DOT/FAA/TC-16/53

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Integrated Domain Assessment of Future Systems Concept of Operations

October 2017

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/TC-16/53		

4. Title and Subtitle	5. Report Date
INTEGRATED DOMAIN ASSESSMENT OF FUTURE SYSTEMS CONCEPT OF OPERATIONS	October 2017
	6. Performing Organization Code: ANG-E272

7. Author(s)	8. Performing Organization Report No.
Nathan Girdner and Jennifer Lamont	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Systems Enginuity, Inc. 8665 Sudley Rd #349 Manassas, VA 20110	
	11. Contract or Grant No.: DTFACT-11-D-00010

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Aviation Administration Aviation Safety – Air Traffic Safety Oversight Service Washington, DC 20591	Final Report
	14. Sponsoring Agency Code: AOV-300

15. Supplementary Notes

The FAA William J. Hughes Technical Center Aviation Research Division COR was Dr. Huasheng Li.

16. Abstract

The FAA established the Air Traffic Safety Oversight Service (AOV) to provide independent safety oversight of Air Traffic Organization's (ATO's) provision of air traffic services. To support its mission, AOV initiated a research effort to develop a safety review support tool—Integrated Domain Assessment of Future Systems (IDA-FS)—to assist AOV with the review, evaluation, and approval of controls proposed to mitigate high-risk hazards associated with new/modified National Airspace System (NAS) systems, given the introduction of multiple changes to the NAS. This concept of operations (ConOps) describes AOV user needs for IDA-FS, proposed functional capabilities aligned to AOV needs, and scenarios for user interaction with the tool to accomplish specific objectives when evaluating Safety Risk Management Documents (SRMDs). The ConOps also demonstrates how the tool will enable AOV users to more effectively and efficiently evaluate SRMDs and NAS change impacts by integrating multiple sources of system and safety data into a single platform. Besides AOV's Approval, Acceptance, and Concurrence process, IDA-FS is also expected to support AOV safety oversight activities for audits and safety compliance monitoring. IDA-FS will assist AOV with audit topic planning by identifying systemic hazard causes and critical controls that span multiple systems and facilities. AOV's compliance monitoring activities are also expected to benefit from the IDA-FS tool that identifies potential ATO Safety Management System compliance deficiencies in terms of high-risk single points of failure and systemic lack of control monitoring.

17. Key Words	18. Distribution Statement
AAC, AOV, Risk control, Safety risk, Safety risk management, SMS, SRMD	This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	68	

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AAC	Approval, Acceptance, and Concurrence
ADS-B	Automatic Dependent Surveillance – Broadcast
AIDS	Accident/Incident Data System
AOV	Air Traffic Safety Oversight Service
ASDE-X	Airport Surface Detection Equipment–Model X
ASIAS	Aviation Safety Information Analysis and Sharing System
ASR	Airport Surveillance Radar
ASRS	Aviation Safety Reporting System
ATC	Air traffic control
ATO	Air Traffic Organization
ATQA	Air Traffic Quality Assurance
CARTS	Common Automated Radar Terminal System
CEDAR	Comprehensive Electronic Data Analysis and Reporting
ConOps	Concept of operations
EA	Enterprise architecture
ECP	Engineering Change Proposal
ERAM	En Route Automation Modernization
ESD	Event sequence diagram
FP	Flight plan
GUI	Graphical user interface
HRH	High-risk hazard
HTS	Hazard Tracking System
IDA-FS	Integrated Domain Assessment of Future Systems
IOC	Initial Operating Capability
IOT&E	Independent Operational Test and Evaluation
ISA	Independent Safety Assessment
LT	Local tower
NAS	National Airspace System
NCP	NAS Change Proposal
NextGen	Next Generation Air Transportation System
NMAC	Near mid-air collision
NSIP	NextGen Segment Implementation Plan
OI	Operational Improvement
RD	Requirements document
RET	Request Evaluation Team
REW	Request Evaluation Worksheet
RL	Request Lead
RT	Remote tower
SBS	Surveillance and Broadcast Services
SOS	STARS Operational Site
SMART	Safety Management Action Review Team
SME	Subject matter expert
SMS	Safety Management System
SRM	Safety Risk Management

SRMD	Safety Risk Management Document
SRMDM	Safety Risk Management Decision Memo
SRMP	Safety Risk Management Panel
STARS	Standard Terminal Automation Replacement System
SURF-IA	Airport Surface with Indications and Alerts
TRACON	Terminal Radar Approach Control
UI	User interface

EXECUTIVE SUMMARY

Ensuring the safety of the flying public is the number one priority of the FAA, and managing safety risks is increasingly important during the transition to the Next Generation Air Transportation System (NextGen). Many changes to the National Airspace System (NAS) are expected to take place in the same timeframe, and these changes cumulatively interact to impact the safety of the NAS with both positive and negative safety effects.

The FAA Air Traffic Safety Oversight Service (AOV) is responsible for independent safety oversight of air traffic services provided by the Air Traffic Organization (ATO). In accordance with FAA Order 1100.161 Change 1, AOV reviews ATO Safety Risk Management Documents (SRMDs) and approves or rejects controls that are proposed to mitigate high-risk safety hazards. AOV's Approval, Acceptance, and Concurrence (AAC) Work Instructions define a step-by-step process for AOV's review of SRMDs along with approval and rejection criteria based on ATO Safety Management System (SMS) Manual compliance.

One of the major challenges that AOV faces is that the current ATO Safety Risk Management process focuses on individual changes to the NAS, which means that an SRMD and associated risk controls do not necessarily consider potential interactions with other changes in the NAS. Focusing only on individual changes increases the probability that hazards created by unanticipated consequences of interactions between changes will not be identified before deployment. A tool and process to evaluate potential risks of both individual and multiple, overlapping changes in the context of the dynamic and complex NAS environment are needed.

To support its mission, AOV launched an Integrated Domain Assessment of Future Systems (IDA-FS) research effort to develop a safety review tool to assist AOV with the approval process for risk controls in ATO SRMDs, given the context of multiple NAS changes. The IDA-FS tool will identify interactions and interdependencies among NAS systems and system safety hazards, providing a basis for AOV's evaluation of SRMDs and high-risk hazard (HRH) controls.

