Contribution ID: **126** Type: **Oral Presentation**

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

Tuesday, 17 March 2026 11:20 (20 minutes)

The proliferation of distributed space systems, encompassing large-scale satellite constellations and federated ground segments, is generating unparalleled opportunities for global open science, particularly in the domains of earth observation, intelligence, security, and defense. However, this federated model poses significant challenges to operational integrity and data trustworthiness. The increasing reliance on AI-driven discovery underscores the necessity for not only the accuracy of underlying data, but also the transparency of its origin and processing. Addressing this issue necessitates a holistic approach that unifies the operation of secure infrastructure with the principles of FAIR, sovereign, and trusted data.

This contribution presents a pioneering architectural framework derived from ongoing research at the German Aerospace Center (DLR), encompassing projects for resilient and trustworthy networking of space systems) and for trustworthy, responsive mission control). The proposed approach establishes end-to-end trust in a federated e-infrastructure by addressing the system and data layers in a coordinated manner.

The organization's areas of expertise include infrastructure integrity, network security, and operational resilience. The development of resilient networking protocols and operational concepts for distributed ground segments is underway. These protocols and concepts are intended to ensure service continuity during component failures or targeted attacks. This encompasses the implementation of robust federated identity management and threat models (e.g., STRIDE), which are adapted to address specific threats pertinent to space, including signal spoofing and ground station compromises. By ensuring the security of the communication and computational infrastructure, a trusted foundation is established for all subsequent data operations.

The foundation's credibility is leveraged to ensure data governance and cultivate a reliable data ecosystem. Standardized, machine-actionable data provenance (W3C PROV) is integrated throughout the entire data lifecycle, from sensor acquisition to final processing. Automated provenance capture is a process that ensures all data products are traceable, verifiable, and transparent. This fulfills a critical component of the FAIR data principles (findable, accessible, interoperable, and reusable). This verifiable data integrity is imperative for the development of trustworthy AI models and the facilitation of secure, sovereign research collaboration across international borders.

The findings of our research indicate that the attainment of data sovereignty and secure collaboration necessitates more than mere data management; it demands a networking and operations infrastructure that is both resilient and reliable, and which has been proven to be secure.

Primary author: Mr SCHREIBER, Andreas (German Aerospace Center (DLR))

Presenter: Mr SCHREIBER, Andreas (German Aerospace Center (DLR))

Session Classification: FAIR, Sovereign & Trusted Data - I

Track Classification: Track 6: FAIR, Sovereign & Trusted Data