PROCEEDINGS OF SCIENCE

# Building Trust in Aerospace Infrastructures: Resilient Operations and Provenance-Driven Data Sovereignty

**Andreas Schreiber***

*German Aerospace Center (DLR), Institute of Software Technology*
*Linder Höhe, 51147 Cologne, Germany*

*E-mail:* andreas.schreiber@dlr.de

Distributed space systems—spanning satellite constellations and federated ground operations—face a dual challenge: securing the underlying infrastructure against hybrid threats while ensuring that data produced and exchanged across these systems remains trustworthy and traceable. The growth of AI-driven discovery makes transparent, machine-actionable data provenance an essential rather than optional property. We present a framework that addresses both concerns in a coordinated manner. On the infrastructure side, federated identity management and proactive threat modeling (STRIDE/DREAD) protect against risks ranging from signal spoofing to cyberattacks on ground segments. On the data side, W3C PROV standards are applied throughout the complete data lifecycle—from sensor acquisition through processing to archival—to deliver machine-actionable provenance. The central argument is that data sovereignty and secure collaboration require a networking and operations infrastructure that is both resilient and reliable, and that has been demonstrably secured. By aligning this framework with the German Space Security Strategy (2025) and the BMFTR Cybersecurity Roadmap (2027), and by validating it through a closed-loop security cycle with AI-driven causality analysis, we show how FAIR-compliant data sovereignty and operational resilience can be achieved jointly in critical aerospace environments.

*International Symposium on Grids & Clouds (ISGC2026)*
*17–21 March 2026*
*Academia Sinica, Taipei, Taiwan*

*Speaker

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0) All rights for text and data mining, AI training, and similar technologies for commercial purposes, are reserved. ISSN 1824-8039 . Published by SISSA Medialab.



PoS(ISGC2026)009

## 1. Introduction

The strategic importance of space as a security dimension has never been higher. Modern military and civil operations depend on a seamless "system-of-systems" involving satellites, ground stations, and high-performance data processing. However, global geopolitical tensions have led to an increase in hybrid threats, ranging from cyber-attacks on ground segments to physical interference with orbital assets.

In this context, the German Federal Government released the first **Space Security Strategy (WRSS)** in 2025, prioritizing the resilience of critical space infrastructures. Simultaneously, the **BMFTR Cybersecurity Roadmap 2027** emphasizes technological sovereignty through advancements in AI-security and quantum communication.

We present strategies for establishing trust in these complex environments. We draw on DLR research projects concerned with resilient overlay networking for satellite constellations and with verified, provenance-aware mission control for responsive space operations. Our approach bridges the gap between infrastructure security and data sovereignty by implementing a provenance-driven architecture that supports the FAIR principles even in decentralized, high-stakes aerospace environments.

As a concrete use case (Section 6), we consider large LEO and VLEO satellite constellations, which are exposed to a wide spectrum of potential disruptions affecting their performance and dependability. These range from active threats—targeted jamming, strategic interference, cyber-attacks, and compromised satellites—to environmental factors such as ionospheric disturbances, space weather, and geomagnetic storms. The interplay of orbital dynamics, network behaviour, and on-board resource constraints necessitates a multi-layer simulation framework to study resilience and performance realistically and to develop effective countermeasures.

## 2. Related Work

### 2.1 Provenance for Resilient Mission Control

Recent research has highlighted the utility of provenance in space operations beyond simple metadata logging. *Schreiber et al. (2018)* established provenance as a building block for Open Science, but its application in Mission Control Systems (MCS) provides critical traceability for command sequences. In resilient systems, provenance graphs enable "Forensic Readiness" by allowing operators to reconstruct state changes across distributed nodes during an anomaly [10, 15].