This ConOps provides a summary of AOV user needs for IDA-FS and an overview of the IDA-FS system concept and capabilities proposed to meet identified user needs. High-level IDA-FS functions are presented along with the tool's intended operating environment and users. Several use cases are also outlined to illustrate IDA-FS system capabilities and interactions with AOV users. Finally, a case study is discussed to show how these cases can be applied to an actual NAS system and corresponding safety hazard data.

The IDA-FS ConOps provides a foundation for future definition of system requirements for the tool. This document is not intended to describe the technical approach for IDA-FS model or tool implementation details such as user interface design. Instead, this ConOps defines the essential IDA-FS functional capabilities and user scenarios for interacting with the tool. Specific requirements for tool functionality, inputs, and outputs will be developed during the next research phase.

1. INTRODUCTION

1.1 BACKGROUND

The FAA established the Air Traffic Safety Oversight Service (AOV) to provide independent safety oversight of Air Traffic Organization (ATO) air traffic services. FAA Order 1100.161 CHG 1 outlines the manner by which AOV conducts safety oversight, the respective responsibilities of ATO and AOV regarding National Airspace System (NAS) safety, and the requirements and safety standards under which the ATO operates.

AOV oversight techniques include audits, document reviews, and inspections to monitor ATO compliance with safety standards. Safety and operational data is regularly analyzed for hazards, risk mitigation effectiveness, and safety trends. One of AOV's responsibilities defined in the FAA Order 1100.161 CHG 1 is to approve the controls proposed by ATO for mitigating or eliminating initial or current high-risk hazards (HRHs) prior to system implementation. The AOV Approval, Acceptance, and Concurrence (AAC) Request Work Instruction outlines a step-by-step process for AOV safety specialists to review and address the Safety Risk Management Document (SRMD) from request receipt to response [1]. The AAC Request Work Instruction provides guidance for AOV's Request Evaluation Team (RET) to review ATO's SRMDs and to make an approval or rejection recommendation on the controls proposed by ATO for mitigating or eliminating HRHs identified in its SRMDs.

As part of AOV's air traffic safety oversight role described in FAA Order 1100.161, AOV must approve (or reject) controls for initial or current HRHs before the ATO can implement the proposed NAS change. To support its mission, AOV initiated a research effort to develop the Integrated Domain Assessment of Future Systems (IDA-FS) to support evaluation of controls proposed to mitigate HRHs associated with new and modified NAS systems. The tool is intended to assist in identifying safety interactions among multiple changes to the NAS to provide context for AOV's review of HRH controls and ATO SRMDs.

FAA Order JO 1000.37 defines the roles and responsibilities of the ATO with respect to Safety Risk Management (SRM) [2]. The ATO is responsible for implementing SRM for any proposed change to the NAS and any safety risks identified within ATO's span of control. To implement and promote SRM processes in all ATO systems, the ATO developed the Safety Management System (SMS) Manual. The ATO SMS Manual documents the policies that govern ATO safety and provides guidance on the SRM process used to identify, analyze, assess, and treat safety risks.

In accordance with the ATO SMS requirements, proposed NAS changes must be examined for system safety risk. Initial high risk must be mitigated to an acceptable level or eliminated before a change to the NAS is implemented. The ATO SMS Manual describes the methods and activities that must be used to identify and treat safety risks in the NAS. When a change to the NAS is proposed, a Safety Risk Management Panel (SRMP) is convened to identify hazards related to the change. Risks associated with the hazards are analyzed in terms of severity and likelihood [3]. The hazards are then treated by developing controls to mitigate the effects or reduce the likelihood of each hazard. According to the SMS Manual, hazards that are classified as having high risk must be treated to reduce the risk to medium or low.

The ATO prepares SRMDs to describe the safety analysis for a proposed change to the NAS and to document evidence justifying whether the proposed change is acceptable from a safety perspective. The SMS Manual defines who must approve SRMDs and accept the risks identified for the NAS change. All stakeholders involved in implementing the change to the NAS or related safety risk controls must review and sign off on the SRMD, and the residual safety risk must be accepted by the appropriate authority before the change can be implemented.

1.2 PURPOSE

The purpose of the concept of operations (ConOps) is to describe AOV user needs for IDA-FS and provide an overview of the IDA-FS system concept and functional capabilities proposed to meet identified needs. The ConOps also includes a profile of IDA-FS users, the tool's intended operating environment, and scenarios on how IDA-FS can be used by AOV to support SRMD reviews and approval of HRH controls.

1.3 SCOPE

The IDA-FS ConOps document provides a summary of the current needs for the IDA-FS tool, resources that can support or enable the tool, and the high-level functions needed to meet the defined user needs. This ConOps may be used by AOV stakeholders seeking information on IDA-FS functional capabilities and potential operational usage scenarios for the application of IDA-FS. It should be noted that this ConOps describes an initial prototype of the IDA-FS solution. As a result, IDA-FS maintenance and support concepts and system administration/management are not addressed herein. It should also be noted that IDA-FS operational and interface design requirements are not addressed in this ConOps but will be defined during a future research phase.

1.4 PROBLEM STATEMENT

One of the major challenges that AOV faces through the review and approval process is that current ATO SRM process focuses on individual changes to the NAS, which means that an SRMD and associated controls do not necessarily consider potential interactions with other systems and changes in the NAS. In reality, multiple changes to the NAS often take place at the same time and may collectively impact the safety of the NAS either positively or negatively. AOV's current AAC process, which also focuses on individual changes, does not identify hazards created by unanticipated consequences of interactions between projects or NAS changes. As a result, AOV has recognized a need for a methodology and tool to assist in reviewing ATO SRMDs and approving HRH controls with a view toward understanding the potential for overlooked hazards given individual and multiple changes to the NAS. IDA-FS is the safety review tool being developed to meet this need.

