BUILDING TRUST IN AEROSPACE INFRASTRUCTURES:
RESILIENT OPERATIONS AND PROVENANCE-DRIVEN DATA SOVEREIGNTY

Andreas Schreiber, German Aerospace Center (DLR)

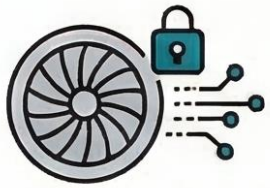
Andreas Schreiber's ISGC History: Security, Trust, and Provenance

15-year evolution of secure, traceable, and sovereign aerospace data infrastructures.

SECURITY TRUST PROVENANCE

2011

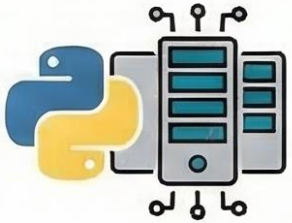
Industrial Security and Service Provenance



Focused on secure Grid policies for turbine manufacturing and service-oriented provenance architectures.

2012

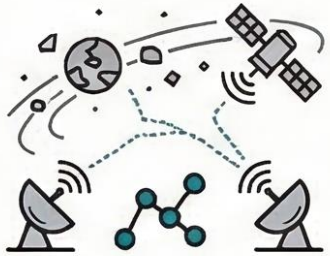
Python for Science and HPC



Highlighted Python's expanding role in engineering, scientific applications, and distributed high-performance computing.

2016

Traceable Space Debris Data Processing



Utilized BACARDI and Skynet systems to record processing provenance in graph databases for full traceability.

2018

Blockchain and Open Science Standards

Integrated the W3C PROV standard with blockchain technology to ensure scientific data integrity and reproducibility.

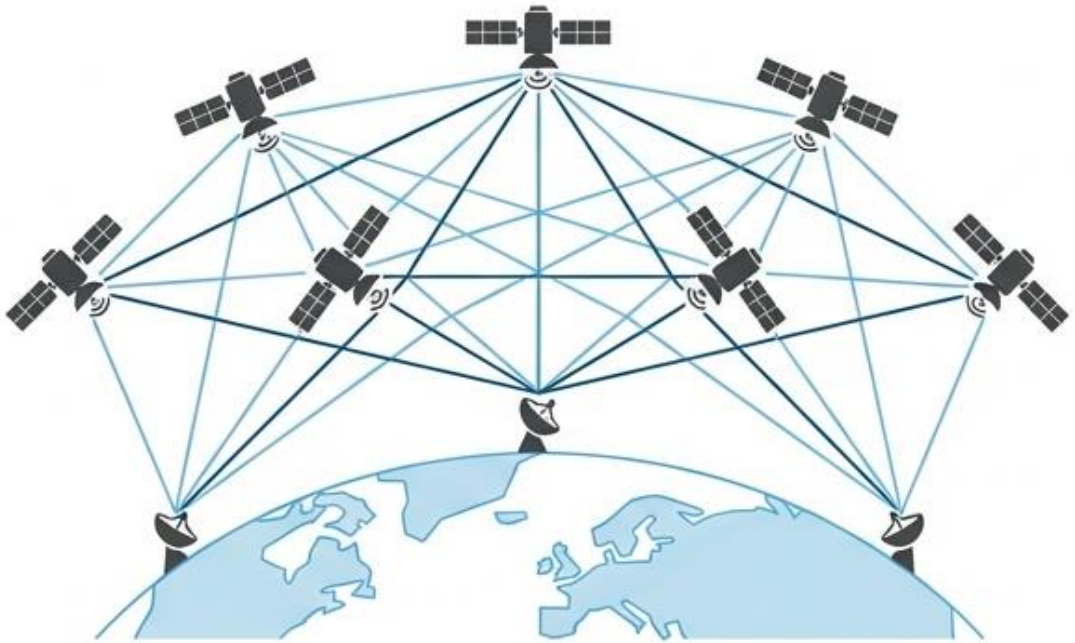
2026

Resilient Infrastructure and Data Sovereignty

Pioneering end-to-end trust through FAIR data principles and resilient operations for federated aerospace infrastructures.

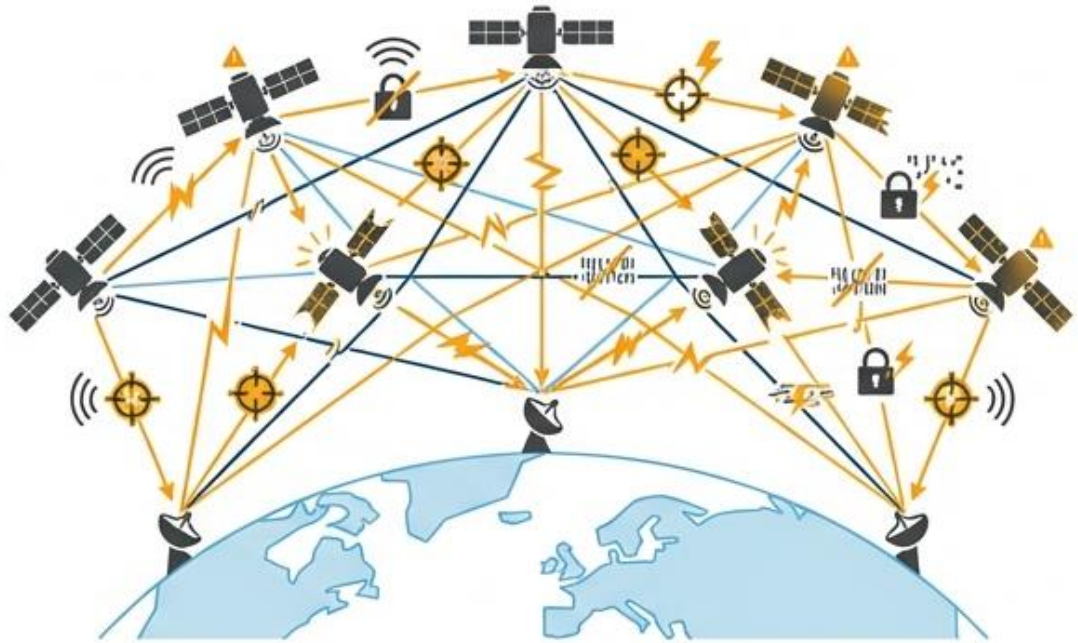
Federated space ecosystems drive open science but lack centralized trust

The Opportunity



Distributed space systems provide unparalleled capabilities for Earth observation, intelligence, and AI-driven scientific discovery.

