4.12 National Airspace System Safety Management System Revised 1/2012

When new capital investments are determined to have an effect on the safety of the National Airspace System, safety management shall be conducted and documented throughout the lifecycle of a product or service in accordance with the FAA Safety Management System (SMS). The safety management system requires use of safety risk management to identify safety risks to the National Airspace System and to conduct product development at a rigor commensurate with the severity of the resultant hazard should that product experience failure. For software-intense systems, the establishment of a development assurance program in accordance with RTCA Document (DO) 278A, Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management Systems, RTCA, Inc., is one acceptable means to demonstrate that a software product was developed at the appropriate level or rigor.

Critical safety issues identified during service analysis are further addressed in: (1) an operational safety assessment; (2) a system safety assessment of alternative solutions to mission need reported in the business case; and (3) when service organizations provide program-specific safety risk management planning in the implementation strategy and planning document.

Each service organization involved in acquisition management shall institute a system safety program that includes at a minimum: hazard identification, hazard classification (severity of consequences and likelihood of occurrence), measures to mitigate hazards or reduce risk to an acceptable level, verification that mitigation measures are incorporated into product design and implementation, and assessment of residual risk. Status of system safety shall be presented at all decision points and investment reviews. Detailed guidelines for safety management are found in FAST, FAA SMS manual, SRMGSA, and RTCA DO-278A.