### 2.2 Trust in Decentralized Cloud-based Systems

The shift toward decentralized "Combat Clouds" and hybrid satellite-terrestrial networks requires new trust models. Traditional perimeter-based security is insufficient. *Zero Trust Architectures (ZTA)* and decentralized identity management (DID) are becoming standard. Recent studies on *Provenance-based Trust* suggest that the trustworthiness of a node can be dynamically calculated based on its historical interactions captured in a causality graph, which is particularly relevant for federated ground segments [14, 16].



PoS(ISGC2026)009

## 3. Background

### 3.1 Threat Modeling (STRIDE)

Proactive security begins with a systematic identification of attack vectors. STRIDE was originally introduced by Kohnfelder and Garg [11] and later formalised within Microsoft's Security Development Lifecycle [12, 13]. Its application to space and cyber-physical systems has been studied in [15]. We adapt the **STRIDE** framework for the space domain:

- **Spoofing:** Forged GPS signals or hijacked telemetry commands.
- **Tampering:** Manipulation of sensor data or firmware updates.
- **Repudiation:** Denying a malicious command execution in a federated MCS.
- **Information Disclosure:** Interception of unencrypted cross-links.
- **Denial of Service:** Jamming of RF uplinks or flooding ground station networks.
- **Elevation of Privilege:** Exploiting ground-segment software vulnerabilities.

### 3.2 Risk Assessment (DREAD)

To prioritize mitigation, we employ **DREAD** [12, 14], assessing threats based on **D**amage, **R**eproducibility, **E**xploitability, **A**ffected users, and **D**iscoverability. In aerospace, "Damage" often refers to the loss of a multi-million-euro asset or critical national capability.

### 3.3 Provenance (W3C PROV)

We define provenance according to the W3C PROV standard [16–18]. By modeling system entities, activities, and agents, we create a directed acyclic graph (DAG) that represents the "causal history" of every data product and system state. This is superior to traditional logging as it preserves the relationships between distributed events. The PROV Data Model [17] defines the core abstractions; PROV-O [18] provides an OWL ontology for interoperable provenance exchange; PROV-N [19] specifies a human-readable notation; and the comprehensive introduction by Moreau and Groth [21] offers a consolidated treatment of the entire family.

Compared with traditional log-based approaches, W3C PROV offers several decisive advantages for security and traceability in distributed systems:

- **Causality chains instead of mere chronology:** Traditional logs list events in temporal order; W3C PROV captures *why* each state arose—which processes influenced it and which agents were involved—enabling root-cause analysis rather than simple event replay.
- **Standardisation and machine-actionability:** W3C PROV is a standardised, machine-readable format that can be integrated across the complete data lifecycle, from sensor acquisition through to final processing and archival.
- **Enabling the FAIR principles:** Automated provenance capture makes data products traceable, verifiable, and transparent—a critical prerequisite for fully realising the **FAIR** principles (Findable, Accessible, Interoperable, Reusable).
- **Automated security analysis:** The graph structure of provenance data scales naturally with AI methods. Large provenance graphs can be mined automatically for *Threat Intelligence*—for instance, to determine whether a modelled risk was actually exploited at runtime.



PoS(ISGC2026)009

- **Foundation for trustworthy AI:** The verifiable data integrity guaranteed by W3C PROV is essential for training reliable AI models and for enabling sovereign research collaboration across international boundaries.

In summary, W3C PROV serves as the technological instrument to move from purely administrative record-keeping to active **data sovereignty management** and a trustworthy data ecosystem.

## 4. Data Sovereignty through FAIR and Provenance

### 4.1 The FAIR Principles

The FAIR principles—**F**indable, **A**ccessible, **I**nteroperable, **R**eusable—were formally defined by Wilkinson et al. [7] and have since become the gold standard for scientific data management. In aerospace, the *ESA-FAIR* initiative [8] and NASA's *Open-Source Science Initiative* [9] emphasize that "Reusability" (R1.2) is impossible without rich provenance.

### 4.2 FAIR in Space Missions

In the context of the **German Space Strategy**, data sovereignty means that the originator of the data maintains control over its usage. Provenance supports this by:

1. **Attribution:** Clearly identifying the source sensor (Findability).
2. **Verifiability:** Ensuring the processing chain is intact (Integrity/Interoperability).
3. **Sovereignty Enforcement:** Using provenance-aware access control to restrict data use based on its origin.