1.5 DEFINITIONS

Definitions for the following terms used throughout this report are from FAA Order 1100.161 CHG 1, Air Traffic Safety Oversight:

- Acceptance–The process in which the regulating organization has delegated the authority to the service provider to make changes within the confines of approved standards and only requires the service provider to notify the regulator of those changes within 30 days. Changes made by the service provider in accordance with their delegated authority can be made without prior approval by the regulator.
- Approval–The formal act of approving a change submitted by a requesting organization. This action is required prior to the proposed change being implemented.
- Control–A mitigation that exists or is proposed to prevent or reduce hazard occurrence or to mitigate the effect of a hazard. Examples of a control include design choices, additional systems, procedures, training, and warnings to personnel.
- Hazard–Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.
- HRH–A hazard identified in a safety analysis that has an initial, current, or final risk rating of "High," as defined by the ATO SMS Manual.
- Oversight–To validate the development of a defined system and verify compliance to a predefined set of standards; regulatory supervision.
- Risk–The composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state.
- SRMD–A document prepared by ATO to describe the safety assessment of a change to the NAS. An SRMD is prepared in accordance with the current version of the ATO SMS Manual.
- System safety–The application of technical and managerial skills to the systematic, forward-looking identification and control of hazards throughout the life cycle of a project, program, or activity.

1.6 DOCUMENT STRUCTURE

This document consists of six sections. An overview of the IDA-FS system concept is outlined in the Executive Summary. Anticipated tool benefits to AOV users and safety oversight processes are addressed in section 2. Section 3 provides a background description of AOV activities, resources, safety data sources, and tools used to accomplish AOV's safety oversight tasks. Section 4 provides a summary of AOV needs for IDA-FS based on findings from interviews conducted with AOV inspectors and analysts. Section 5 discusses the operational environment and users for IDA-FS and provides an overview of operational scenarios and IDA-FS functions. Finally, concluding remarks and supplemental notes are included in section 6.

2. IDA-FS BENEFITS TO AOV

Anticipated benefits that IDA-FS provides to AOV include:

- Standardization of SRMD evaluation process
- Automated identification of affected system interfaces
- Accelerated identification and comparison of related safety analyses
- Automated identification of system dependencies
- Improved searching for system anomaly and safety incident data

2.1 STANDARDIZATION OF SRMD EVALUATION PROCESS

IDA-FS uses a model-based approach that will reduce AOV's dependency on individual reviewer's background and experience with particular NAS systems, which will allow AOV analysts to work on a wider variety of SRMD reviews, waiver requests, audits, and other AOV tasks. The cumulative effect of the IDA-FS benefits is expected to be an overall standardization and streamlining of AOV safety review and oversight processes. By organizing data on system and hazard interactions into a single tool and automating system and hazard information searches, AOV analysts will be able to spend more time on investigating and evaluating NAS system interactions and their impact on safety.

2.2 AUTOMATED IDENTIFICATION OF AFFECTED SYSTEM INTERFACES

IDA-FS allows for automated identification of internal and external system interfaces affected by a given NAS change. ATO change proponents identify the systems and subsystems affected by a NAS change and address the scope of the change and supporting hazard analysis in an SRMD. AOV currently relies on its individual subject matter experts' (SMEs') understanding of the systems involved to evaluate the sufficiency of the system description and safety analysis scope. The IDA-FS tool will automate the process of identifying NAS systems affected by a given NAS change. It will also provide supplemental information about system functions and interfaces to AOV analysts. This information will help to standardize the AOV review and evaluation processes and reduce AOV's dependency on a particular reviewer's background knowledge and experience with the system of interest.

2.3 ACCELERATED IDENTIFICATION AND COMPARISON OF RELATED SAFETY ANALYSES

IDA-FS is expected to streamline and simplify the evaluation of hazard causes, a component of AOV's SRMD process. IDA-FS will be able to automatically identify common causes within the hazard analysis for an individual system and across multiple NAS systems. IDA-FS will also automate identification of hazards with a single point of failure, which are of particular safety concern in the review of high risks. In addition, the tool will highlight hazards that do not have any controls or mitigations identified for one or more hazard causes. Currently, AOV must manually inspect for common causes, single points of failure, and other hazard cause issues on an individual SRMD basis. AOV lacks the capability to perform these time-consuming and error-prone tasks on a systemic basis, looking across multiple NAS changes and corresponding SRMDs.

IDA-FS will also accelerate the comparison of hazards and other safety analysis elements from related systems and SRMDs. Current AOV AAC guidance encourages analysts to review historical SRMDs to cross-check an SRMD under review and to generate ideas for potential audit topics. IDA-FS will be able to automatically identify SRMDs of interest to AOV analysts based on the systems and hazards being examined. The tool will permit side-by-side comparisons of safety analysis elements, which can assist reviewers in evaluating oversights and inconsistencies across analyses, as well as evaluating whether a proposed control has been implemented successfully in another system or facility.

2.4 AUTOMATED IDENTIFICATION OF SYSTEM DEPENDENCIES

IDA-FS allows for the automated identification of system dependencies that could impact the availability or effectiveness of hazard controls. AOV currently lacks the capability to identify and track such dependencies and must instead rely on individual knowledge and foresight to detect NAS changes that affect existing controls. In addition to identifying NAS system interactions and interfaces, IDA-FS links existing and recommended controls to NAS systems as part of the IDA-FS model. This will allow AOV users to quickly assess the systems and existing hazards and controls that may be affected by a proposed NAS change.

2.5 IMPROVED SEARCHING FOR SYSTEM ANOMALY AND SAFETY INCIDENT DATA

IDA-FS will assist AOV with pinpointing searches for system anomaly and safety incident data relevant to SRMDs under review. AOV currently uses a variety of data sources for safety and incident data but lacks a standardized process and mechanism for finding anomaly and incident reports directly relevant to specific NAS systems. IDA-FS will streamline searching of multiple data sources for historical system anomalies and related safety incidents data that can be used to cross-check ATO SRMD evidence for assessed risk.

3. SAFETY OVERSIGHT PROCESSES AND RESOURCES

Figure 1 shows an overview of the relationship between IDA-FS and AOV safety oversight processes that will be supported by IDA-FS. The primary focus of IDA-FS functionality is to support the AOV AAC process, particularly SRMD reviews and AOV decisions to approve HRH controls. It is also anticipated that IDA-FS will support other AOV processes, including audit planning and analysis, Safety Management Action Review Team (SMART) activities, and ongoing safety and compliance monitoring. An overview of each process and supporting IDA-FS capabilities is provided in this section.

