Paper ID: 17108
oral

46th SYMPOSIUM ON SAFETY AND QUALITY IN SPACE ACTIVITIES (D5)
Knowledge Management and Collaboration in Space Activities (2)

Author: Mr. Glauco da Silva
Institute of Aeronautics and Space (IAE), Brazil

Dr. Carlos Lahoz
Institute of Aeronautics and Space (IAE), Brazil

A NEW PROCESS FOR SPACE COMPUTER SYSTEM DEPENDABILITY ANALYSIS

Abstract

Many of the space safety engineering practices currently used for computer critical systems are still traditional approaches, such as Failure Modes and Effects Analysis (FMEA). Although, when properly adapted could be obtain significant results, this kind of analysis should not be limited to use only these techniques, due to the contribution of software in accidents is completed different from those involving purely mechanical or electronic components. Furthermore, in safety analysis the massive amount of data to be analyzed need intelligent ways to assist in the process of gathering information and support the decision process, to evaluate, classify and organize the critical items, the potential severity of failures, the common mitigation provision that could be adopted, and to create a history of potential solutions to reuse. This paper presents the studies to create a new model of space computer dependability analysis, called PRO-Elicere that intends to associate traditional knowledge of safety analysis, as software FMEA (SFMEA) and software Hazard and Operability Studies (SHAZOP), to intelligent mechanisms to decision support to analyze the potential hazards and failure of a critical system. First, some techniques and tools that support to space system dependability analysis will be present in order to identify the current approaches that explore the use of computational resources, both to hardware and to software hazard analysis. After that, the paper will briefly discuss how to combine the use of traditional dependability analysis techniques (SFMEA and SHAZOP) and the concept of knowledge discovery and intelligent databases, in order to improve the dependability of space critical computer systems. Finally, the expected result of this research is that the PRO-Elicere could be a part of the Verification and Validation (VV) software activities of the projects under development by Aeronautics and Space Institute (IAE), such as the Brazilian Satellite Launcher (VLS). The VLS is a small rocket, originally designed to launch satellites for environmental data collection and remote sensing.