52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Quality and safety, a challenge for traditional and new space (1)

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

INTEGRATED SAFETY ANALYSIS: A TOOL FOR THE SAFE OPERATIONS OF COMPLEX ADAPTIVE SYSTEMS

Abstract

Traditional hazard analysis techniques do not deliver adequate insight early in the design process, when most of the safety-related decisions are made. Furthermore, traditional techniques based on reliability theory resulted in the use of excessive design margin and redundancy as the "default" vehicle design choices. This equivocation of safety and reliability may have made sense for simpler launch vehicles of the past, but most modern space launch vehicle accidents have resulted from incorrect software specifications, component interaction accidents, and other design errors independent of the reliability of individual components. The successful Probabilistic Risk Assessment approach eliminated hazards and enabled high reliability in safe operations and overall mission outcome during the Apollo Program. Subsequently, "faster, better, cheaper" space program initiatives which focused on accelerating technological performance shifted from hazard analysis and prevention to risk management of optimal tradeoffs between safety and costs. From 1980 to 2015, 35This paper will explore current and future methods proposed to mitigate hazardous behaviors due to complexities of emergent component-component interactions that violate system safety goals. Addressing management issues of both hazards and design errors indicate an Integrated Safety Analysis (ISA) by which systems engineering and risk management decisions are risk-informed and used to develop a risk-informed safety cases (RISC) to ensure that significant gaps or faults leading to safety deficits are identified and corrected.