The Threat

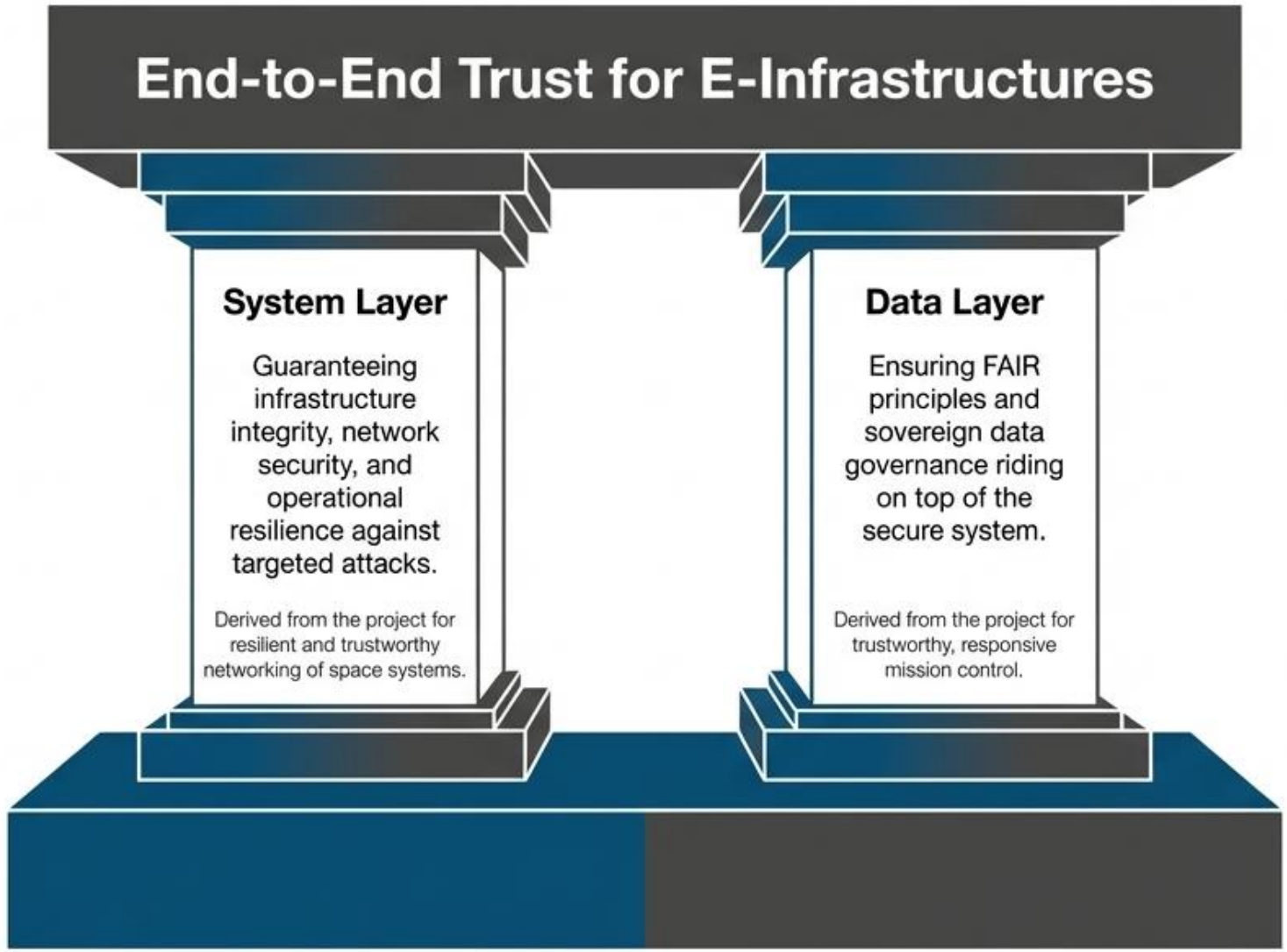


Federated models inherently lack centralized oversight. AI models are highly susceptible to poisoned data if the origin cannot be verified.

The Imperative

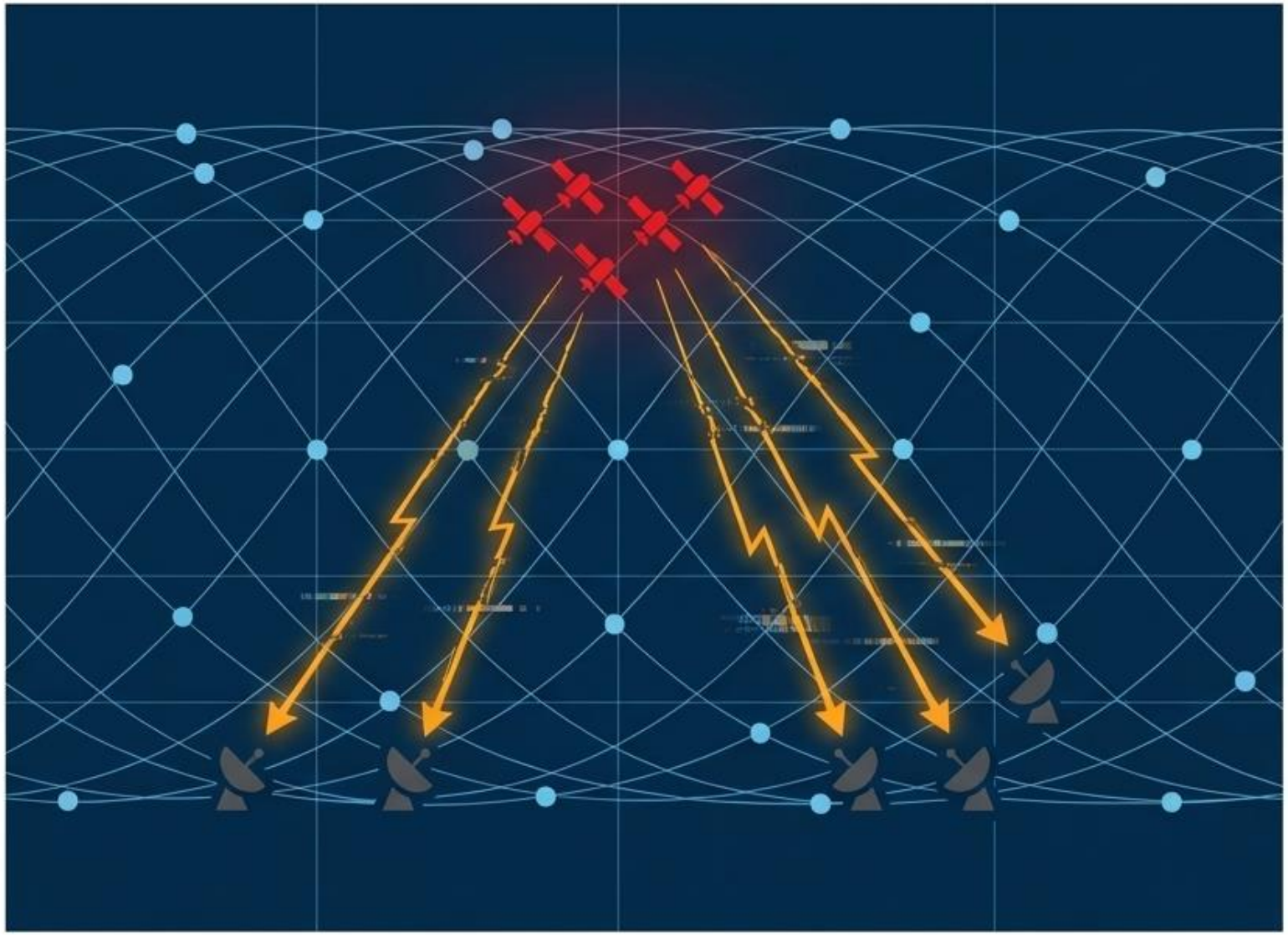
Scientific output is only as trustworthy as the data it consumes; data is only as trustworthy as the physical network that delivers it.

