Paper ID: 84951
oral

57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
For a successful space program: Quality and Safety! (1)

Author: Ms. Silvana Radu
European Space Agency (ESA-ESTEC), The Netherlands

Dr. Paulo Rosa
Elecnor Deimos, Portugal
Mrs. Benedicte Girouart
European Space Agency (ESA), The Netherlands

SAVOIR FDIR HANDBOOK: INSIGHTS FROM THE LATEST UPDATE

Abstract

Space AVionics Open Interface aRchitecture is an initiative to federate the space avionics community and to work jointly in order to improve the way that the European Space community builds avionics subsystems to improve and align the design processes, multiple working groups have been established between ESA, Agencies and Industry to produce documentation that shall support the objectives of SAVOIR.

Among domains covered by SAVOIR is the Fault Detection, Isolation, and Recovery (FDIR) discipline, for which a dedicated working group was created, entrusted with the responsibility of preparing the FDIR handbook published in 2019 (SAVOIR-HB-003).

FDIR and system engineering are transversal disciplines that complement each other. System engineering aims to develop a system with the purpose of behaving in a way that achieves mission objectives and system requirements, while FDIR engineering aims to cover the unwanted behavior which may prevent the system to achieve its goals. FDIR engineering is a viewpoint of system architecture and follows similar processes and schedule. Adequate health management can be complex to handle, requiring a specific mindset, especially when addressing concerns or conditions that vary significantly depending on mission.

After several years of use, ESA, together with agencies, industrial and academic organizations, decided, through the SAVOIR Advisory Group (SAG), to reconvene the SAVOIR FDIR working group and revise the handbook based on lessons learned. The need of updating the handbook was identified due to the realization that some topics were to be added, or that the handbook was to be tailored for specific, less conventional missions. The work performed by the working group aimed to address these issues and culminate in an updated version of the handbook.

The objective of the paper is to present these changes, justifying the choices made and providing details on how the proposed FDIR design and practices are adapted for specific missions, such as CubeSats or Close Proximity Operations (CPO), all based on lessons learned, gathered from ESA, Agencies and Industry.

Moreover, the paper tackles some of the Reliability, Availability, Maintainability and Safety (RAMS) additions which help clarify the use of RAMS tools in support of FDIR design, process, and verification. Apart from the changes implemented, the paper and the update of the handbook highlight, to the space community, the importance of health management and the adoption of common and well-established practices for the development of FDIR for spacecraft platforms, tailored for unconventional missions, but fundamentally based on lessons learned.