Paper ID: 51239
oral

52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Mr. Julien Airaud
Centre National d'Etudes Spatiales (CNES), France

A HOLISTIC APPROACH TO SPACE CYBER-SECURITY

Abstract

The proposed paper aims to present a holistic approach to space cyber security to protect space missions and assets from the threats targeting their vulnerabilities. From regulations and standards to cyber security controls and processes, this paper will also introduce how Centre National d'Etudes Spatiales (CNES), the French space agency is reacting and adapting.

As our sector is evolving rapidly with emerging actors, new space applications and systems built with redefined hardware, software and operational models, cyber-security actors are converging towards space assets, acknowledging at the same time that states and societies are reliant on them and that space systems are worthy targets with vulnerabilities that can be exploited for greater impact.

From the ground segments (payload and control centers, launch facilities) to the space vehicle itself, space actors have changed their respective practices to research, design, build, launch and operate missions. Cost optimization and time-to-market constraints are not the only drivers impacting the development and procurement processes: partnerships and collaboration agreements, reusability, interoperability, technology exchanges, etc. are as well increasing the attack surface and the likelihood of security incidents. Meanwhile, the volume and the sophistication of cyber-attacks are exploding: all Space actors have to enhance accordingly their cyber security strategy and process, from threat models to cyber operations.

We will explore the resources at hand to build a holistic approach. These resources, regulations, standards, frameworks, collaboration, organizational or technical tools can be reused from the past. Some of them, like tailored Intrusion Detection Systems, can be expected from the future thanks to research and development and market traction. We, as cyber actors, need also to be inspired by others fields: continuous integration in software development, automation from satellite constellations operation, etc. All space evolutions can be therefore perceived as opportunities to leverage the overall level of security but an earlier and deeper integration of cyber security in the whole mission lifecycle will be required. Some of CNES works will be presented to illustrate this new paradigm.