Data sovereignty requires a provably secure physical foundation



The Synthesis: We cannot separate data management from infrastructure engineering.

Identifying neuralgic nodes through simulated LEO network degradation



Threat Vectors

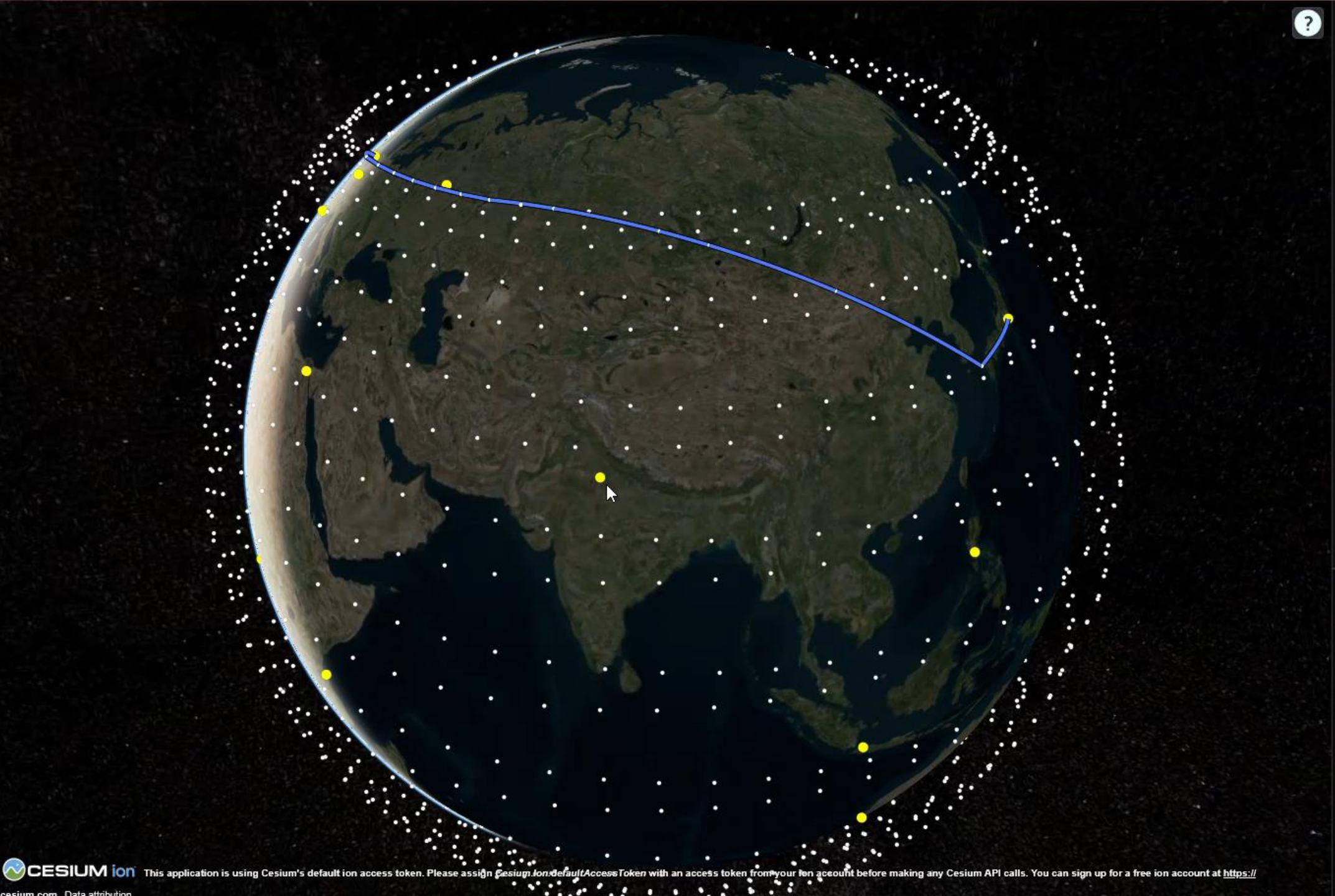
Modern space systems face constant exposure to jamming, spoofing, and cyber-based interference.

Simulation Parameters

We mathematically evaluate network criticality by simulating targeted attacks that remove specific subsets of satellites.

End-to-End Impact

By measuring the resulting latency and routing failures, we identify the specific “neuralgic nodes” that are absolute prerequisites for systemic stability.



Blocked Regions

Hold SHIFT and drag on the globe to add a rect

Clear all patches | Center view

Simulation

Render Hz: 30 Se

Sim speed: 30 Se

Route demo

Choose two cities to show the best live path.
Path recomputes periodically (and stays visua

From:

London

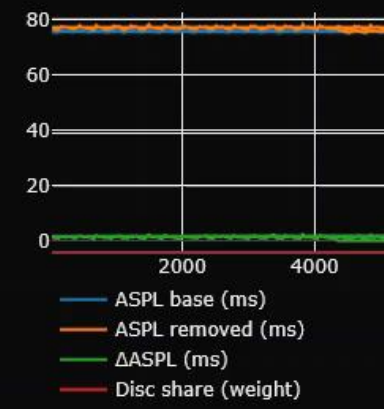
To:

Tokyo

Set route

"Attack" = current situation incl. blocked regio
"Baseline" = same moment, but with no remo

Route OK



Proactive threat modeling bridges qualitative identification and quantitative risk

STRIDE: The Identification Framework (Qualitative)

- **S** - Spoofing
- **T** - Tampering
- **R** - Repudiation
- **I** - Information Disclosure
- **D** - Denial of Service
- **E** - Elevation of Privilege

