58th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Dr. Bruce Chesley
Teaching Science and Technology, Inc (TSTI), United States

Dr. Jerry Sellers
Teaching Science and Technology, Inc., United States
Ms. Terri Johnson
United States

A CYBER-FUNCTIONAL ARCHITECTURE FRAMEWORK FOR SPACE SYSTEMS: BALANCING SECURITY AND MISSION SUCCESS

Abstract

As space systems become increasingly interconnected and reliant on digital infrastructure, the need for robust cybersecurity frameworks and standards has never been more critical. Recent calls for unified cyber standards for space systems underscore the urgency of establishing clear, actionable guidelines for securing these assets. However, beyond defining standards, it is equally important to develop methods for assessing their implementation to evaluate whether a given space cybersecurity architecture is truly "good" at providing appropriate security for a given mission.

This paper addresses the fundamental challenge of evaluating the cybersecurity posture of space system architectures, proposing an approach that balances mission success and cyber resilience. Specifically, we explore how a functional architecture for cybersecurity—one that is implementation-agnostic—can be developed to provide a structured approach for analysis and assessment.

Our concept builds on established design patterns in both space system and cybersecurity domains. Space system patterns include the NASA Space Mission Architecture Framework, Human Spaceflight Reference Models, and CubeSat standards, while cybersecurity patterns encompass defense-in-depth, zero trust architectures, network segmentation, and fault-tolerant design. By integrating these frameworks, the proposed cyber-functional architecture framework enables a holistic assessment of space system architectures from a security perspective.

Key to this approach is avoiding the pitfalls of some standards initiatives, where compliance criteria remain ambiguous and difficult to assess. Instead, we aim to provide tangible methods and tools for evaluating the balance of cybersecurity measures against mission requirements and operational constraints. This includes developing metrics, criteria, and tools for assessing compliance with cyber-functional design principles.

We demonstrate the benefits of this approach by assessing Level 3 and 4 requirements for a representative space mission using the proposed methods. By aligning cybersecurity architecture patterns with mission-driven space system architectures, we propose a framework that ensures security is treated as a foundational design principle rather than a compliance afterthought.