SPACE SYSTEMS SYMPOSIUM (D1)
System Engineering Tools, Processes and Training (1) (3)

Author: Dr. Carlos Lahoz
Institute of Aeronautics and Space (IAE), Brazil, lahozchnl@iae.cta.br

Mrs. Luciene Alves
National Council for Scientific and Technological Development (CNPq), Brazil, lubialves@gmail.com
Mrs. Martha Abdala
Institute of Aeronautics and Space (IAE), Brazil, marthamada@iae.cta.br

DEPENDABILITY TECHNIQUES APPLIED IN A CASE STUDY OF SPACE SOFTWARE

Abstract

This paper describes the approach of using combined dependability techniques for verification and validation (VV) of a space software, as part of a research project performed at Institute of Aeronautics and Space (IAE/Brazil). The case study used to practice the dependability techniques are based on the flight software of the Brazilian Satellite Launcher (VLS). Dependability techniques such as Software Fault Tree Analysis (SFTA) and Software Failure Modes, Effects and Criticality Analysis (SFMECA) are adjusted and applied to identify common causes of software failures, its criticality, performance problems and hazards arising mainly from dysfunctional interactions between software and system components. Although these techniques are not new, the SFTA top-down combined to SFMECA bottom-up approach intents to reduce these techniques workload and makes use of the advantages of each one. At the end, the compensating provisions obtained from the process application helped to identify new functional and non-functional requirements to improve the VLS software dependability. The proposed approach was divided into four distinct activities: 1) Preparation for dependability process application: this activity consists of tailoring the SFTA and SFMECA techniques for application in the system under investigation, and defines more suitable items used in dependability analysis, for instance the severity levels, the criticality classification and the generic failure modes. 2) SFTA analysis: a fault tree is designed based on the possible failures in the system requirements for software and the consequential failures in the respective software requirements. In this approach, the basic events are characterized by software failure in meeting system requirements. 3) SFMECA application: the SFMECA is applied in the SFTA basic events and HAZOP (Hazard and Operability studies) guidewords are used to classify generic failure modes, taking into account the deviation of design intent related to resources (data or physical devices) or tasks (event or data flow), that have a relationship with the system component analyzed. 4) Identify new requirements: from the compensating provisions extracted by SFMECA analysis, new functional and non-functional requirements could be suggested and incorporated into the software design and code. The sequence of the vehicle events under responsibility of the flight software is presented, as example to explain how the dependability techniques should be applied. These events characterize the several phases for which the vehicle must pass for the execution of its mission. Also, the customized items used in the combined dependability analysis can be reused in other similar software space projects.