IAF SYMPOSIUM ON COMMERCIAL SPACEFLIGHT SAFETY ISSUES (D6)
Commercial Spaceflight Safety and Emerging Issues (1)

Author: Dr. Ronald Freeman
American Institute of Aeronautics and Astronautics (AIAA), United States

DETECTING UNKNOWN AND UNDERAPPRECIATED (UU) RISKS IN THE PRIVATE SECTOR OF SPACE OPERATIONS AND SAFETY

Abstract

Privatization of American aerospace industry indicates a progressive assumption of space operations to realize space servicing needs and exploration objectives. Whether or not SSAs were the appropriate legal instrument for aerospace commercialization, other risks traditionally assessed such as safety and technical risks were not addressed. The risk for launch failures producing loss of control, low performance, or material damage is no longer theoretical in the private sector. The most effective and inexpensive option from the natural hierarchy of design choices of hazard elimination/control is to implement at the outset of engineering design. One potential cause of poor design is insufficient attention given to requiring sound human and automation/robotic integration. Human factors engineering is used during the design phase to reduce human error by making machines and systems error tolerant. This paper explores several methods in the literature that are used to address unknown and underappreciated (UU) risks of each component (hardware, software, or human) and the reliabilities of their interfaces. There are multiple possible conflicting goals in the design and operation of a complex system, including that between safety and immediate productivity. An effective process for interaction design requires sound analysis of the work to be supported, or needs analysis. An explicit needs analysis should guide the requirements specification for an automation or software system. The needs analysis should be used to guide not only verification (that the implemented system matches requirements) but also validation (that the system serves the intended needs). The paper further explores future trends in safety-guarding complex adaptive systems per innovative cyber-physical system task analysis methods and Satisfiability Modulo Theory-based solvers that are used to check verification conditions generated during safety property checking of programs.