Identifies the gap → Assigns the priority

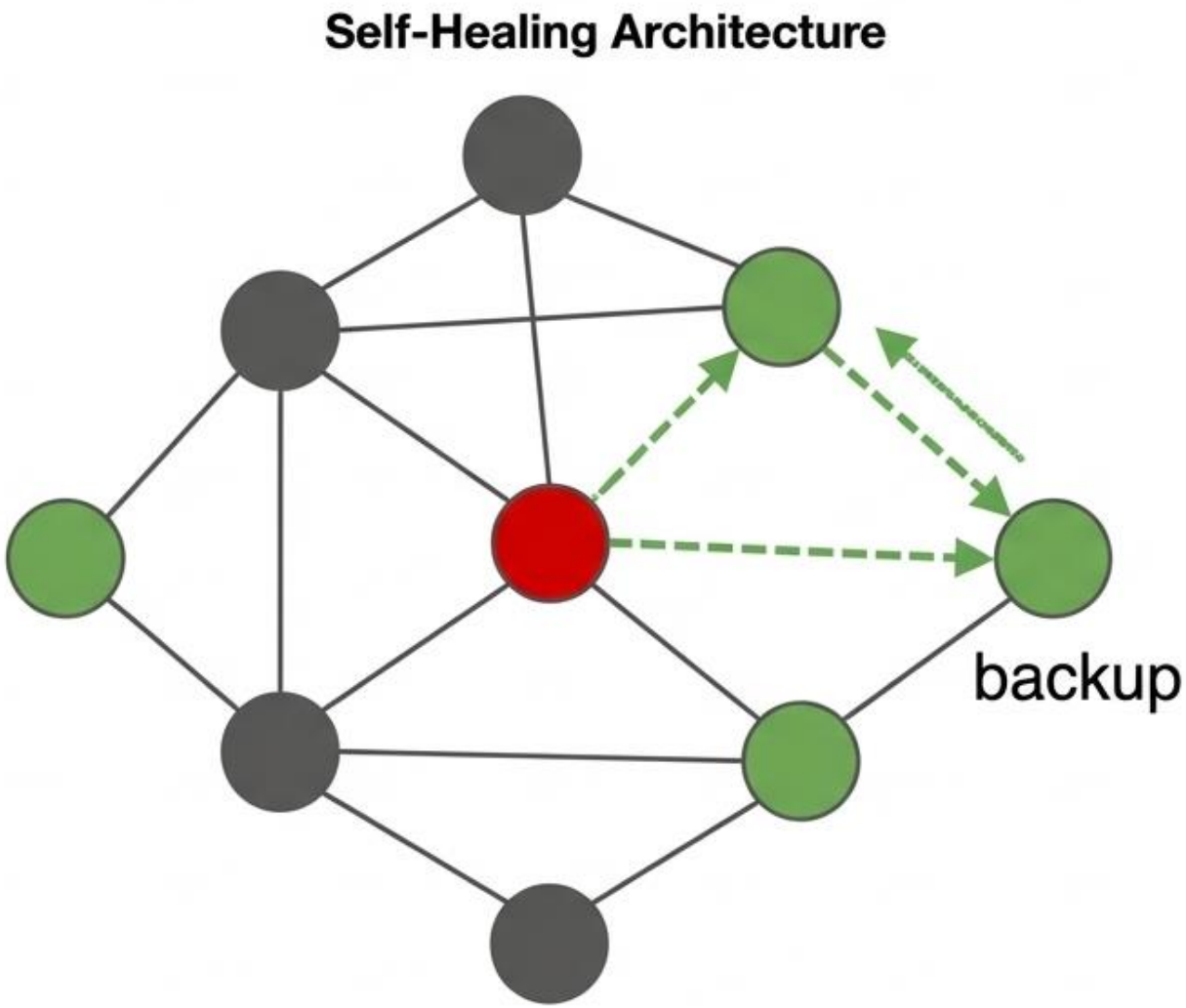
DREAD: The Scoring System (Quantitative)

- **D** - Damage potential
- **R** - Reproducibility
- **E** - Exploitability
- **A** - Affected Users
- **D** - Discoverability

Space-specific vectors: Telemetry spoofing, ground station supply chain compromise, information disclosure in distributed nodes.

Outcome: Ensures engineering resources are deployed exactly where the LEO simulations dictate they are most critical.

Self-healing architectures guarantee state synchronization under stress



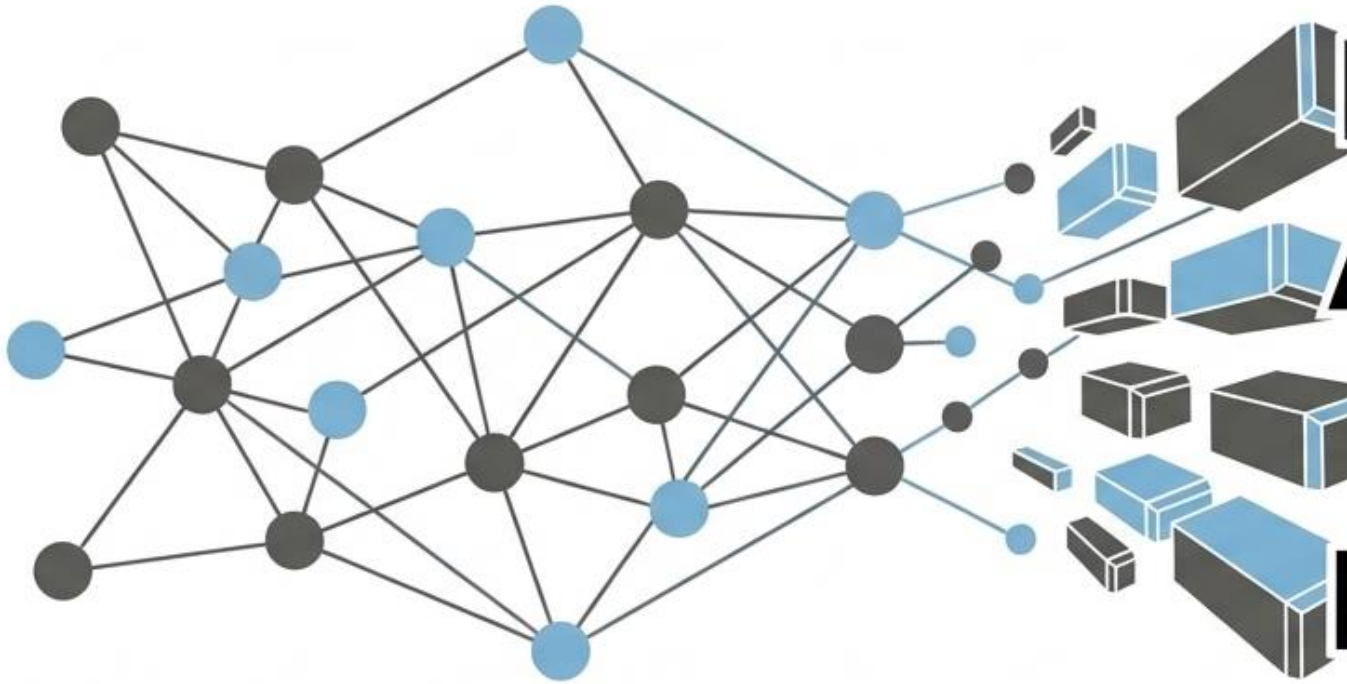
Engineering Objectives

< 60 seconds
Target network recovery time

≥ 95%
State synchronization maintained

- **Automated Reconfiguration:** Instantaneous failover protocols execute during a node collapse within the distributed mission control system.
- **Result:** The communication and computational foundation is secured, ready to transport sovereign data.

