SPACE SYSTEMS SYMPOSIUM (D1)
System Engineering Tools, Processes & Training (I) (3)

Author: Dr. Miriam Alves
Institute for Aeronautics and Space (IAE), Brazil, miriammcba@iae.cta.br

Dr. Doron Drusinsky
Naval Postgraduate School, United States, ddrusin@nps.edu
Dr. James Bret Michael
Naval Postgraduate School, United States, bmichael@nps.edu
Dr. Man-Tak Shing
Naval Postgraduate School, United States, shing@nps.edu

MAKING SPACE SYSTEMS MORE DEPENDABLE: A PARADIGM CHANGE FOR VERIFICATION AND VALIDATION

Abstract

Space systems have an intrinsic requirement that distinguishes them from other applications: the final product has to be highly dependable. Improvements in the quality of flight and ground systems are intrinsically influenced by how effectively Verification and Validation (VV) activities take place when developing software systems. The increasing demand for lower development costs and faster delivery time, while maintaining high quality requirements, has imposed new challenges to the research and space industry communities to put forward more optimized and efficient VV techniques. Recent changes in the software development paradigm, which centers on the development of formal specifications and design models that will serve as a basis for the system development, moved the focus of the VV activities from testing and code analysis to analyzing and testing the specification. Extensive model validation will be necessary to attend these new demands. New efficient and effective VV techniques are needed to augment and, in some cases, to replace the techniques currently in use. Moreover, to make the VV process substantial and suitable for the space industry, the use of new techniques also imposes new challenges for more reliable supporting tools and flexibility in the current space software standards. This paper presents a formal technique and a supporting tool for VV with the potential to meeting these new challenges. The technique, based on statechart-assertions, makes it possible the creation of a formal specification model that represents the customer requirements and allows the validation of this formal specification against the customer understanding of what the system should do, what it should not do and how it should react under adverse conditions. Time-constraint requirements can be validated and verified by observing the system temporal properties over time. The refereed technique has been successful used in some space software systems and to date, the research results and experience have shown that the technique fits well in the new context of multinational space system development, where the software VV activities are distributed across the globe. One of the big advantages of this formal technique is its flexibility of application and facility of use, generating rapid results, without compromising time and costs.