

Safety Management and the Use of EA

Presented to: NASEA Conference

By: James Daum, Safety Group Manager (AJP-19)

Date: June 25, 2009



Federal Aviation
Administration

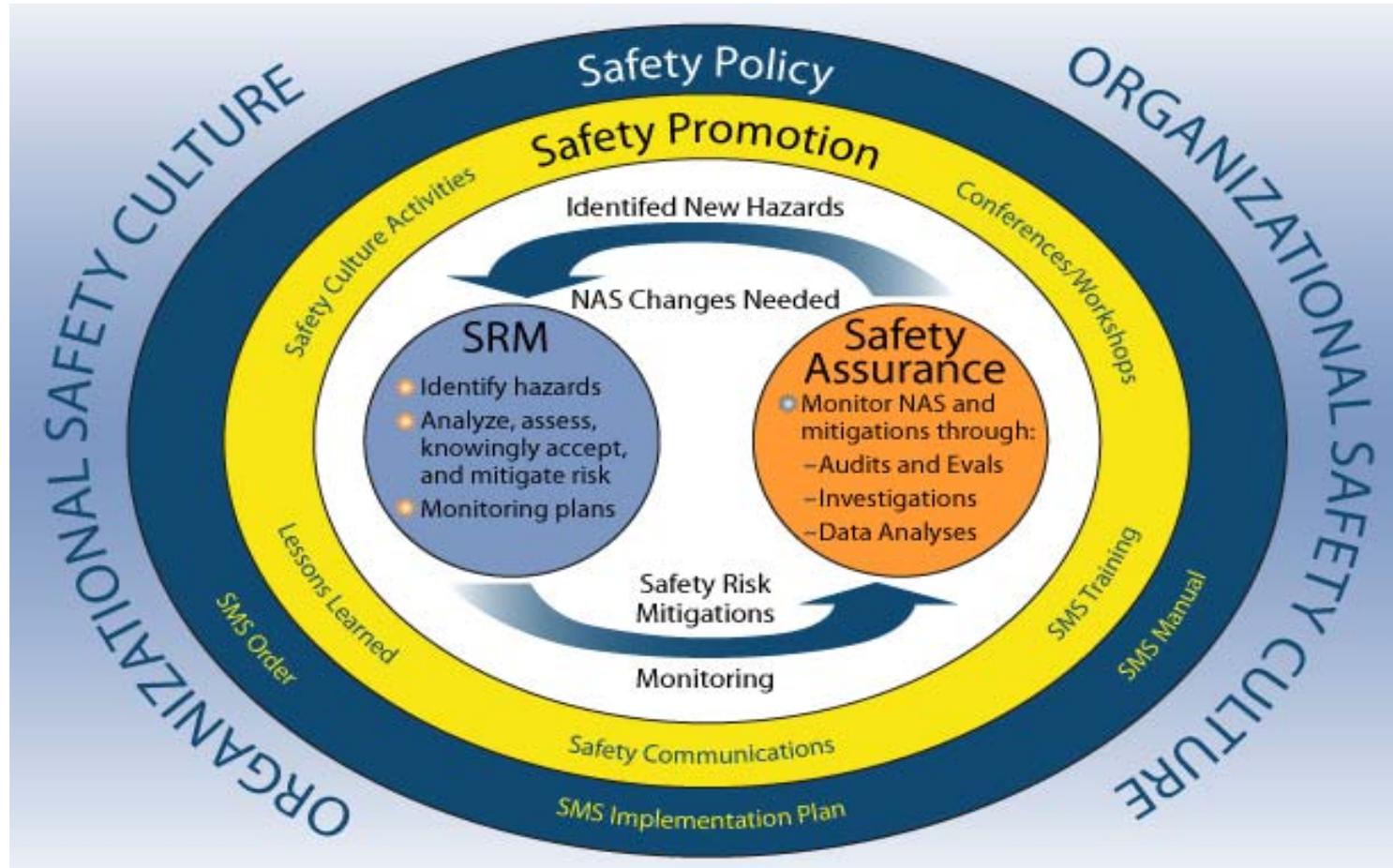


Safety Management Basics

- **What is safety?**
 - Freedom from unacceptable risk
- **What does the Safety Management System (SMS) provide?**
 - The SMS provides a systematic and integrated method for managing the safety of Air Traffic Control (ATC) and navigation services in the NAS.

