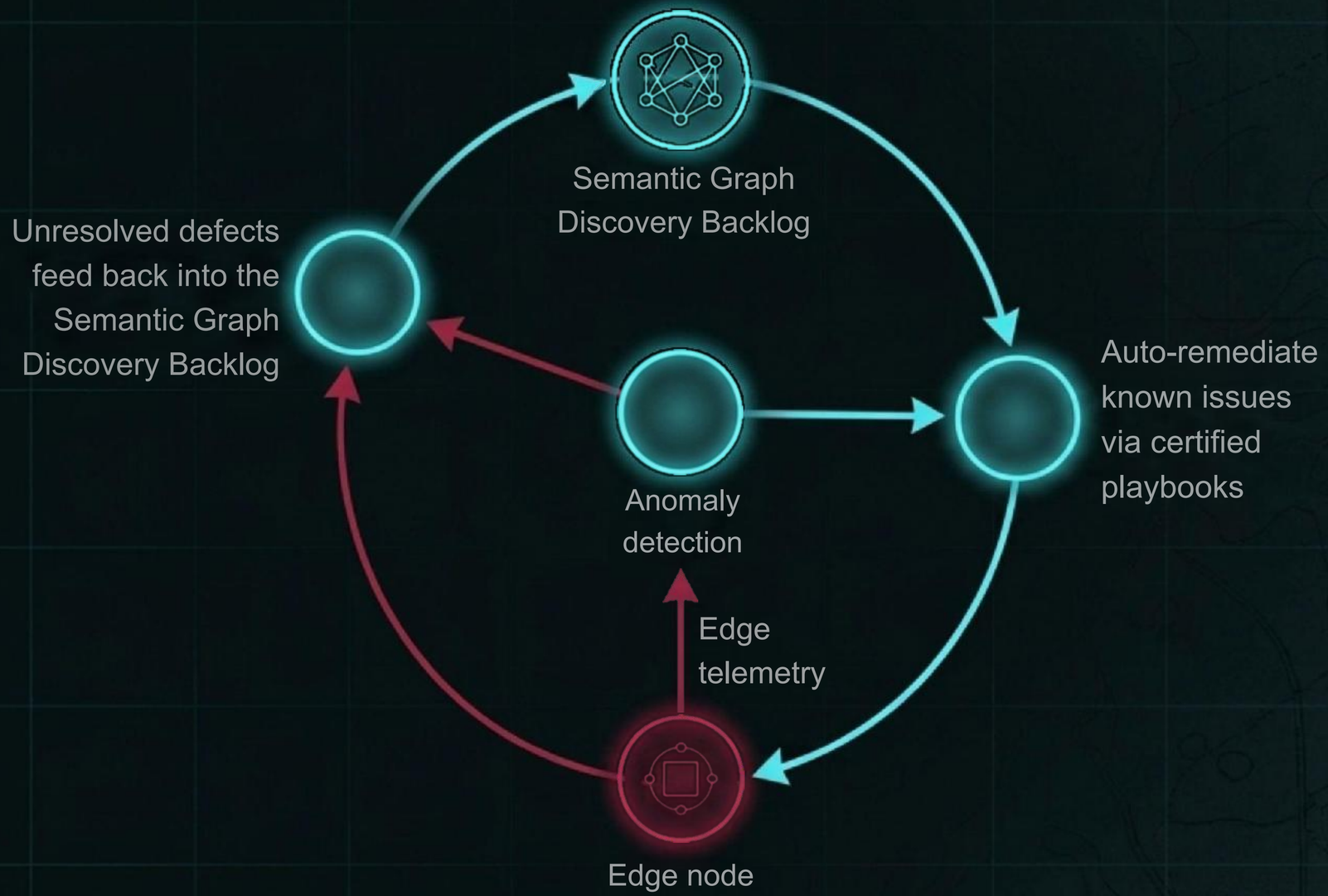
Cryptographically Signed Pipelines

Real-time CVE triage, backport patching, and curated package registries with rapid response SLAs

AI Safety Governance

Policy-to-controls automation mapped directly to NIST AI RMF guidelines and risk-driven safety testing.

