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

Author: Mr. Andoni Arregui
GTD, Germany

Mr. Fabian Schriever
GTD, Germany
Mr. Christoph Weiß
GTD, Germany
Mr. Thomas Wucher
GTD, Germany

ENSURING SAFETY IN CRITICAL CATEGORY 'A' FLIGHT SOFTWARE THROUGH MC/DC AND OBJECT-TO-SOURCE TRACEABILITY VERIFICATION

Abstract

The demand for human-rated, safety criticality 'A' flight software is rapidly increasing due to new challenges in space exploration that require international collaboration. For these most critical pieces of software, international standards such as the European Cooperation for Space Standardization (ECSS) in the space industry and the DO-178 for civil avionics require the achievement of Modified Condition/Decision Coverage for structural coverage and the verification of object-to-source code traceability.

Achieving MC/DC coverage will shed an additional light onto the yet unverified logical behaviours of flight software. The object-to-source traceability verification will shed light onto that last step of flight software generation which is else left unverified –the compilation and linking process– ensuring no unverified behaviour is added to the software.

Despite clear requirements for this kind of software are outlined in the ECSS standards, a thorough assessment of previous experiences –including the Automated Transfer Vehicle (ATV), and the Orion European Service Module's Propulsion Drive Electronic (PDE)– reveals that the approaches employed to show evidence for category 'A' requirements are often flawed. This discrepancy underscores the need for a systematic approach to software development for current and future challenges.

Recognising this, the European Space Agency (ESA) saw the need for a systematic approach when developing this type of software. In this framework, GTD was commissioned to develop guidelines and open-source tools aimed at assisting software engineers in systematically applying techniques to meet these stringent requirements.

This paper will present the primary concerns addressed by MC/DC and object-to-source code traceability verification, the tools developed, and the application of these guidelines. Our focus will be primary from a software engineering perspective, aiming to demonstrate how these techniques can enhance software development and ensure safety. This shall be done without becoming a burden to the software development imposed by a standard or the Software Product Assurance Process, or reliance on opaque proprietary tools. The tools presented are meant to contribute to free the application of these techniques

from the constraints of specific toolsets.

Software engineers should be able to experiment and apply the techniques discussed using the proposed open-source tools, enabling them to choose the most suitable tools for their projects.