Aviation safety is the fundamental mission of the Federal Aviation Administration.

Safety Management System



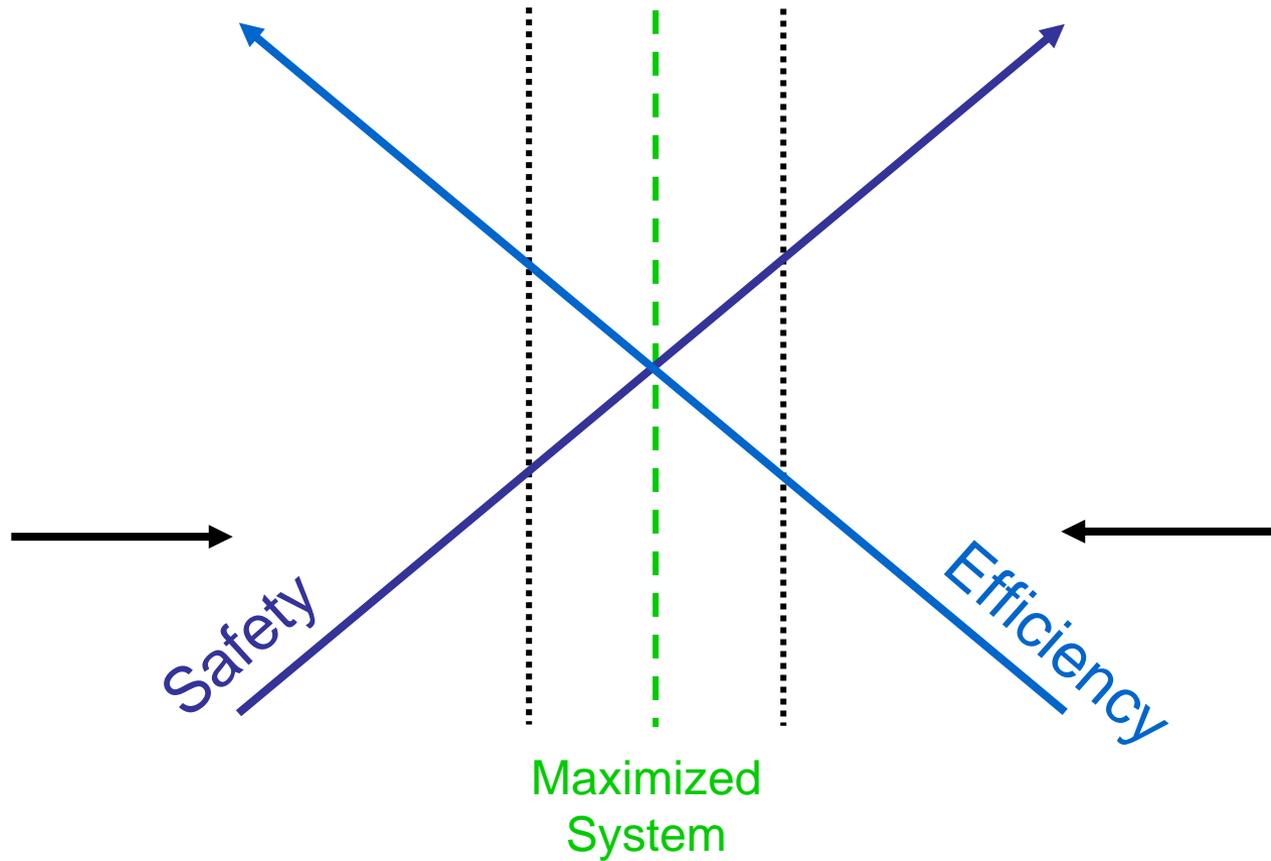
Safety and NextGen

- **U.S. air transportation system (NAS) is the safest in the world**
- **NextGen safety objective**
 - Make the NAS ***even more safe*** than it already is.
- **Why the need to increase safety?**
 - Significant growth and increased complexity in the air transportation system requires commensurate improvement in safety performance.
- **How will we meet this NextGen safety objective?**
 - Evolve from today's post-accident data analysis to integrated historical and prognostic evaluation and management of hazards and their potential safety risk to prevent future accidents.
 - Design the future air transportation system and safety management systems to control relatively benign events and how they combine in unexpected ways to create hazardous conditions.

