IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

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

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

START WITH THE RIGHT REQUIREMENTS: A FIRST-PRINCIPLES APPROACH FOR CYBER SECURE SPACE MISSIONS

Abstract

As the volume of cyber-attacks targeting space systems and networks continues to rise, space systems designers are becoming acutely aware that cyber events pose critical risks to mission success. Consequently, "designing in" good cybersecurity needs to part of the development lifecycle of all space systems. Unfortunately, current design practices do not treat cybersecurity requirements as core to mission success. Rather, cybersecurity requirements are "bolted on" in the form of compliance with standards or regulatory requirements; adherence to a framework; or as a best practice. This approach leaves cyber incident prevention and response as a reactionary stance throughout the mission resulting in more and more resources and attention being added as threats evolve over the mission lifetime. To shift this pattern, this paper introduces a first principles approach for cybersecurity requirements that are derived from the definition of mission success.

Requirements development is a core discipline of systems engineering in general, and space mission and system design specifically. Our premise is that starting with the right requirements for cybersecurity will also prove to be a powerful approach for creating cybersecure space capabilities that achieve integrated mission outcomes. By placing cybersecurity requirements at the core of mission planning, rather than as an afterthought in the name of compliance, we pave the way for new best practices to reduce cyber risks and impacts to the overall mission.

The paper describes an integrated requirements development approach to mission design and cybersecurity within the context of the Space Domain Cybersecurity Framework. We emphasize the role of cybersecurity first principles in the framework as a starting point to derive requirements that address fundamental mission needs that depend on cyber resilience. Using the example of the spacecraft on-board Command and Data Handling (CDH) Subsystem, we illustrate requirements allocation across multiple levels of the system architecture. As we trace these requirements from mission goals and first principles down to specifications at the CDH and software subsystem level, we explore the challenges of producing verifiable requirements specifying the form, fit, features, and functions of cybersecurity attributes.