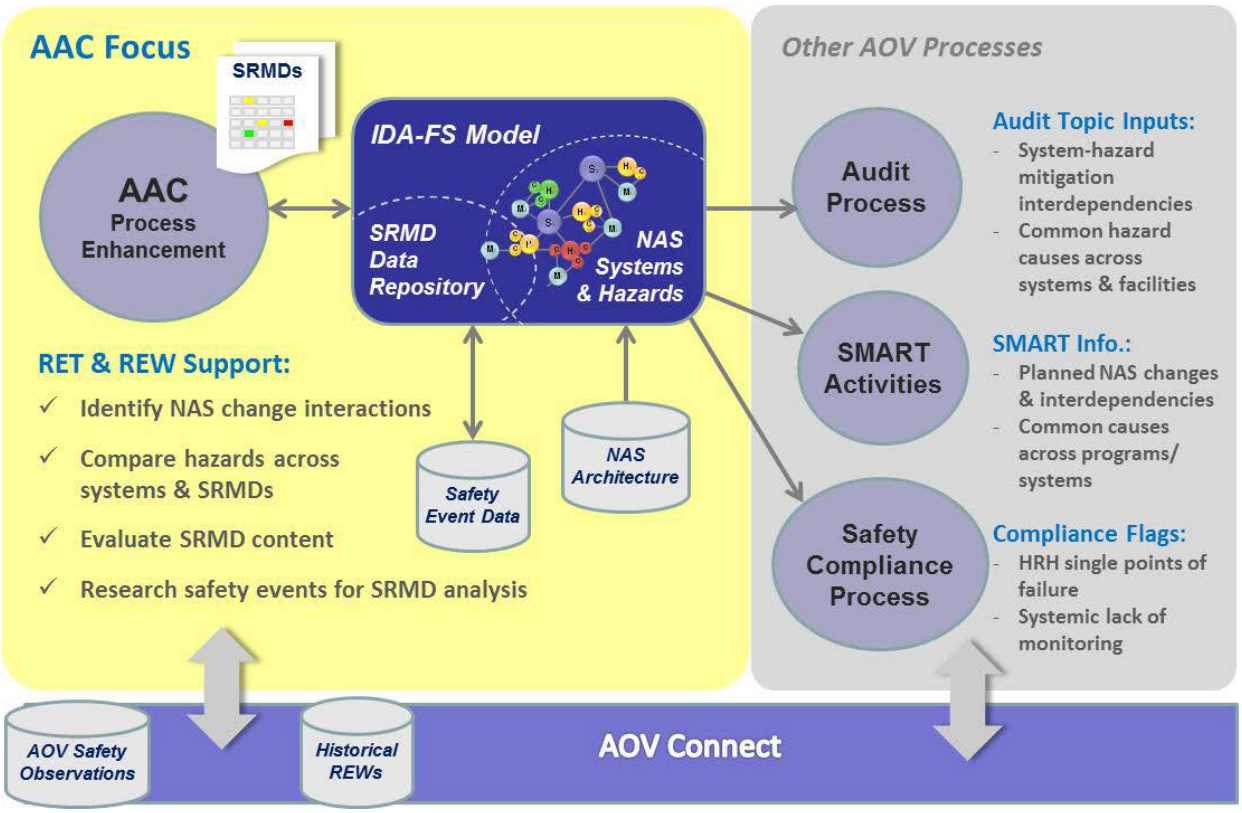

Figure 1. IDA-FS system integration with AOV

3.1 AOV RESPONSIBILITIES

3.1.1 AAC Process

The ATO is required to obtain AOV approval for proposed mitigations for initial HRHs. Approval is primarily based on SRMDs provided by the ATO. AOV's AAC Request Work Instruction describes AOV's responsibilities and workflow for review and feedback to the ATO regarding various ATO packages, such as SRMDs and air traffic control (ATC) procedure waivers.

When AOV receives an SRMD for review, an AOV Request Lead (RL) and a RET are assigned to conduct the SRMD review. Once the RET is convened, the members use the Request Evaluation Worksheet (REW) to structure the SRMD evaluation. The REW is a checklist that helps the RET to objectively evaluate the SRMD and associated hazard controls [4]. Decisions on each REW criterion are primarily based on subject matter expertise of each member of the RET; AOV's planned future enhancements to the REW are expected to include additional guidance on SRMD evaluation criteria and control approval decision making [5].

The primary focus of IDA-FS functionality is to support the AOV AAC process for SRMD reviews and approval of HRH controls. Accordingly, IDA-FS will support RET members in identifying interactions due to NAS changes, comparing hazards across systems, evaluating SRMD content in accordance with the REW, and researching prior safety events to independently cross-check the ATO's safety analysis. The current version of the AOV REW checklist, dated March 31, 2013,

was used as a guide to characterize IDA-FS operational capabilities AOV needs to address REW criteria. Table 1 shows the REW criteria supported by IDA-FS capabilities that will assist with AOV's evaluation of each criterion. IDA-FS capabilities are discussed in detail in section 5.5 of this ConOps.

Table 1. REW criteria and IDA-FS capabilities

REW Criteria	IDA-FS Capabilities
3.1) Has the system for which the change is being proposed been adequately described?	[1] Identify change impacts.
3.2) Was the description of the proposed change sufficiently defined and documented in the SRMD?	[1] Identify change impacts.
	[2] Identify operational interactions.
3.3) Does the SRMP include all impacted stakeholders with relevant experience?	[3] Identify potential stakeholders (based on list of affected systems and facilities).
4.2) Do the identified hazard(s) coincide with RET's or RL's finding(s)?	[1] Identify change impacts.
	[2] Identify operational interactions.
	[4] Identify interfacing systems not addressed in the hazard cause list.
	[5] Compare similar SRMDs and content.
	[10] Investigate prior incidents and effects.
	[11] Capture remarks from reviewers.
	[12] Query remarks.
4.3) Are there any single-point-failure or common-cause failure hazard(s) identified?	[7] Identify hazard cause issues.
5.1) Is there evidence to support the determination of the worst credible outcome of an event (severity)?	[10] Investigate prior incidents and effects.
5.2) Is there quantitative/qualitative evidence to support the determination of likelihood of an event?	[8] Identify inconsistent controls.
	[10] Investigate prior incidents and effects.
	[5] Compare similar SRMDs and content.
5.3) Does the predicted safety risk reflect the adverse impact of a potential hazard(s)?	[5] Compare similar SRMDs and content.
	[2] Identify operational interactions.

