GmbH

Guideline for the Promotion of Critical Flight Software to ECSS Category A

Method and tools to achieve the challenging and strictest criticality level

Andoni Arregui (GTD GmbH) | 2023-05-31

Abstract

Flight software development to ECSS Category A qualification level is a technical challenge that up to now has not been required too often in the European space industry (e.g., ATV MSU, ESM PDE)[Bou] [Pre] and for which the production of qualification evidences and the corresponding Software Product Assurance activities to verify them are not straight forward although the requirements are clear in ECSS. Currently more and more space systems require operating systems and software building blocks to be qualified to category A, to enable the development of project specific category A software on top of them for new high criticality applications (e.g., I-HAB, ERM, Space Rider, MSR-ERO, ADRIOS). As many of these operating systems and other software building blocks are qualified up to ECSS Category B, we developed on behalf of ESA a methodology and its accompanying tools to systematically upgrade such software components up to category A. Together with the open source tools based methodology GTD developed to help in the achievement of the required MC/DC structural coverage and the object to source code traceability verification, we will address the Software Product Assurance related aspects to ensure that the right questions can be posed from this perspective to properly assure this highest criticality software.

The requirements to obtain a category A qualification are clearly defined within the ECSS E-ST-40C and Q-ST-80C but the methods and tools to achieve these requirements are not. Neither is it easy from the Software Product Assurance point of view to review this evidence and pose the right questions to achieve the required level of confidence.

The produced guideline addresses the production of evidence for the required full MC/DC coverage and the verification of the traceability between object and source code while it also aims at giving the Software Product Assurance teams enough information on how to interpret the produced evidence and to ask the right questions to the engineering teams to ensure that they also correctly interpret the produced evidence. The focus of the presentation will be on the best practices for the Software Product Assurance Teams when facing category A qualification processes.

References

[Bou] Olivier Boudillet. *Category A Software Development for the ATV.*

[Pre] Antonio Preden. *Critical Software for Human Spaceflight - The equipment software for Orion Propulsion.*