Provably secure infrastructure is merely the prerequisite for FAIR data



F - Findable

A - Accessible

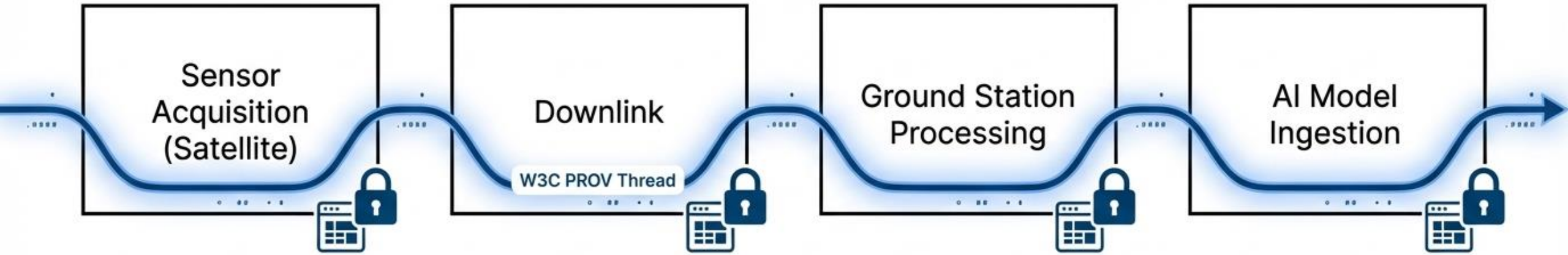
I - Interoperable

R - Reusable

Data Sovereignty Imperative

Securing the pipe is not enough; we must secure the payload. To fulfill FAIR principles in global open science, data must be more than simply stored—its entire operational history must be inextricably bound to it from origin to output.

Automated W3C PROV capture mathematically binds history to data



The Provenance Engine

Standardized Format

Utilizing the machine-actionable W3C PROV ontology.

Full Automation

Provenance capture occurs without human intervention across the entire lifecycle.

Granular Traceability

Every transformation, involved actor, and environmental variable is recorded permanently.

Result

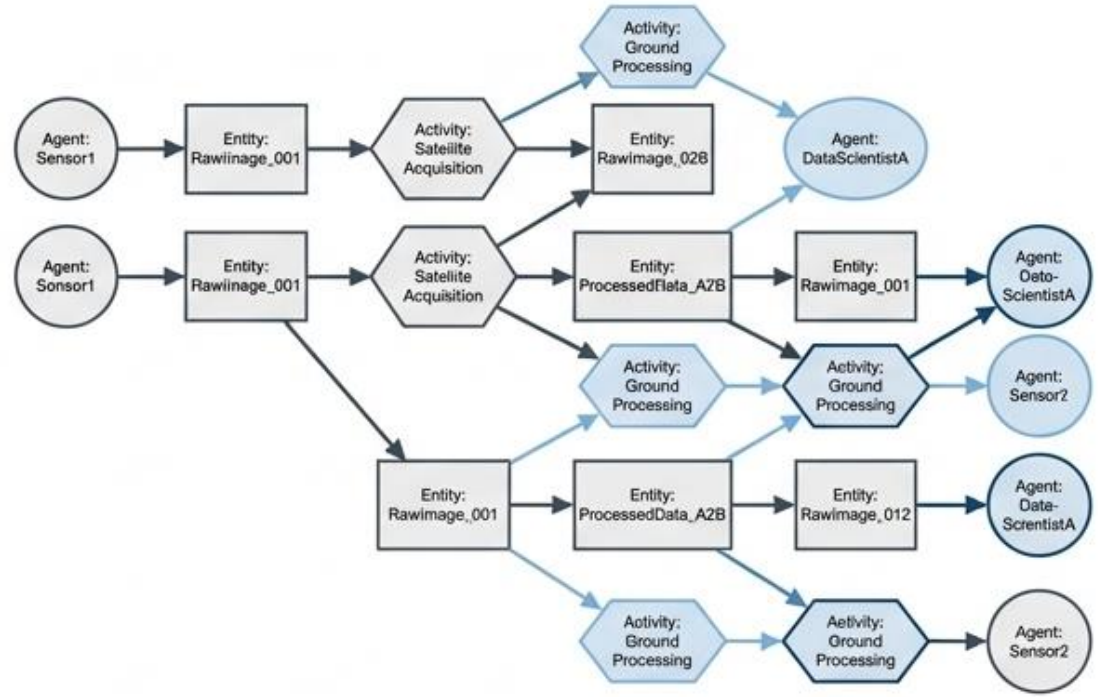
Downstream data products become fundamentally traceable, verifiable, and transparent.

Causality chains expose downstream infections that traditional logs miss

Traditional Logs

Events vs. Relationships: Logs only record isolated events. They are disconnected and easily spoofed.