“ATO’s most fundamental imperative is to ensure the safety of the national airspace system. ...

Therefore, as we build the Next Generation Air Transportation System, the resulting cross-organizational changes to the NAS will require us to maintain an intensive, proactive, and systematic focus on safety. This focus is achieved through the implementation of the Safety Management System (SMS).” Hank Krakowski, Chief Operating Officer, Air Traffic Organization

NextGen Safety Challenge



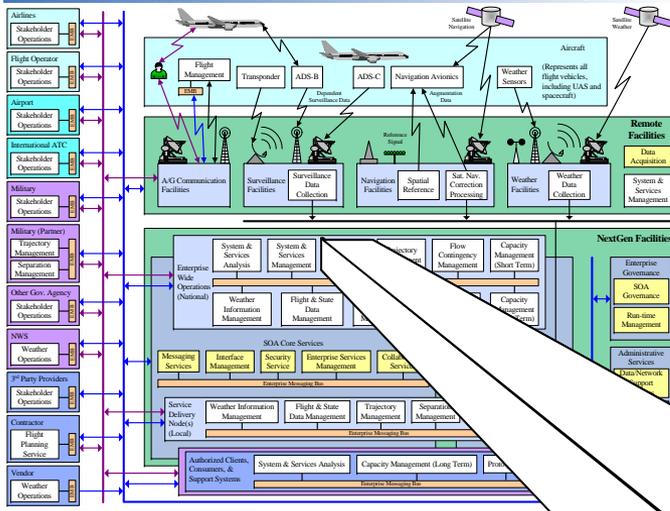
EA Helps Meet NextGen Safety Objectives

- **Programmatically via:**
 - The Safety Infrastructure Roadmap
- **Technically via:**
 - System Views to identify systems that support the SMS
 - Operational Views of how SMS integrates with NAS activities
 - Technical Views that document safety standards
 - System Views/Operational Views that feed the SRM process
 - System Views/Operational Views document SRM mitigations
 - System View Overlays to highlight areas of safety risk

