49th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Risk Management for Safety and Quality in Space Programs (1)

Author: Mr. BENEDITO SAKUGAWA
Agência Nacional de Aviação Civil - ANAC, Brazil

Dr. Ana Maria Ambrosio
Instituto Nacional de Pesquisas Espaciais (INPE), Brazil
Prof. Geilson Loureiro
Instituto Nacional de Pesquisas Espaciais (INPE), Brazil
Dr. Carlos Lahoz
Instituto de Aeronáutica e Espaço (IAE), Brazil

A FRAMEWORK FOR OVERSIGHT OF SOFTWARE'S SUPPLIERS OF SAFETY-CRITICAL SPACE SYSTEMS BASED ON CIVIL AVIATION BEST PRACTICES

Abstract

The Brazilian Program of Space Activities for the period 2012-2021 has among its priorities: to engage industry at all stages of the space project development, the standardization and certification, and mastering of critical technologies. Considering the outsourcing growth of increasingly complex systems, the certification demand tendency, the relevance and critical role of software for embedded space systems, the commonality between space and aviation domains, and the current maturity level of Brazilian space industries, this paper presents a framework for oversight of software's supplier of safety-critical space systems, based on metrics and best practices of the civil aviation. The metrics are used for evaluation of the oversight and decision making support. They are generated by using the civil aviation past twelve years oversights' results. Those oversights have been performed by the National Civil Aviation Agency (ANAC), some jointly with the Federal Aviation Administration (FAA) and the European Aviation Safety Agency (EASA), mostly on-site at the supplier's facilities, and comprises systems for flight controls, brake, landing gear, electrical generation and distribution, pressurization, cockpit displays, flight management, etc. Software safety systematic comparison between space and aviation domains was performed in order to identify the potential reuse level from aviation and adjustments due to space specific necessities. The comparison shows a great amount of aviation reuse, but due to the space necessities many additions covering different topics are needed (e.g., delivery and acceptance, inflight modification), but the identified differences do not preclude the framework viability. The framework is built on the standards of the European Cooperation for Space Standardisation (ECSS) as base, and focuses on relevancies of company, process and product for software safety impact, together with a reduced set of activities. We believe this approach can better suit to the current stage of Brazilian space industry (small companies), and can help in reducing to an acceptable level the presumed inherent risk that space systems software outsourcing has in adversely impacting safety, by identifying project problems and product potential problems at earlier stages of software development.