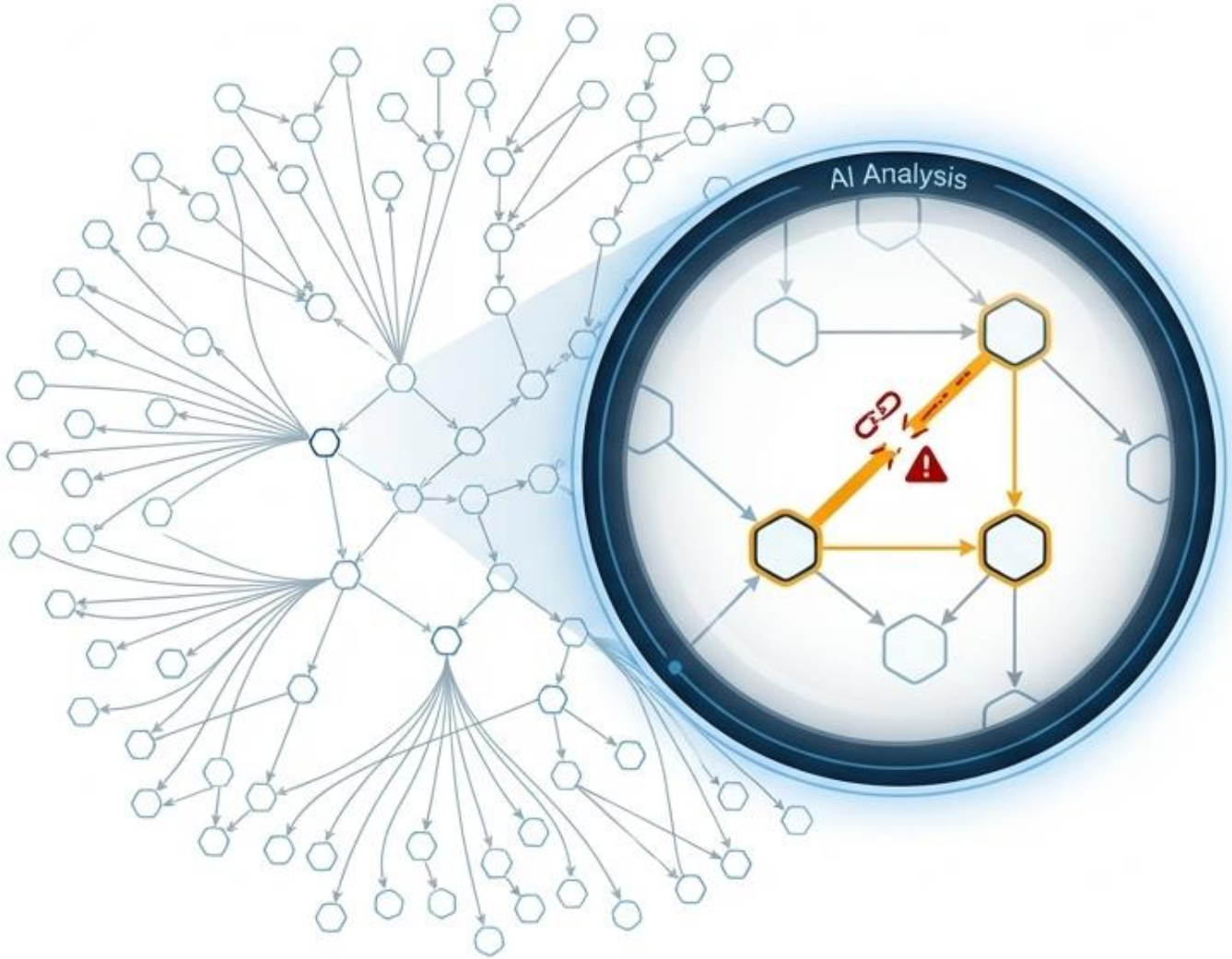
Provenance Causality Chains



W3C PROV captures unbreakable relationships and state changes.

The **Spoofing Defense:** If a LEO sensor is spoofed, traditional logs force a manual forensic nightmare. A provenance causality chain instantly and mathematically reveals every single downstream AI product infected by that specific sensor.

Graph-based provenance enables automated, AI-driven threat intelligence



Machine-Actionable Structure

Because W3C PROV creates structured DAGs, the data is perfectly formatted for machine learning ingestion without manual cleaning.

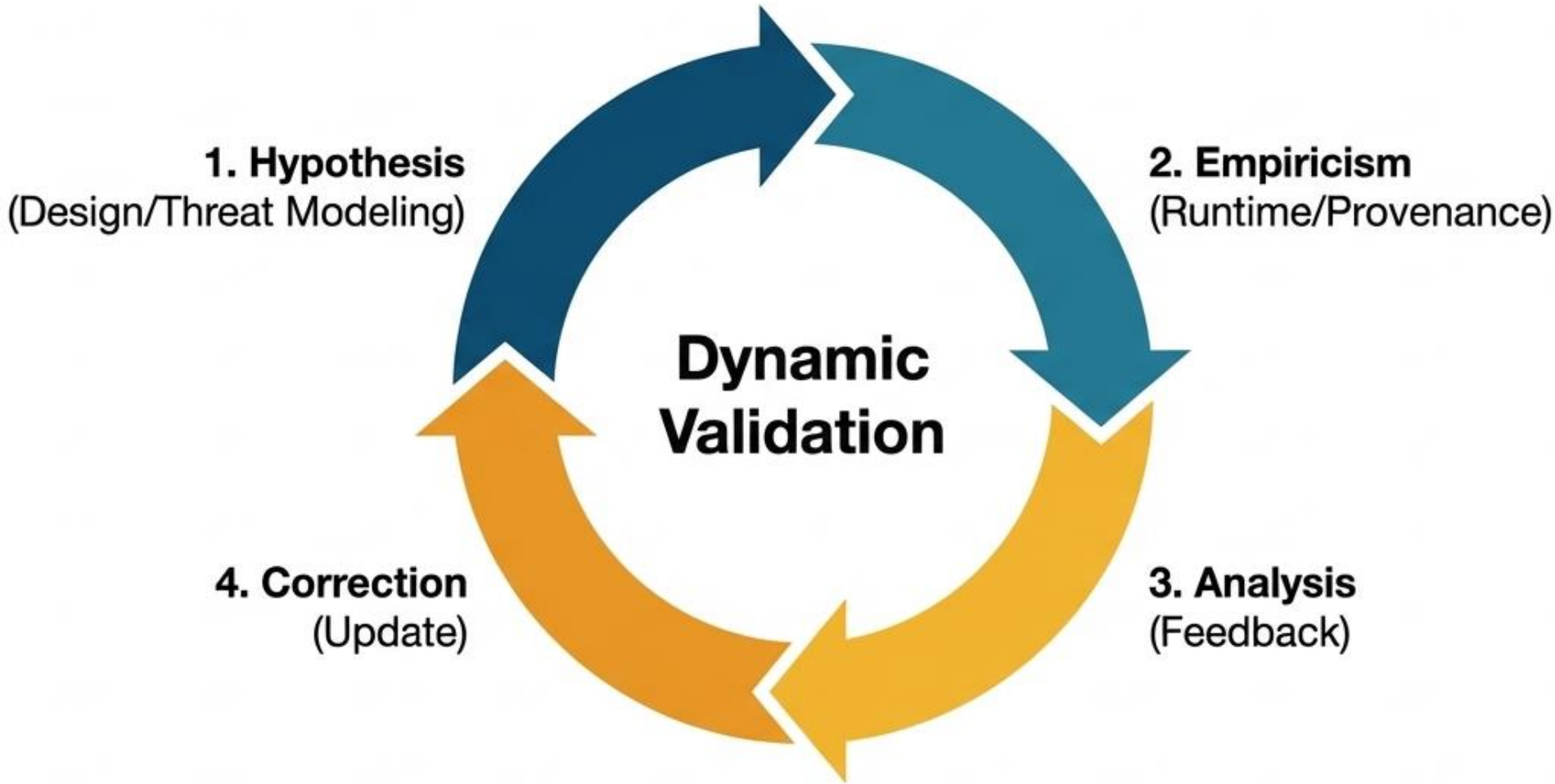
Automated Extraction

We deploy graph-analysis AI to automatically extract Threat Intelligence at scale, rather than relying on human analysts.