Table 1. REW Criteria and IDA-FS Capabilities (continued)

REW Criteria	IDA-FS Capabilities
5.4) Do the identified risk(s) coincide with RET's or RL's finding(s)?	[5] Compare similar SRMDs and content.
	[8] Identify inconsistent controls.
	[10] Investigate prior incidents and effects.
	[11] Capture remarks from reviewers.
	[12] Query remarks.
6.1) Did the SRMP propose appropriate risk mitigation strategies to adequately reduce the risk of the identified hazard(s)?	[7] Identify hazard cause issues.
	[8] Identify inconsistent controls.
	[5] Compare similar SRMDs and content.
	[10] Investigate prior incidents and effects.
6.2) Do the identified mitigation(s) coincide with RET's or RL's finding(s)?	[5] Compare similar SRMDs and content.
	[8] Identify inconsistent controls.
	[10] Investigate prior incidents and effects.
	[11] Capture remarks from reviewers.
	[12] Query remarks.
7.2) Has the program office provided an adequate continuous monitoring plan and hazard tracking method for the identified hazard(s)?	[9] Compare monitoring plan to similar SRMDs.
	[11] Capture remarks from reviewers.
	[12] Query remarks.
8.2) Summarize the RET findings	[14] Generate a report of relevant IDA-FS data.
8.3) Summarize feedback/lessons learned	[14] Generate a report of relevant IDA-FS data.

3.1.2 AOV Audits

As part of its safety oversight mission, AOV audits the safety of air traffic services provided by the ATO. These audits are used to monitor ATO compliance with safety standards and the SMS. Potential audit topics are developed based on data analysis and safety risk assessments to turn suggested topics into actionable audits. Once the audit topics are approved by the AOV Management Team, a team is selected to further develop and conduct the audit. AOV's Audit Process Work Instruction (AOV-002-W2) provides guidance to AOV analysts in developing a potential audit topic into an actionable audit.

IDA-FS will support AOV audit planning and execution by helping analysts identify interdependencies between systems and hazards and common hazard causes identified across systems/facilities. AOV analysts can use the IDA-FS functions to identify systems that may be vulnerable to certain hazards or to identify hazard causes that may impact multiple systems or facilities. Analysts may also use IDA-FS to identify potential audit topics by querying AOV remarks on topics or areas of safety concern attributed to IDA-FS model elements (e.g., NAS systems and safety hazards) and prior AOV SRMD reviews.

3.1.3 AOV SMART Teams

AOV established SMART to monitor Next Generation Air Transportation System (NextGen) initiatives and facilitate collaborative communications with ATO to research AOV's questions and concerns regarding SRMDs. There are five SMART teams led by AOV-330: navigation, surveillance, weather and facility, automation, and communications teams. Each team has a contact in the ATO and engages with both the ATO Office of Safety and the program office (or change proponent) responsible for SRM. The SMART meets bi-weekly and sets up technical interchange sessions with ATO programs or NextGen portfolio managers to obtain information on planned NAS changes in advance of ATO SRMD submittals to AOV.

AOV SMART teams will be able to use IDA-FS to search for data related to planned NAS changes and their interdependencies with current NAS systems. Common causes across programs/systems can also be identified for SMART follow-up action with the ATO.

3.1.4 Safety Compliance Monitoring

IDA-FS will support investigation of ATO SMS compliance issues, such as single points of failure in HRHs and shortfalls in hazard and control monitoring. IDA-FS will notify AOV of potential SMS compliance issues based on user-defined notification criteria. Whenever the IDA-FS model is updated with new or modified NAS architecture or safety hazard data, the tool will analyze the model for potential SMS compliance issues, such as HRH single-point failures and common causes.

3.2 AOV SAFETY RESOURCES AND TOOLS

AOV maintains various databases and websites to support its safety oversight activities related to SRMD reviews. AOV maintains an AAC tracker to record meetings, discussions, emails, and phone conversations with personnel in AOV, ATO, or other organizations. AOV also maintains a correspondence tracker to process and coordinate draft AOV memos, including an AOV-internal recommendation memo from the RET regarding HRH control approval (or rejection) and AOV approval memos to the ATO. AOV also retains a record of all ATO SRMDs and Safety Risk Management Decision Memos (SRMDMs) received in the correspondence tracker. Finally, AOV maintains checklists for AAC process activities and templates for RET recommendation and AOV approval memos on a SharePoint website.

AOV is implementing a Web-based knowledge management infrastructure called AOV Connect. AOV Connect will record, track, and link AAC and other data for safety compliance, correspondence, Safety Management Reviews, and audits among other safety oversight activities [6]. AOV plans to use AOV Connect to capture a subset of ATO safety hazard information, including hazard ID or reference number, hazard title, initial and residual risk ratings, and associated waiver or acquisition portfolio(s). AOV Connect will also provide sorting/searching capabilities for keywords, issues of interest, and Resource Allocation Valuation scores, among other data attributes. AOV Connect, which will be used AOV-wide, is also intended to record, prioritize, and track AOV observations on a variety of topics including safety hazards and controls. The AOV Connect tool is undergoing a phased implementation that will incrementally add

functionality based on feedback from AOV users and refinements to AOV safety oversight processes.

IDA-FS may be able to use hazard and other data from AOV Connect once that platform is fully implemented. However, IDA-FS should not be dependent on AOV Connect to function. IDA-FS may also provide a means of sharing data (e.g., exporting) with AOV Connect and other AOV platforms such as SharePoint. Potential IDA-FS interface requirements will be defined in a future research phase once AOV Connect is fully integrated into the AOV workflow and hazard data is available.

3.3 OTHER RESOURCES AND TOOLS

AOV uses a number of external data resources to support SRMD reviews. Section 3.3.1 summarizes data resources AOV indicated were most frequently used to support SRMD evaluations. Section 3.3.2 addresses additional NAS data and information resources that may be used to support the IDA-FS model or tool capabilities.

3.3.1 Aviation Safety Data Resources

3.3.1.1 ATO Hazard Tracking Databases

AOV coordinates with the ATO to obtain hazard data, SRMDs, and safety event data as needed to support SRMD reviews. Per FAA Order 1100.161 CHG 1 and the ATO SMS Manual, the ATO has a requirement to maintain a database for tracking identified hazards. ATO-wide implementation of such a database is ongoing. Previously, the ATO had implemented a Web-based Hazard Tracking System (HTS) for system acquisitions and operational changes to the NAS. Certain ATO acquisition programs and ATC facilities with ATC procedure waivers used the HTS between 2005 and 2011. However, HTS was not used ATO-wide for all hazard tracking activities. Currently, there is no ATO-wide database of hazard and mitigation monitoring data. ATO programs and facilities may maintain individual databases or other means of tracking hazards and mitigations in compliance with the SMS.