## 5. Infrastructure Resilience and Proactive Modeling

### 5.1 Responsive Space and Infrastructure Integrity

Resilience is defined by the WRSS as the ability to maintain services despite attacks.

- **Responsive Space Cluster:** DLR's competence center focuses on the rapid deployment of small satellite constellations to replace lost assets within days, ensuring continuity of service [12].
- **Systemic Analysis:** Our approach utilizes "Security Design Thinking" to analyze the systemic robustness of LEO networks, identifying critical nodes whose loss would compromise the entire constellation.

### 5.2 The Closed-Loop Security Cycle

We propose a dynamic validation of the security concept through a four-stage cycle.

- **Hypothesis (Proactive Modeling):** Defining the security envelope using STRIDE and DREAD during the design phase.
- **Empiricism (Runtime Provenance):** Capturing real-world interactions as PROV-graphs during mission execution.



PoS(ISGC2026)009

- **Analysis (Causality Verification):** Using AI to compare runtime graphs against the design hypotheses to detect if risks were exploited.
- **Correction (AI-driven Adaptation):** Automatically extracting "Threat Intelligence" from graphs to adapt firewall rules, routing, or the threat model itself.

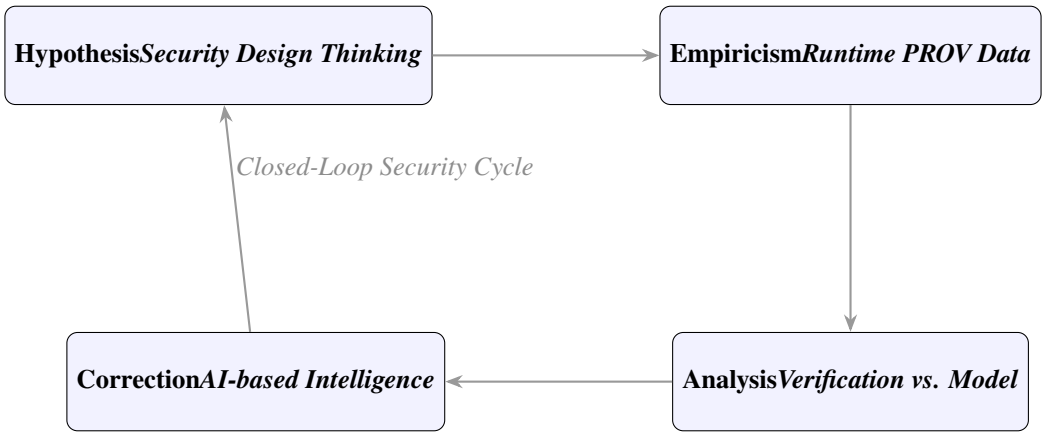


**Figure 1:** The closed-loop security cycle for validating resilient aerospace systems.

### 5.3 Role of AI in Provenance Graph Analysis

Artificial intelligence plays a pivotal role in making provenance-based security analysis both scalable and automated. Four distinct functions can be identified:

- **Threat Intelligence extraction:** AI methods automatically mine large causality graphs for actionable threat information. Because these graphs can be orders of magnitude more complex than traditional logs, manual analysis is no longer feasible at operational scale.
- **Automated scaling:** AI enables efficient processing of the high-volume, heterogeneous data streams produced by decentralised space systems, flagging anomalies that would escape rule-based detectors.
- **Dynamic validation in the security cycle:** During the *Analysis* phase of the closed-loop cycle (Fig. 1), AI compares runtime provenance graphs against the design-time threat model to determine whether a theoretically identified risk was actually exploited in operation.
- **Foundation for trustworthy AI models:** Conversely, the verifiable data integrity guaranteed by provenance graphs is a prerequisite for training trustworthy, sovereign AI models for research—closing the feedback loop between data quality and model reliability.

