IAF SPACE OPERATIONS SYMPOSIUM (B6)
Interactive Presentations - IAF SPACE OPERATIONS SYMPOSIUM (IP)

Author: Mr. Umesh Anilchandra Bhat
Estonian Student Satellite Foundation (ESTCube), Estonia

SECURE MODEL-BASED SYSTEMS ENGINEERING FOR CUBESATS

Abstract

Model-Based Systems Engineering (MBSE) for CubeSat missions starts with a system level model which evolves throughout and often beyond the mission. This mature approach of having a Systems Modelling Language (SysML) model, enables integration between discipline-specific engineering models and simulations. It empowers project stakeholders with a reliable source of system requirements, design, analysis, implementation, and verification. Successful implementation of MBSE results in improved cost estimates, and fewer errors during integration and testing. Furthermore, the insights gained from the current implementation result in numerous benefits in decision-making for the next iteration/mission(s).

But, the involvement of multiple engineering disciplines and software/hardware tools also introduces multiple security risks (further multiplied by complexity) associated with it. This is quite apparent in the case of closed source hardware/proprietary software introduced to CubeSat missions. More often than not, CubeSat missions would involve Commercial off-the-shelf (COTS) components as a cost and time-saving measure. The customer's payloads are often closed as well, resulting in a variety of uncertainties.

Vulnerabilities in one compromised domain/component could potentially affect the entire system unless neutralised. This requires a framework in place to actively negate/contain security incident risks. If not contained, the vulnerabilities could propagate to other domains throughout the evolution of the system.

Conceptualising a secure multi-disciplinary system is ideal, but the security review and maintenance should be "evolution-friendly". It implies that the process of reviewing existing countermeasures and introduction of new ones to the lifecycle should be simple enough (but no simpler), otherwise we start with a reasonably secure system that ends up deteriorating over time.

A few security challenges faced by the MBSE implementation for CubeSat missions are:

- Proper modelling and simulation of the "black-box" components
- Risk Assessment of the disciplines involved
- Prevention of leakage of sensitive information
- Prevention of propagation of vulnerabilities across domains
- Compliance and countermeasures to emerging threats
- Maintaining the risk management framework throughout the evolution of the mission

Our aim is to introduce a security-aware MBSE framework for CubeSat missions with a Proof of Concept (PoC) for the ESTCube-2 (EC2) CubeSat Mission Control (MC). The implementation addresses mission-specific risks, and insights on how to adapt and deploy for all CubeSat missions.