55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Ms. Wichayada Chamnansil
Chulalongkorn University, Thailand

Ms. Suchayaa Khonyaii
Mahidol University, Thailand
Mr. Patcharapol Sankaew
Chulalongkorn University, Thailand
Mr. Chanotai Krajeam
Chulalongkorn University, Thailand
Mr. Chawalwat Martkamjan
Asia Pacific Oceania Space Association-APOSA, Thailand
Mr. Tanis Phongphisantham
Thailand

SECURE BEFORE LAUNCH: SATELLITE SECURITY GUIDELINES VULNERABILITIES CONCERNS FOR SPACE MISSIONS

Abstract

Technology infrastructure such as computer networking, telecommunication systems, and SCADA systems are part of the Industrial Control System (ICS) which have been targeted by attackers. At present, space is playing a more significant role and becoming a part of our industry which is now considered the new frontier of our industry and a new target for hacking. Cybersecurity has been aware for a long time of data security on our internet when space technology takes part in the industry. There are a large amount of data transmitted between space assets and ground stations which may consist of confidential information for various private organizations or information that affects political stability. Although the mentioned data are crucial, cybersecurity aspects were not taken into account during the development process of space assets as they should together with cybersecurity standards for space assets are not regulated by any governing body and lack of regulation which may have serious consequences later. According to the lack of cybersecurity standards and vulnerability of security among the space assets, we aim to analyze potential threats elaborated on the purpose of attackers and vulnerabilities for space assets using previous study cases grouping and analyze a pattern of attacking focusing on 3 points of vulnerability include ground station, radiofrequency, and supply chain which can lead to attacks such as service disruption, loss of control, extortion or ransom, and espionage. Rather than analyzing, we illustrate checkpoints for cybersecurity before launching the mission. This can bring us a goal to demonstrate a new cyber standard for data security awareness of space missions.