Anomaly Detection

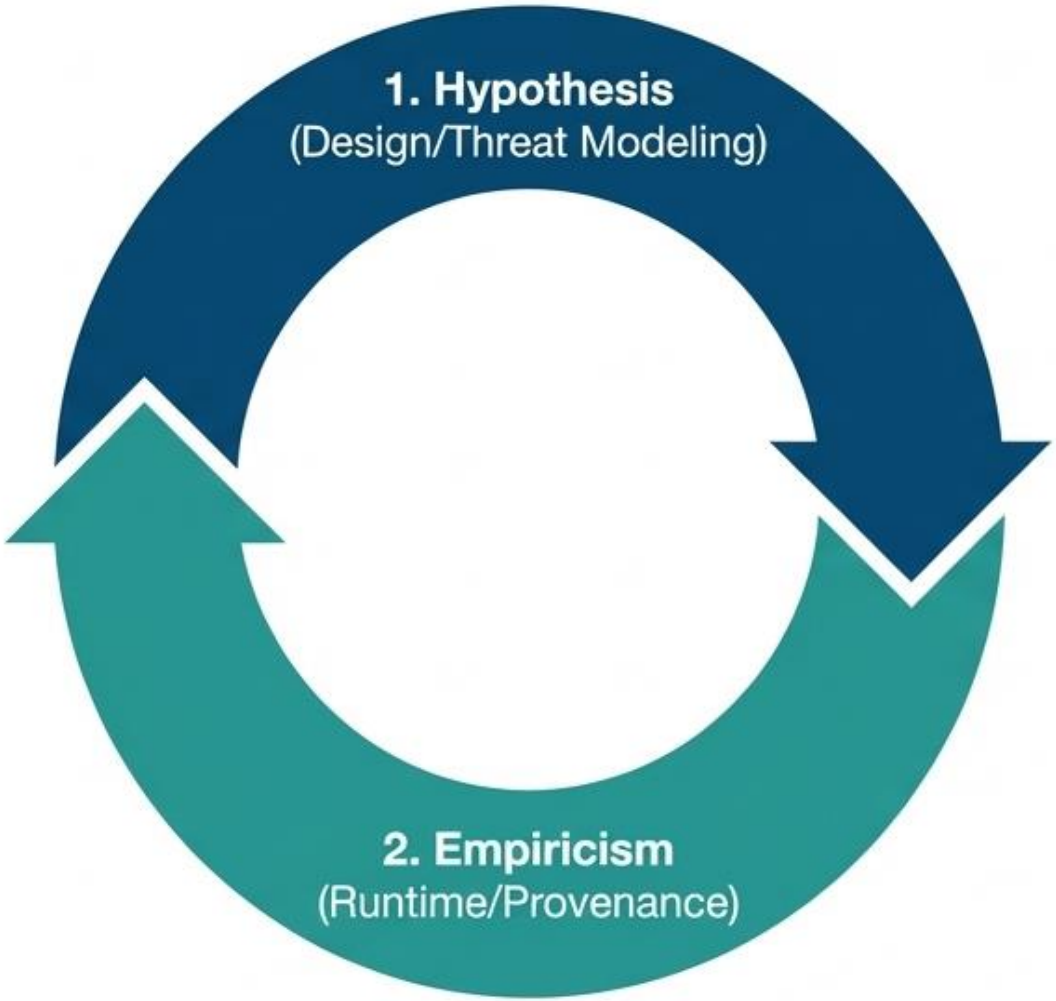
The AI instantly flags anomalous data behaviors by detecting structural deviations in the provenance graph that deviate from our STRIDE/DREAD threat models.

Trust is a continuous, dynamic validation cycle



The Framework: Security in federated systems is a closed-loop engineering challenge. We unite our resilient physical infrastructure with provenance-driven data to create an adaptive validation cycle.

Hypothesis meets Empiricism at system runtime



1. Hypothesis (Proactive Security)

Applying “Security Design Thinking.”

We establish the baseline threat catalog using our LEO simulations and STRIDE models, defining potential attack paths mathematically.