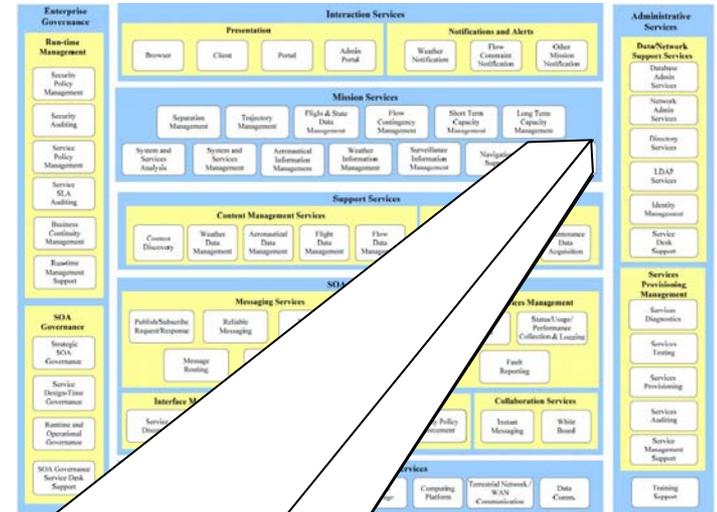


Safety Systems

SV-1 System Interface Description



SV-4 Systems Functionality Description



EA Helps Meet NextGen Safety Objectives Technically via the System Views

Safety Management Services

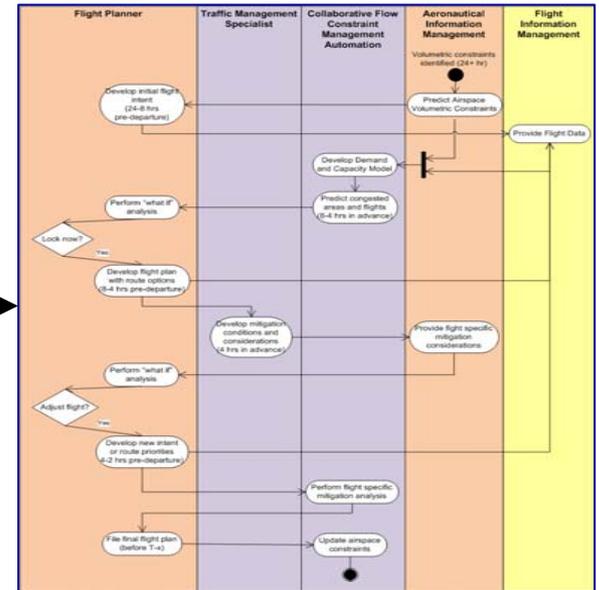
- Trend Analysis
- Failure Prediction
- Risk Prediction
- Risk Management
- Safety Data Publication



SMS Depiction in EA



SMS Integrated
With NAS Activities



Safety Management System

OV-5 Operational Activity Model
(future development)

EA Helps Meet NextGen Safety Objectives Technically via the Operational Views

Safety Management Standards

TV-1 Technical Standards Profile

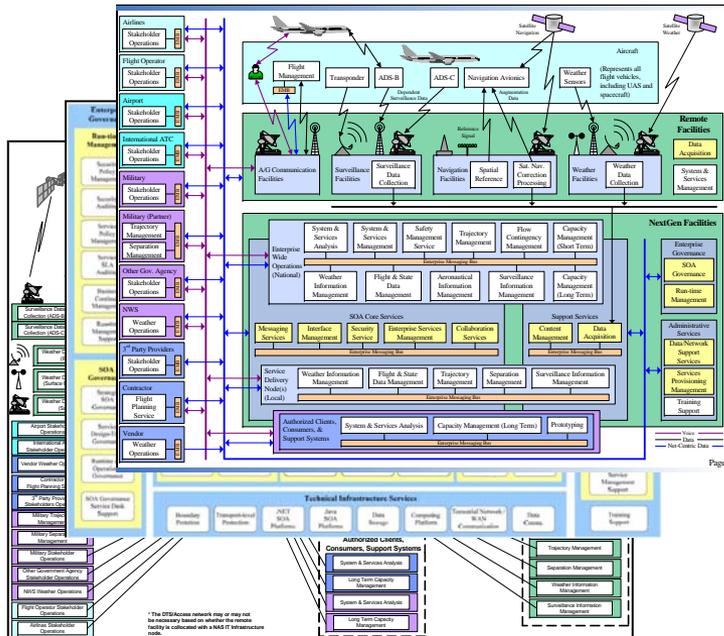
Standard Designation	Standard Title	Standard Date
7.0 Aviation Related Standards		
7.10 Safety		
FAA NAS Mod SSMP	NAS Modernization System Safety Management Program	March 24, 2003
FAA AC 25.1309A	System Design Analysis	June 21, 1988
FAA ATO	Safety Management System Manual, Version 2.1	May 1, 2008
FAA Order 1100.161	Aviation Safety Oversight	
FAA Order 8040.4	Safety Risk Management	June 26, 1998
FAA Order 8740.1E	Aviation Safety Team Program Manager's Handbook	May 30, 2007
FAA Order JO 1000.37	Air Traffic Organization Safety Management System	
FAA SRMGSA V1.4a	Safety Risk Management Guidance for System Acquisitions	February 8, 2007
FAA SSH	System Safety Handbook	December 30, 2000
ICAO Annex 11	Convention on International Civil Aviation Aeronautical Telecommunication, Annex 11, Section 2.26	
ICAO Doc 9859 AN/460	ICAO Safety Management Manual (SMM)	2006
RTCA DO-178B	Software Considerations in Airborne Systems and Equipment Certification	December 1, 1992
RTCA DO-264	Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications	December 14, 2000
RTCA DO-278	Guidelines for Communications, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance	March 5, 2002
SAE ARP4761	Aerospace Recommended Practice - Guidelines and Method for Conducting Safety Assessment Process on Airborne Systems and Equipment	December 1, 1996