In summary, AI enables the transition from purely reactive data management to **proactive, automated security analysis** grounded in causality chains rather than mere event sequences.

## 6. Use Case: Satellite Network Simulation for Resilience and Performance

### 6.1 Problem Setting

Large LEO and VLEO constellations are exposed to a broad spectrum of potential disruptions that can impair their performance and dependability. These include active threats such as targeted



PoS(ISGC2026)009

jamming, strategic interference, cyberattacks, and compromised satellites, as well as environmental factors such as ionospheric disturbances, space weather, and geomagnetic storms. Because orbital dynamics, network behaviour, and on-board resource constraints interact in non-trivial ways, a multi-layer simulation framework is required to study the resilience and performance of such systems realistically and to develop effective countermeasures and prevention strategies.

### 6.2 Framework Architecture

The *Satellite Network Simulation Framework for Resilience and Performance Evaluation* is conceived as a multi-layer simulator for analysing the resilience of LEO and VLEO satellite constellations. Our approach integrates three coupled layers:

1. **Constellation and Network Topology Layer:** Time-varying connectivity and routing, capturing the dynamic geometry of orbital mechanics.
2. **Operational Network Layer:** Traffic flows and link capacities, reflecting realistic data-rate demands and inter-satellite link utilisation.
3. **Hardware Layer:** On-board resource and mission constraints such as computational capacity, memory, and power budgets.

By jointly modelling these layers, the framework enables realistic investigation of the interactions between hardware limitations, dynamic network structure, and traffic behaviour.

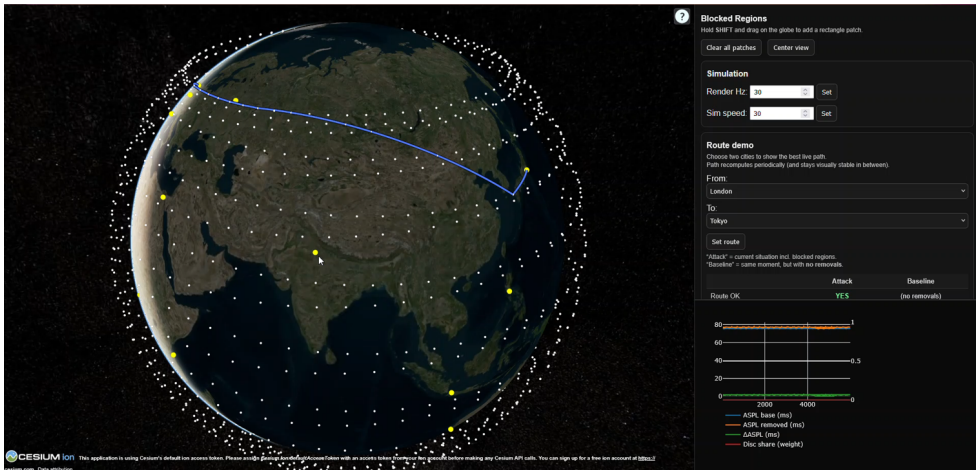


**Figure 2:** Conceptual illustration of the multi-layer LEO/VLEO satellite network simulation framework.

### 6.3 Objectives and Expected Outcomes

The framework enables systematic evaluation of satellite network resilience under diverse disruption, failure, and attack scenarios [1, 2]. This encompasses the analysis of performance degradation, bottlenecks, and cascade effects, as well as the investigation of architectural design choices, routing strategies, and resource management policies. The overarching goal is to derive robust insights for the design of future satellite communication systems and to support the development of efficient protection and adaptation measures. Through simulation-based investigation of realistic disruption and attack scenarios, critical vulnerabilities, dependencies, and potential side-effects



PoS(ISGC2026)009

within complex constellation networks can be identified, allowing architectural decisions and technical protection mechanisms to be systematically evaluated and optimised.

