GNC System Verification and Certification Processes

by Mr. Tewodros Beyene & Mr. Harald Ruess (FORTIS GmbH)

FORTISS has expertise on the implementation of methods for the certification of the design and development of Guidance, Navigation, and Control (GNC) critical systems for civil aviation. Critical GNC systems for space could take benefits from the expertise accumulated in the civil aviation industry.

FORTIS has completed for ESA the assessment of a methodology for the certification of safety GNC critical space systems with two aims in view:

- To improve the certification processes (verification, validation, and certificate issuing) of safety GNC critical space systems with the goal to reduce the cost, manpower and time for certification.
- To perform research on alternative approaches to reliability and certification to the current practices.

The safety GNC critical space systems conceptual design starts in an early phase A and it is an iterative process that takes place simultaneously with, and is dependent on the definition of mission requirements, to ensure the mission goals, objectives and boundaries are met. The safety GNC critical space system design shall encompass all hardware, software, operation elements of the system, all phases of the mission, all aspects of operating the system, the mission environment, the available resources and risk for the mission.

Safety GNC critical space systems are designed and built more and more with complex FDIR and HMS systems inside. And dues to the nature of the space missions, today's safety GNC critical space systems engineering is lacking a systematic approach and transparency of the entire engineering process. Hence, a consolidated formal process able to fit the safety GNC critical space system certification concept to mission goals and objectives, trade-off between fault tolerance level and required autonomy and the FDIR strategies is needed. This process shall also aim to decrease overall complexity of the designed system.

Top-down and bottom-up assessments are all needed. ECSS standard identifies several methods to support the assessment of software dependability and safety (such as FMECA, FTA, HW-SW Interaction Analysis, Hazard Analysis, and Common Cause Failure Analysis). However, they are often available late in a mission's lifecycle and often leading to a late initiation of the FDIR development with unfavourable effect in the maturity level of the FDIR design.

Recent sensors' auto-diagnostic capabilities are proving that the next generation of sensors will enable more efficient FDIR and health monitoring systems, allowing simplification with equivalent coverage using decentralised architecture. This new generation of sensors will have processing capabilities (SW or ASIC) which do not only provide a pointing error measurement to the AOCS functional chain, but allow a sophisticated autonomous and local assessment of nominal or anomalous behaviour, which the sensor can transfer to the higher level for Failure Detection and Isolation (but not Recovery) purpose.

The certification of safety GNC critical space systems involves the successful verification process of the GNC, the successful validation process of the GNC system, and the final procedure by which an authority gives formal assurance that all procedures have been completed correctly.