**EA Documents
Safety
Management
Standards
Technically via
the Technical
Views**

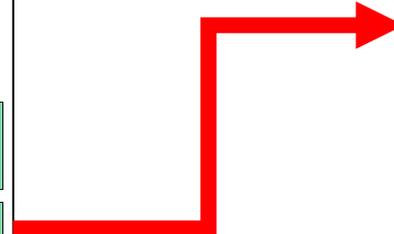
TV-2 Technical Standards Forecast – in development

EA Provides Input to SRM

Safety Risk Management Process

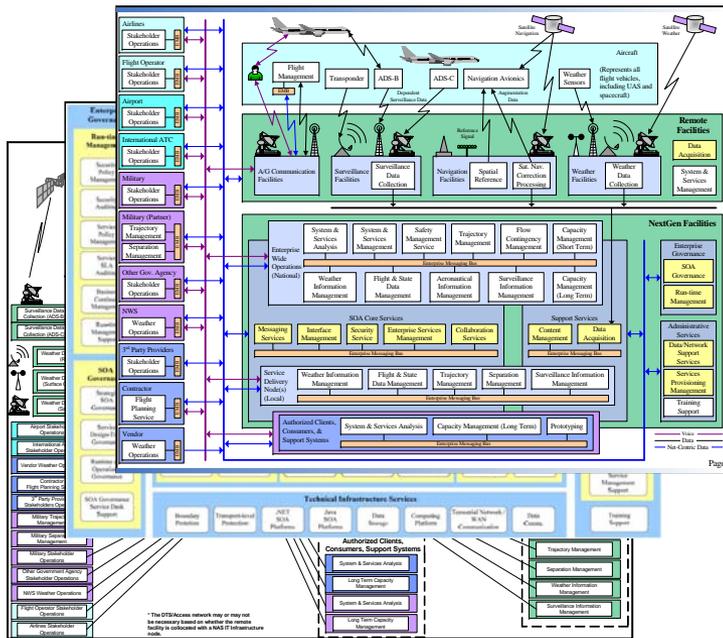


NASEA Views



SRM Results Feed EA

NASEA Views

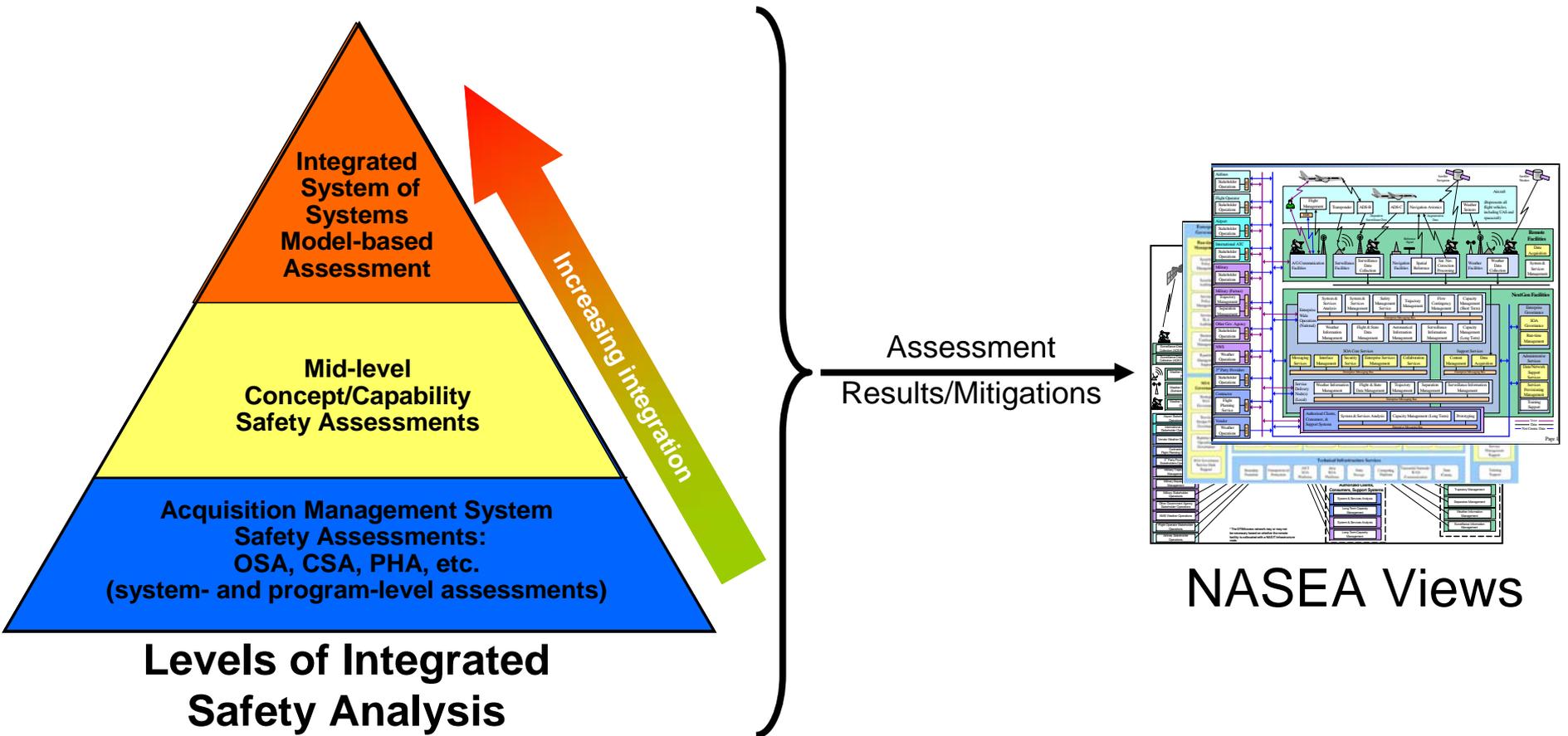


Mitigations Requiring Change in Architecture

Safety Risk Management Process

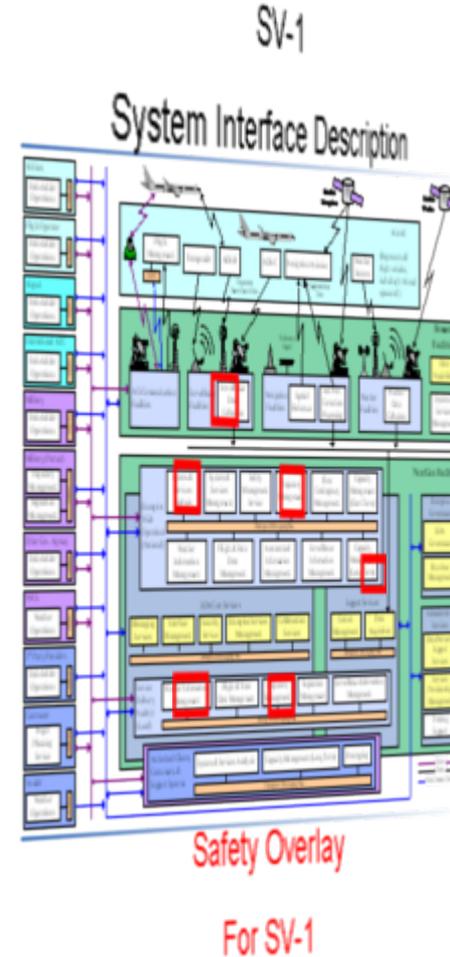


Integrated SRM Supports EA



Safety Overlays

- Safety Overlays are currently in development for:
 - Far-Term SV-1, SV-2, & SV-4
 - Mid-Term SV-1, SV-2, & SV-4
- Safety Overlays highlight pertinent functions, systems, interfaces, etc. that could be a causal factor for catastrophic hazards should failure or degradation be realized.



EA Helps Meet NextGen Safety Objectives Technically via the Safety Overlays

Safety Management and the Use of EA

- **Summary**

- NextGen safety objective → Make the NAS *even more safe* than it already is.
- EA Helps Meet NextGen Safety Objectives via:
 - System View Overlays to highlight areas of safety risk
 - System Views to identify systems that support the SMS
 - Operational Views of how SMS integrates with NAS activities
 - Technical Views that document safety standards
 - System Views/Operational Views that feed the SRM process
 - System Views/Operational Views document SRM mitigations