28th IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
22nd Workshop on Small Satellite Programmes at the Service of Developing Countries (1)

Author: Ms. Ibtissam Latachi
Al Akhawayn University in Ifrane, Morocco

Dr. Tajjeeddine Rachidi
Al Akhawayn University in Ifrane, Morocco
Dr. Mohammed Karim
Sidi Mohamed Ben Abdellah University (USMBA) FEZ Morocco, Morocco

# TOWARD A REUSABLE AND FAIL-SAFE FLIGHT SOFTWARE ARCHITECTURE FOR COST-EFFICIENT STUDENT CUBESAT MISSIONS

**Abstract**

After decades of stagnation, the space sector is starting to draw considerable attention. Indeed, the advent of the cubesat concept started a new space era and ignited a considerable shift in satellite development paradigms since 1999. At the time of writing, over 1350 cubecats have been launched. Cubesats evolved from being an early curiosity with limited applications, to being an excellent tool for aerospace capacity-building, thus achieving national self-sustainability in this field. Subsequently, cubesats evolved into being a highly versatile test-bed platform achieving different mission objectives related to earth observation, telecommunication, deep-space exploration, etc. The key factors driving this revolution include standardization, advent of new technologies, agile development approaches, and entrepreneurship. Indeed, cubesats facilitated access to space by opening the possibility of using affordable off-the-shelf components and reusing open-source hardware and reference software architectures. Nevertheless, this flexibility multiplied the inherent risks commonly encountered in aerospace projects. These risks are further exacerbated by following ad-hoc development approaches, often due to the lack of simple guidelines in the literature. To mitigate these risks, it is crucial to devise reliable hardware and software architectures. Therefore, this work aims to establish processes to design a reusable and reliable software architecture for a student-built cubesat mission and serve as an initial reference for flight software development in Morocco.

Our development methodology is based on a system engineering approach applied throughout the mission life cycle within a custom-tailored ECSS framework. Moreover, our design approach relies on implementing a reliable hardware architecture using off-the-shelf modules with extensive flight-heritage, while focusing all efforts on developing a simple, yet reliable software solution that verifies key quality criteria, such as reliability, modularity, reusability and extensibility. The onboard computer chosen is a COTS system-on-module running FreeRTOS to enable real-time onboard management. To ensure overall mission reliability, a feasible strategy was devised. It relies on using modular hardware and software architectures onboard, defensive programming, and throughout software verification & validation testing. Moreover, following the fail-safe approach, a hierarchical fault-tolerance architecture was implemented after systematic assessment of the possible risks using reliability block diagrams and functional FMECA. Finally, to ensure modularity, reusability and extensibility, the flight software follows a layered, service-oriented architecture with a finite state machine implemented in the application layer for deterministic execution of the mission functionalities. A client-server model, leveraging uniform APIs and CSP protocol network infrastructure, was also used to ensure resources access and enhance cross-platform data exchange.