3.3.1.2 FAA Independent Safety Assessment Reports

AOV receives Independent Operational Test and Evaluation (IOT&E) or Independent Safety Assessment (ISA) documentation and feedback on new system acquisitions. IOT&E or ISA reports are prepared to identify safety concerns, operational problems, and technical documentation deficiencies associated with new systems before those systems are authorized for in-service operational use. AOV reviews these reports to cross-check the hazards and safety risk assessments presented in ATO SRMDs prior to a system In-Service Decision.

3.3.1.3 Aviation Safety Event Databases

The ATO has databases that AOV analysts periodically use to cross-check assumptions and data presented in ATO safety analyses. Though AOV's access to ATO's databases is limited, AOV can request specific database reports from the ATO as needed. Until 2012, the ATO maintained the Air Traffic Quality Assurance (ATQA) database on safety events involving air traffic operational errors and deviations, near mid-air collisions (NMACs), pilot deviations, vehicle/pedestrian

deviations, and runway incursions, among other events. Though the ATO has discontinued ATQA, AOV may still consult ATQA to review historical safety events. In 2011, the ATO established the Comprehensive Electronic Data Analysis and Reporting (CEDAR) database. CEDAR maintains occurrence reports involving air traffic services; example mandatory occurrence reports include airborne losses of separation, airport surface losses of separation, and airborne ATC anomalies (airspace/altitude/route/speed) not involving losses of separation.

The FAA and other government agencies maintain databases that may be of use to AOV safety analysts in reviewing SRMDs. These resources are used by AOV when researching similar systems and historical incidents related to hazards identified in SRMDs under review:

- FAA and National Transportation Safety Board Accident/Incident Data System (AIDS)–AIDS contains data records for general aviation and commercial air carrier incidents since 1978.
- FAA Aviation Safety Information Analysis and Sharing System (ASIAS)–ASIAS allows users to perform queries across multiple databases on aviation accidents, incidents, and pilot reports of NMACs.
- NASA Aviation Safety Reporting System (ASRS)–ASRS contains voluntary reports on safety incidents and concerns identified primarily by flight crews, though air traffic controllers may also voluntarily report ATC-related safety events.

The IDA-FS tool is expected to interact with external databases to query and assemble data relevant for SRMD reviews. Specific databases and interface details will be defined later in the IDA-FS development process.

3.3.2 NAS System Architecture Resources

Background information on NAS systems is needed to establish the IDA-FS model and support AOV's review of SRMDs related to NAS changes. To ensure the IDA-FS model is up-to-date with the NAS architecture, information on NAS systems, subsystems, interfaces, and planned changes is required. The NAS enterprise architecture (EA), FAA configuration management data, and NextGen plans are potential resources for obtaining information on legacy NAS systems and planned NAS changes.

3.3.2.1 FAA NAS EA

The purpose of the NAS EA is to establish a foundation from which evolution of the NAS can be explicitly understood and modeled. To that end, the NAS EA program maintains information about the current state of the NAS from a system perspective. The NAS EA website provides NAS architecture diagrams, requirements documents (RDs), and service roadmaps. The primary focus is on the current state of the entire NAS, including legacy systems, with roadmaps showing pending system acquisitions and updates as part of the NextGen effort.

NAS architecture diagrams show system interconnections throughout the NAS and are specified at either a NAS-wide level (i.e., enterprise-level) or a program-level. The NAS-RD provides the functional and performance requirements for FAA systems that provide ATC services. The NAS-RD, which is updated annually to capture changes to the operational NAS, ensures that all

operational system capabilities are traceable to requirements. Mid-term and far-term versions of the NAS-RD are used to document preplanned functional improvements to the NAS. Finally, NAS Service Roadmaps outline the strategic activities for sustaining and improving NAS operations and implementing NextGen. These Service Roadmaps are updated periodically as research and analyses more clearly define the evolution of NAS services.

The information developed and provided by NAS EA may be of use to IDA-FS in accurately modeling system interactions, current requirements, and planned changes.

3.3.2.2 FAA NAS Configuration Management Data

FAA Order 1800.66, Configuration Management Policy, requires that changes to the NAS EA undergo a NAS Change Proposal (NCP) process. An NCP form is used to document the change, impacted ATC facilities, and impacted system interfaces among other information of potential use for IDA-FS. Related FAA Notice JO 1800.146 requires that all NCPs be accompanied by an SRMD or SRM decision memo. The ATO maintains the WebCM database portal as part of its process of change and configuration management. The NCP forms and supporting documentation, including SRMDs or SRMDMs, are accessible via the WebCM portal. The WebCM portal is primarily intended for NAS change proponents and NCP reviewers to manage NCPs. It therefore has limited searching and filtering capabilities to locate particular SRMDs or proposed system changes.

3.3.2.3 FAA NAS Documentation

The FAA maintains online directories of technical data on a number of NAS systems. The NAS Documentation Services Digital Library, managed by AJW-172, contains system documentation including maintenance handbooks, technical manuals, user instructions, and SRMDs for a variety of NAS systems including automation, communications, surveillance, and weather systems. This digital library is available to FAA employees and may be useful in obtaining additional information about systems and interfaces being changed.

3.3.2.4 FAA NextGen Segment Implementation Plan

The FAA's NAS EA defines goals in a set of Operational Improvements (OIs) planned through 2025, and the NextGen Segment Implementation Plan (NSIP) describes in detail the changes expected to be implemented between 2010 and 2015. The NSIP also provides a high-level overview of post-2015 changes based on the NAS EA. The NSIP and the NAS EA serve as the primary basis for identification of planned NAS changes, their implementation timelines, and the FAA office accountable for implementation of each OI increment. The information provided in the NSIP may be a source of useful information in investigating the interaction between a given NAS change documented in an SRMD and future changes planned as part of the NextGen initiative.

4. AOV NEEDS ANALYSIS

An analysis of AOV needs for IDA-FS was conducted in March 2013. The analysis included research on AOV policies and procedures for SRMD review, control AAC, and AOV headquarters

and service area roles in the SRMD evaluation process. The IDA-FS Needs Analysis Report summarizes the results of the research and AOV interviews to identify observed shortfalls in legacy processes and tools AOV uses for SRMD reviews and control approval decisions [7].

