

CHANGE REQUEST COVER SHEET

Change Request Number: 11-64

Date Received: 11/8/2011

Title: System Safety Management

Name: David Woodson

Phone: 202-267-7601

Policy OR Guidance: Policy

Section/Text Location Affected: 4.12 System Safety Management

Summary of Change: Revises current policy to reflect that software assurance processes are at a level commensurate with safety analysis results

Reason for Change: To converge to a common set of software development assurance methodologies between air and ground systems as they apply to the safety of the National Airspace System

Development, Review, and/or Concurrence: AJS, AOV, AVS, AVP, AIR, AJP, AJE, AJW, AJA

Target Audience: Ground systems software development offices

Potential Links within FAST for the Change: None

Briefing Planned: No

ASAG Responsibilities: None

Potential Links within FAST for the Change: None

Links for New/Modified Forms (or) Documents (LINK 1)

Links for New/Modified Forms (or) Documents (LINK 2)

Links for New/Modified Forms (or) Documents (LINK 3)

SECTIONS EDITED:

Acquisition Management Policy:

Section 4.12 : National Airspace System Safety Management System [\[Old Content\]](#) [\[New Content\]](#) [\[RedLine Content\]](#)

SECTIONS EDITED:

Section 4.12 : System Safety Management

Old Content: Acquisition Management Policy:

Section 4.12 : System Safety Management

Safety management shall be conducted and documented throughout the lifecycle of a system in accordance with the FAA's Safety Management System (SMS). The SMS requires use of safety risk management to identify safety risks to the National Airspace System.

Critical safety issues identified during service analysis are recorded in an enterprise architecture roadmap; a system safety assessment of alternative solutions to mission need is reported in the business case analysis report; and 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 and in the FAA's SMS manual.

New Content: Acquisition Management Policy:

Section 4.12 : National Airspace System Safety Management System

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.

FAST Version 01/2012

CR 11-64

p. 2

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.

Red Line Content: Acquisition Management Policy:

Section 4.12 : National Airspace System Safety Management System

Safety***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 system product or service in accordance with the FAA's Safety Management System (SMS). The SMS 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 ~~recorded~~***further addressed*** in: ***(1) an enterprise architecture operational safety roadmap; assessment; (2) a system safety assessment of alternative solutions to mission need-is reported in the business case analysis report; 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 ~~and in the~~, FAA's SMS manual, ***SRMGSA, and RTCA DO-278A.***
