

Security of LLM Applications in Satellite Communications

The Problem

LLMs Cannot Be Trusted Unconditionally

Large language models have become capable enough to assist in demanding operational contexts — including satellite communications, where they can support controllers with log analysis, anomaly interpretation, and procedure lookup. But capability is not the same as reliability.

An ESA SatCom demonstrator project put this to the test, deploying an AI assistant in a realistic satellite operations scenario and then systematically attacking it. The findings:

The AI Assistant fell victim to attacks — e.g., supply chain attacks via compromised documents in the knowledge base

The AI Assistant invented things — it hallucinated telemetry values and presented them as facts

The AI Assistant revealed sensitive data — it disclosed restricted subsystem data to users who were not authorized

The AI Assistant failed to follow established business rules and policies — e.g., generating spacecraft commands that bypassed human oversight

32%	of attacks against LLMs were successful	27%	of interactions contained errors and undesired output
------------	--	------------	--

Average across two models and three different attacks and instructions, respectively. Consistent with findings from published LLM reliability studies. (see for example: ACE <https://arxiv.org/pdf/2512.04921>).

The Solution

When mistakes are not an option

This does not mean that LLMs cannot be used in critical satellite communications operations. However, LLM-based systems must be thoroughly tested and secured at runtime. The project has demonstrated how a systematic and thorough red teaming exercise can be set up with minimal effort, and how the insights and test cases gained from this can be translated into effective security measures.

Contact:

Dr. Patrick Stender

OHB Digital Connect GmbH

patrick.stender@ohb.de

This activity was carried out with the support of the European Space Agency (ESA) under the ARTES 4S programme. The views expressed in this publication can in no way be taken to reflect the official opinion of the European Space Agency.