## 7. Conclusion

Achieving trust in modern aerospace infrastructures requires a shift from static security to a dynamic, provenance-aware architecture. By integrating the national strategic goals of the *Weltraumsicherheitsstrategie 2025* and the *BMFTR Roadmap 2027*, we provide a framework that ensures both the resilience of the physical infrastructure (Responsive Space) and the sovereignty of the data (FAIR/PROV). Our closed-loop security cycle provides the necessary feedback mechanism for systems to survive in an increasingly contested space domain.

## References

[1] BMFTR, *Cybersicherheit – Forschungspolitische Impulse (Eckpunktepapier)*, Bundesministerium für Forschung, Technologie und Raumfahrt, 2026. https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/5/31882_Eckpunktepapier_Cybersicherheit.pdf

[2] Bundesregierung, *Weltraumsicherheitsstrategie der Bundesregierung 2025*, Bundesministerium der Verteidigung, 2025. https://www.bmvg.de/resource/blob/6042578/eb7df89c9b7038d0788fad436bb72e89/weltraumsicherheitsstrategie-2025-de-data.pdf

[3] A. Schreiber, *Provenance as a Building Block for an Open Science Infrastructure*, ISGC, 2018.

[4] DLR, *Responsive Space Cluster Competence Center*, https://www.dlr.de/en/rs/research-transfer, 2026.

[5] S. Kim et al., *Zero-Trust Architectures for Federated Space Systems*, IEEE Aerospace, 2025.

[6] ESA, *Guidelines for FAIR Data Management in Earth Observation*, 2024.

[7] M. D. Wilkinson et al., *The FAIR Guiding Principles for scientific data management and stewardship*, Scientific Data, vol. 3, no. 160018, 2016. https://doi.org/10.1038/sdata.2016.18

[8] ESA, *ESA FAIR Enablement Initiative: Making Space Data FAIR*, https://esa-earthcode.github.io/open-science-catalog/, 2024.

[9] NASA, *Open-Source Science Initiative (OSSI)*, https://science.nasa.gov/open-science-overview, 2024.

[10] J. Doe, *Trust Management in Decentralized Cloud Environments*, Journal of Cyber Security, 2025.

[11] L. Kohnfelder and P. Garg, *The Threats to Our Products*, Microsoft Interface, Microsoft Corporation, 1999.

[12] M. Howard and D. LeBlanc, *Writing Secure Code*, 2nd ed., Microsoft Press, 2003.



PoS(ISGC2026)009

[13] A. Shostack, *Threat Modeling: Designing for Security*, Wiley, 2014.

[14] J. D. Meier et al., *Improving Web Application Security: Threats and Countermeasures*, Microsoft Corporation, https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649461(v=pandp.10), 2003.

[15] N. Marahrens et al., *Challenges in threat modelling of new space systems: A teleoperation use-case*, Advances in Space Research, 2022. https://doi.org/10.1016/j.asr.2022.05.058

[16] P. Groth and L. Moreau (eds.), *PROV-Overview: An Overview of the PROV Family of Documents*, W3C Note, https://www.w3.org/TR/prov-overview/, 2013.

[17] L. Moreau et al., *PROV-DM: The PROV Data Model*, W3C Recommendation, https://www.w3.org/TR/prov-dm/, 2013.

[18] T. Lebo et al., *PROV-O: The PROV Ontology*, W3C Recommendation, https://www.w3.org/TR/prov-o/, 2013.

[19] L. Moreau et al., *PROV-N: The Provenance Notation*, W3C Recommendation, https://www.w3.org/TR/prov-n/, 2013.

[20] L. Moreau et al., *PROV-CONSTRAINTS: Constraints of the PROV Data Model*, W3C Recommendation, https://www.w3.org/TR/prov-constraints/, 2013.

[21] L. Moreau and P. Groth, *Provenance: An Introduction to PROV*, Synthesis Lectures on the Semantic Web: Theory and Technology, Morgan & Claypool, 2013.

PoS(ISGC2026)009