9 System Safety Considerations

9.1 System Safety

System safety is a standardized management and engineering discipline that integrates the consideration of human, machine, and environment in planning; designing; testing; and maintaining operations, procedures, and acquisition projects. System safety is applied throughout a system's lifecycle to achieve an acceptable level of safety risk within the constraints of operational effectiveness, time, and cost.

For each new system acquisition, the Program Office (PO) must establish and implement a System Safety Program that meets the requirements of the Air Traffic Organization (ATO) Safety Management System (SMS). The status of system safety must be presented at all decision points and investment reviews. Detailed guidelines for safety management and development assurance are found on the Federal Aviation Administration (FAA) Acquisition System Toolset (FAST) website; in the ATO SMS Manual; in SAE Aerospace Recommended Practice (ARP)[1] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; in RTCA[2] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; and in RTCA DO-254A, *Design Assurance Guidance for Airborne Electronic Hardware*.

Section 5.4 of the preliminary Program Requirements Document (PRD) constitutes the safety plan required by the Safety Risk Management Guidance for System Acquisitions (SRMGSA) for the Investment Analysis Readiness Decision (IARD). The PO must develop a Program Safety Plan (PSP) consistent with this safety plan for the IARD and update it for the Initial Investment Decision (IID) and Final Investment Decision (FID). The PSP's scope, content, and list of required Safety Risk Management (SRM) activities are based on the Safety Strategy Meeting that should be conducted between the PO and the Safety and Technical Training (AJI) Safety Engineering Team, AJI-314.

9.2 Integrated Safety Management

The highly distributed and interconnected nature of the National Airspace System (NAS)—and Next Generation Air Transportation System (NextGen), in particular—presents complex safety challenges to the NAS. In addition, many changes to the NAS necessary for implementing NextGen initiatives may occur in a parallel or overlapping manner. The past SRM paradigm was focused on analyzing individual changes; it was insufficient for addressing all the hazards identified as a result of the planned interactions and interconnectivity.

The legacy NAS is a "system of systems" that provides multiple services to users. The NAS is evolving into an even more complex configuration. Future acquisitions are beginning to blur the lines of a "system" with defined/fixed boundaries and interfaces. Systems, programs, and projects no longer have unique or exclusive functionality. In fact, the functionalities not only overlap, but may also build on one another, subsume each other, or combine for a joint function or capability. This perspective was not considered historically but is important to applying the concept of integrated safety in acquisitions. Integrated Safety Management must be performed to assess risks of initiatives in support of agency Risk-Based Decision Making.

1. An ARP is a guideline from SAE International.
2. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."