4.1 LIMITATIONS OF CURRENT PROCESSES

The AOV needs analysis identified nine key shortfalls in AOV AAC processes and tools. Upon further input and direction from AOV management, functions to address five of the identified shortfalls were allocated to the IDA-FS tool. Remaining shortfalls are to be addressed by other AOV initiatives, including AOV Connect and AOV's AAC–Process Enhancement.

Table 2 summarizes the identified the AOV shortfalls that are addressed (in whole or in part) by IDA-FS.

Table 2. Capability shortfall allocation matrix

Capability Shortfall	IDA-FS	AAC–Process Enhancement	AOV Connect
1) The lack of a standardized methodology and toolset for AOV to perform SRMD review and approval in a consistent manner across the organization	X	X	X
2) The lack of AOV guidance in information searching and assembling	X		X
3) The lack of methodology and tools to identify the interactions between multiple changes to the NAS	X		
4) The lack of Web-based tool to support AAC process	X		X
5) The lack of well-defined criteria to assist AOV in HRH control effectiveness	X	X	

4.2 FINDINGS ON IDA-FS NEEDS

AOV AAC shortfalls allocated to the IDA-FS solution were used to derive functional needs for the tool within the scope of the IDA-FS mission. Preliminary functional needs for IDA-FS are as follows:

- Identify NAS system equipment and facilities impacted by the change to the NAS in the SRMD under review.
- Identify potential interactions of proposed changes in an SRMD with other changes in the NAS.
- Help analysts to confirm that the identified hazard list is complete for the change to the NAS.
- Help analysts to confirm that all potential hazard causes were identified.
- Help AOV evaluate whether the SRMD has sufficient information to substantiate the assessed risk.
- Confirm that objective evidence is provided for initial/current risk assessment.
- Assess the objective evidence provided for predicted residual risk assessment (depending on implementation phase).
- Provide query capabilities on hazard/mitigation data to check how hazards and controls are addressed in other systems or at different facilities.
- Assist AOV with evaluating the effectiveness of proposed controls.
- Cross-check that all proposed controls are addressed in the hazard tracking and monitoring plan.

This preliminary list of IDA-FS functional needs are translated to tool functional capabilities in section 5.2 of this document.

5. IDA-FS CONOPS

5.1 MISSION

The overall mission for the IDA-FS tool is to support AOV's decision process for approving HRH controls in ATO SRMDs in the context of multiple NAS changes. To meet this mission, AOV has outlined the following key objectives for the IDA-FS tool:

- Organize information on NAS systems and the changes to the NAS.
- Identify qualitatively the interactions between multiple changes to the NAS.
- Support the evaluation of SRMD content and compliance with approved SMS processes.
- Support AOV's assessment of controls proposed to mitigate HRHs.

IDA-FS draws upon data on NAS systems, system interfaces, system interactions, and system safety data to develop a model of system and safety interactions in the NAS. IDA-FS will support AOV users in their review of SRMDs and evaluation of proposed controls. IDA-FS will also provide supporting data regarding related systems, similar safety analyses and results, and prior safety incidents related to the system or hazards under investigation. IDA-FS enables AOV users

to more effectively and efficiently evaluate SRMDs and NAS change impacts by integrating multiple sources of system and safety data into a single platform.

5.2 FUNCTIONAL OVERVIEW

Figure 2 shows an overview of the IDA-FS system. To support AOV's review of ATO SRMDs, IDA-FS performs four primary tasks with the support of IDA-FS model:

1. Identify affected NAS elements–This task analyzes the interactions among the NAS systems using the IDA-FS model and identifies NAS elements affected by NAS changes. NAS elements include systems, facilities, and system safety hazards. Those NAS elements impacted by one or more NAS changes may be potential safety concern areas requiring AOV attention during SRMD reviews or other AOV safety oversight activities.
2. Evaluate hazards in SRMDs–This task helps AOV analysts to evaluate hazard lists and hazard causes for completeness, cross-checks assessed risk against safety event frequencies and effects, and ensures that the hazard identification and risk analysis in SRMDs is in compliance with ATO SMS process.
3. Evaluate effectiveness of controls–This task supports the evaluation of the effectiveness of the proposed controls in an SRMD to ensure that the controls address the intended hazard/cause and that they will reduce the risk as indicated in the SRMD. This task also helps ensure that proposed controls are adequately addressed in the monitoring plan in an SRMD.
4. Maintain SRMD and NAS data–This task allows AOV to update and refine the underlying IDA-FS model in response to NAS changes. NAS systems, subsystems, and internal and external interfaces must be updated as the NAS architecture changes. Similarly, those hazards, causes, and controls attributed to one or more NAS systems must also be updated whenever new SRMDs are produced.