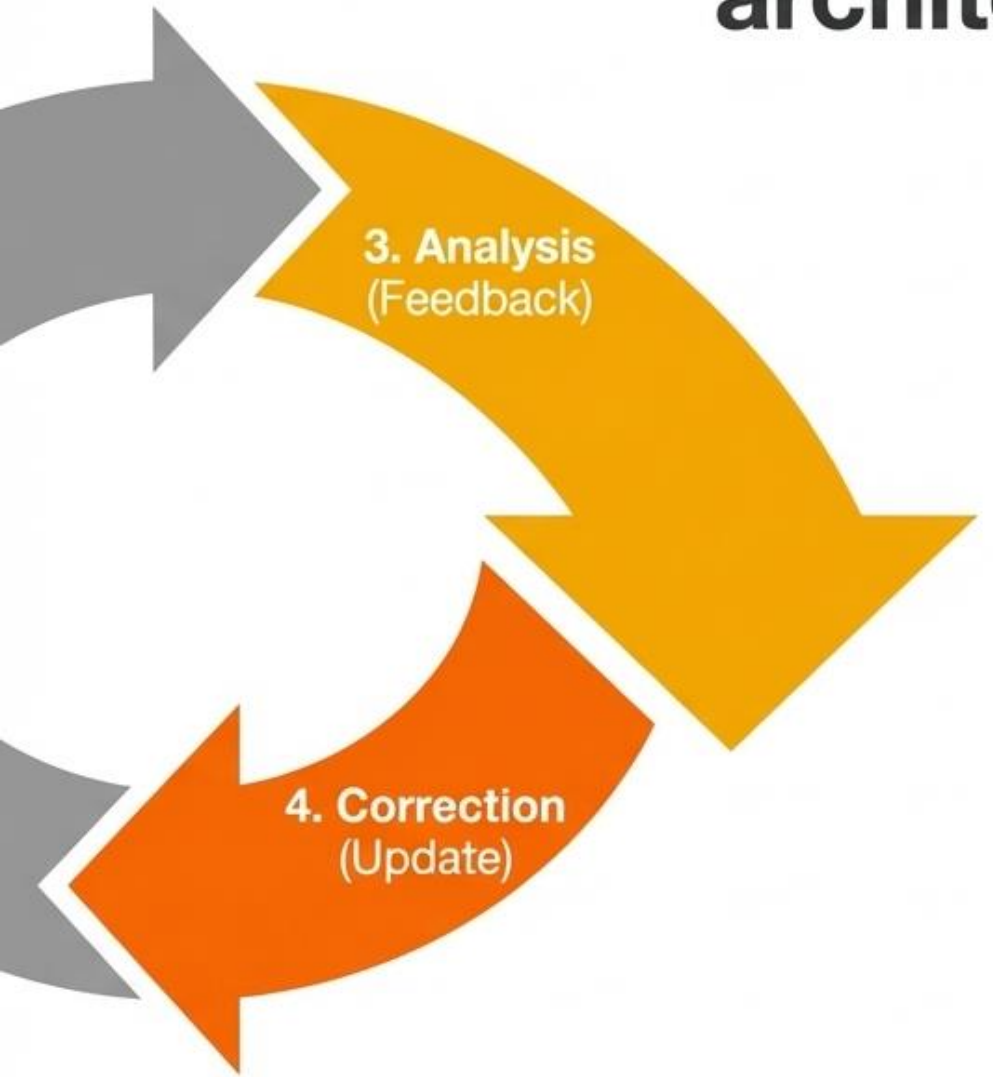
---

2. Empiricism (Provenance Analysis)

The system goes live. Real-world interactions are captured entirely via automated W3C PROV. We

shift from theoretical threat paths to empirical causality chains of how data and threat actors actually behave under stress.

Continuous analysis drives automated architectural correction



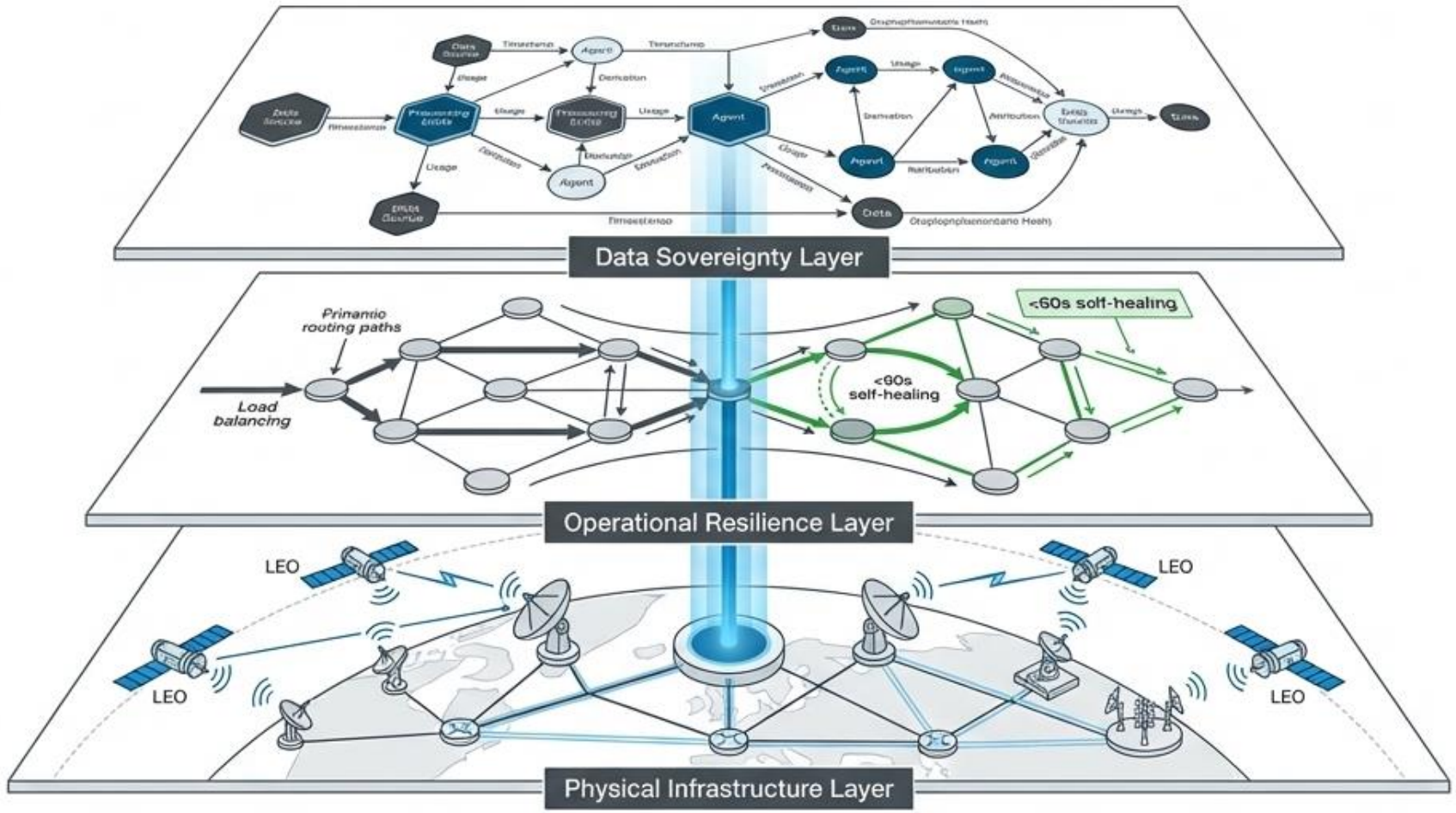
3. Analysis (The Feedback Protocol)

AI-driven evaluation of large-scale provenance graphs continuously compares empirical reality against our initial threat models. Question answered: Was a theoretical risk actually exploited, or did a novel vector emerge?

4. Correction (The Adaptive Update)

Automated updates are pushed directly to the physical network architecture and the threat catalog. The infrastructure is continually hardened for the next iteration of the cycle, ensuring permanent resilience.

End-to-end trust unites physical routing with data sovereignty



The Unified E-Infrastructure: Sovereign, cross-border research collaboration is only achievable when system operations and data governance are treated as a single engineering continuum.

Key Messages

- Secure and trustworthy foundations are essential for data sovereignty.
- Automated W3C PROV causality chains fulfill FAIR principles.
- Closed-loop validation ensures adaptive network resilience.

If you have any questions, feel free to ask them now or contact me by email

Andreas Schreiber
Department Intelligent and Distributed Systems,
German Aerospace Center (DLR)
Andreas.Schreiber@dlr.de

Imprint

Topic:	**Building Trust in Aerospace Infrastructures: Resilient Operations and Provenance-Driven Data Sovereignty** IGSC 2026, Academia Sinica, Taipeh
Date:	2026-03-17
Author:	Andreas Schreiber
Institute:	Software Technology