Continuous Sustainment & Closed-Loop Operations



METRIC

Feedback Loop

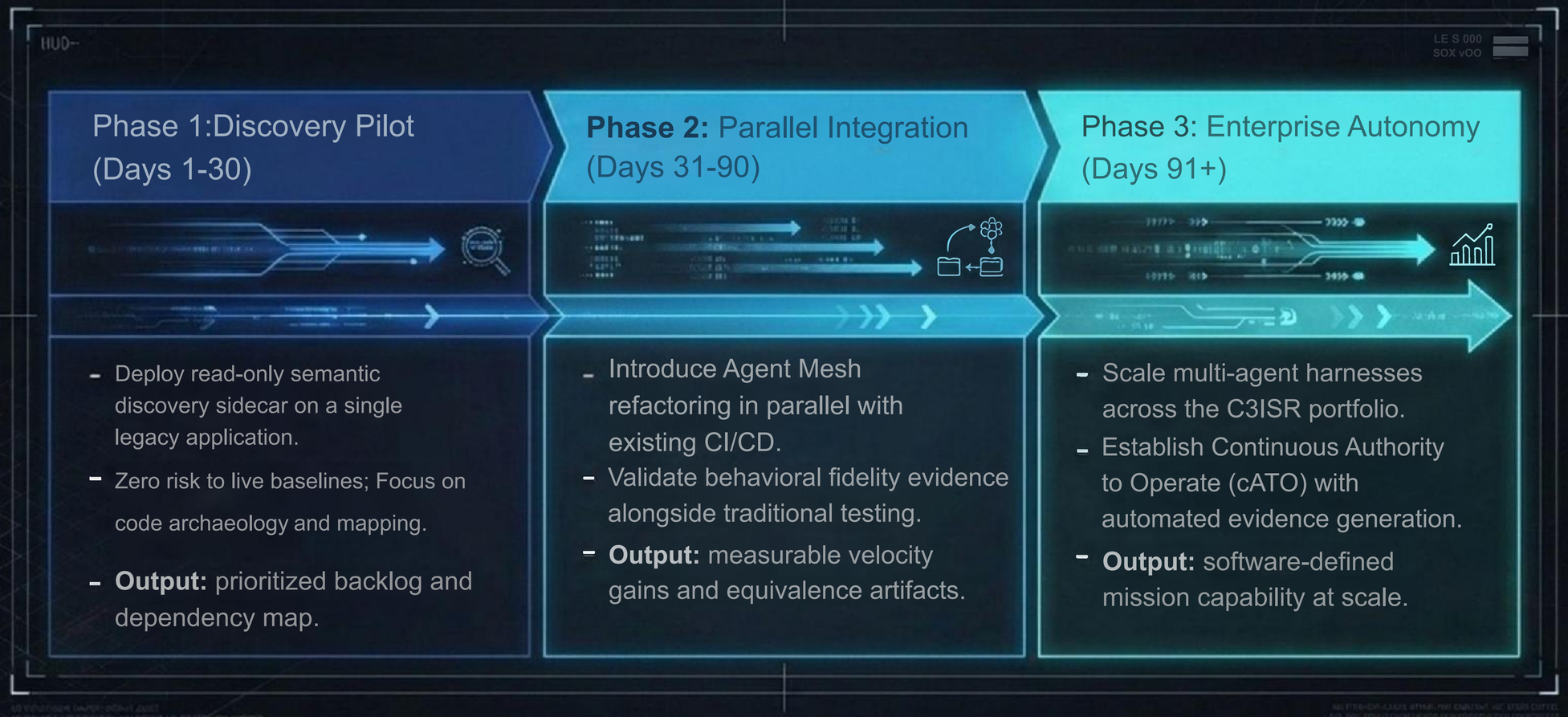
KEY MESSAGE

Reactive sustainment becomes proactive. Known issues are healed automatically; novel issues become new prioritized backlog items.

Impact

Order-of-magnitude reduction in edge Mean Time to Repair (days/weeks → hours/minutes)

Programmatic Adoption Playbook: Low-Risk Integration



Stakeholder & Programmatic Impact

AGILITY

Order of Magnitude

Requirements Compression

Dramatically compress multi-month requirement-to-backlog cycles (often by an order of magnitude)

VELOCITY

10x–50x

Refactoring Speedup

In targeted refactoring workloads without proportional headcount growth

RELIABILITY

95%+

Platform Upgrade Success

Targeting 95%+ first-pass OS upgrade success closing multi-month unpatchable CVE windows

RESILIENCE

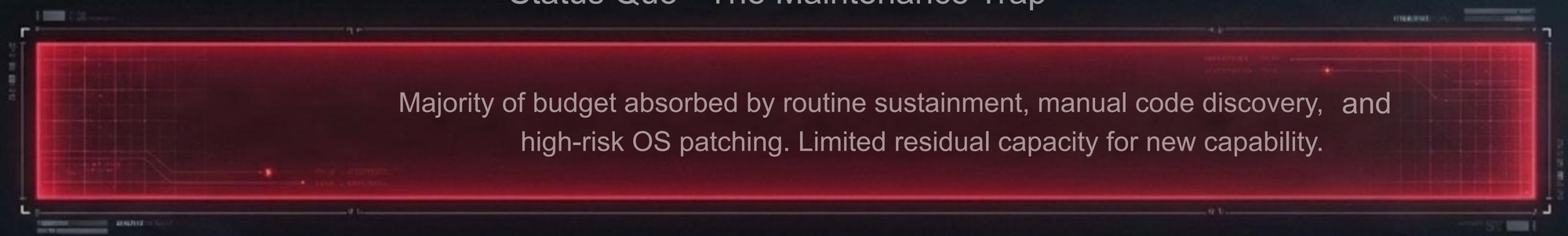
95%

Edge MTTR

Order-of-magnitude reduction in Mean Time to Repair (days/weeks → hours/minutes)

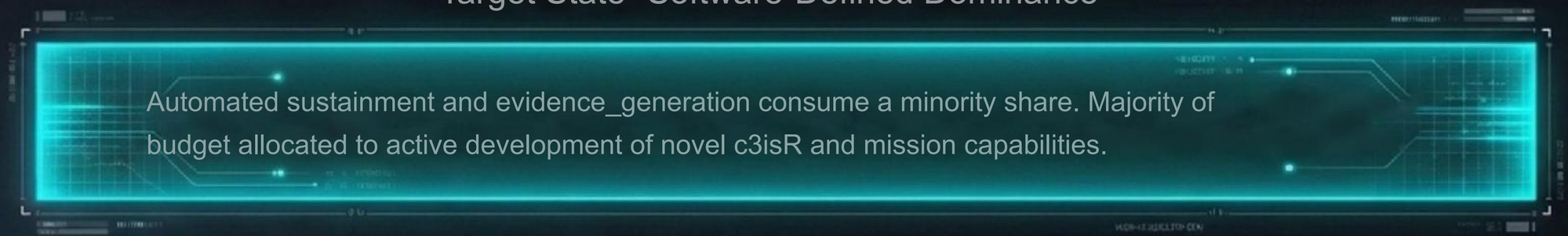
The Shift in Software Sustainment Economics

Status Quo - The Maintenance Trap



Majority of budget absorbed by routine sustainment, manual code discovery, and high-risk OS patching. Limited residual capacity for new capability.

Target State- Software-Defined Dominance



Automated sustainment and evidence_generation consume a minority share. Majority of budget allocated to active development of novel c3isR and mission capabilities.

Bottom line

By automating code archaeology, testing, verification, and OS remediation, programs shift the balance from a heavy legacy tax toward front-line warfighting capability.

Core Architectural Principles for the DAF



1. Modernization is Architectural

Solving technical debt across air, sea, ground, and space platforms requires changing the software factory model, not simply adding headcount to legacy code.



2. Bounded AI Acceleration

Multi-agent meshes deliver large velocity gains only when enclosed within strict policy-as-code guardrails and verifiable behavioral evidence. Humans and Authorizing Officials retain the final approval gate.



3. Data-Centric Assurance & Continuous Capability

Cryptographically signed, automated evidence enables Continuous Authority to Operate (cATO) and turns warfighter need into continuous, software-defined capability at the speed of mission.

Q&A

Refactoring at the Speed of Mission // Track 1

-> Code Archaeology & Semantic Mapping Pilots

-> AO/DAO Governance & cATO Evidence

-> Air-Gapped / DDIL Deployment Architecture