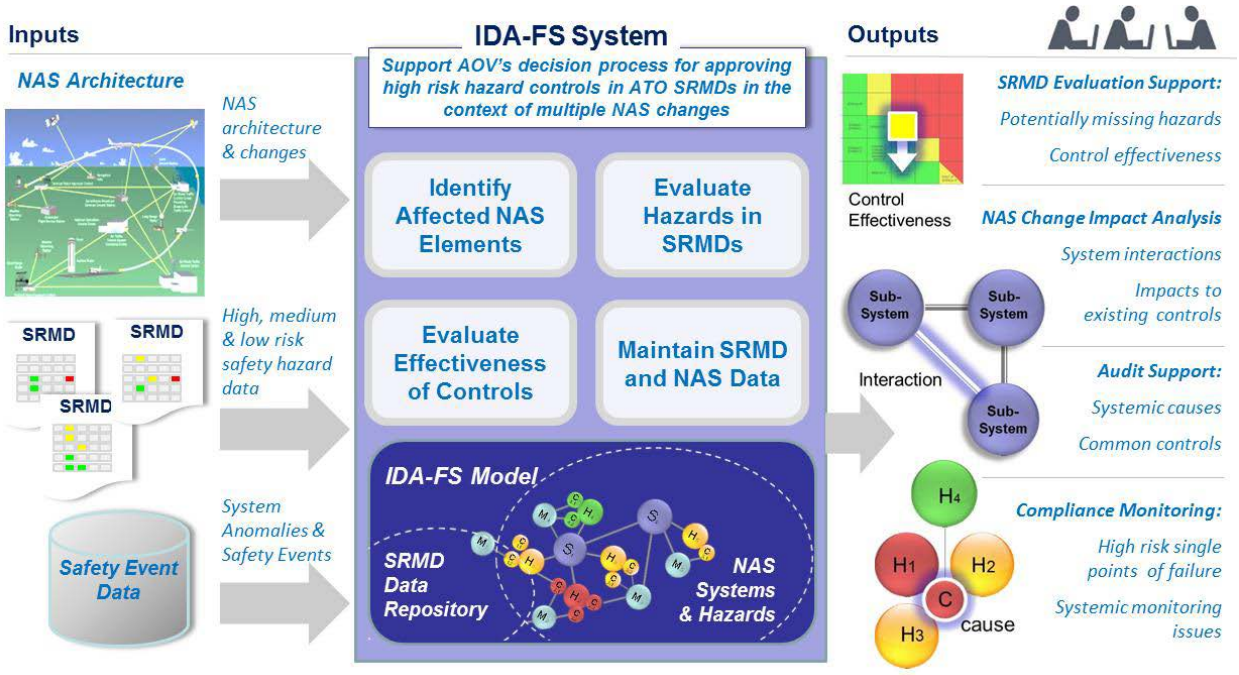

Figure 2. IDA-FS concept overview

5.3 USERS

As discussed in section 3.1, IDA-FS supports AOV's AAC process for SRMD reviews and certain AOV audit, SMART, and compliance-monitoring activities. AOV RET members, including headquarters analysts and engineers and service area air traffic safety inspectors, will interact with IDA-FS to identify the impacts of proposed NAS changes on other systems and hazards and evaluate the adequacy of SRMD content. AOV's evaluation of SRMD content includes reviewing the SRMD for compliance with SMS processes and independently checking for hazard list completeness and evaluating the controls proposed to mitigate HRHs.

AOV audit team members may also interact with IDA-FS to identify potential audit topics. For example, audit team members may use IDA-FS to identify interdependencies between systems and hazards and common hazard causes identified across systems/facilities.

AOV personnel engaged in compliance monitoring may interact with IDA-FS to identify certain ATO SMS Manual compliance deficiencies by ATO program, system, and/or facility. For example, AOV may use IDA-FS to identify high-risk single points of failure or common causes, which may indicate a system vulnerability or deficiency in hazard controls.

Finally, AOV SMART team members who monitor ATO program implementation issues may also interact with IDA-FS to support their oversight activities. For example, SMART teams may use IDA-FS to search for planned changes to the NAS architecture and their interdependencies with current NAS systems to coordinate with the ATO.

5.4 MODEL BACKGROUND

The IDA-FS model is the foundation of the tool. The IDA-FS model is established by linking the physical NAS architecture (e.g., surveillance systems, automation, and communications equipment) with safety hazard and control information. Each NAS system in the model is characterized in terms of its direct and indirect interfaces with other systems. NAS systems are associated with hazard information identified in SRMDs. This model of system and hazard interrelationships will permit IDA-FS to identify interactions between systems and hazards, given the proposed and implemented NAS changes.

Figure 3 shows a concept diagram of the notional IDA-FS NAS model. Systems and system interfaces are modeled in accordance with NAS EA data on system interactions. Each system is then linked to hazards, causes, and mitigations (or controls). The model can be queried and analyzed by IDA-FS to support AOV safety oversight tasks.

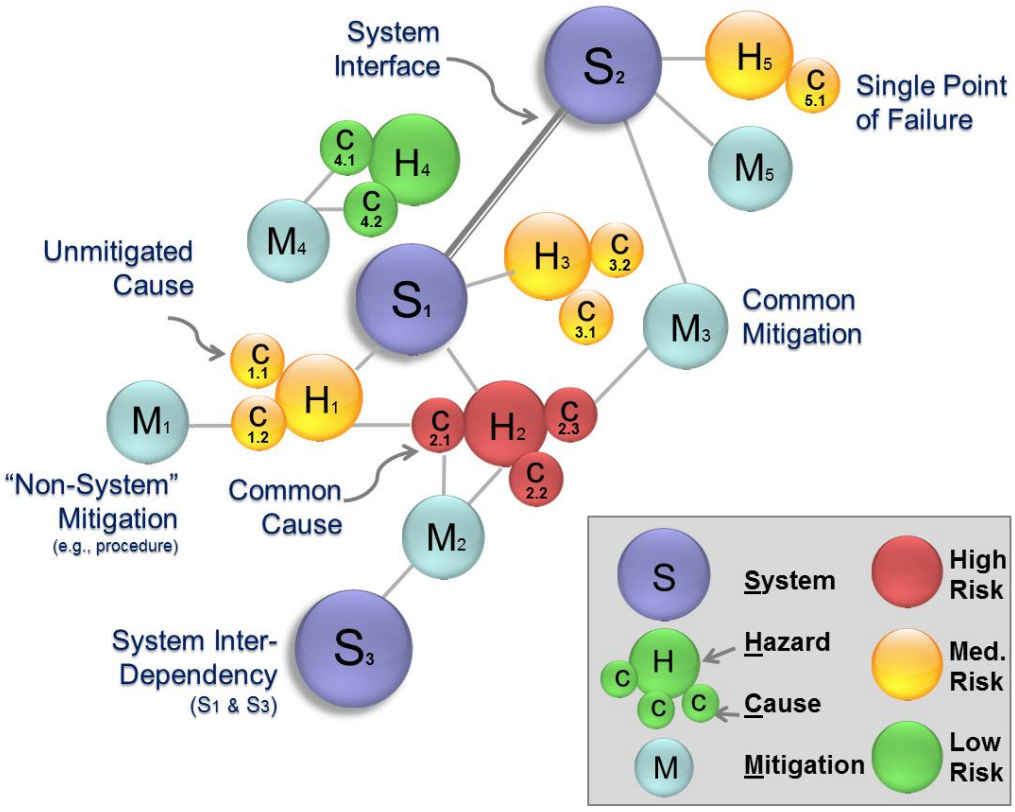

Figure 3. IDA-FS notional model

5.5 OPERATIONAL FLOW

The IDA-FS model must be updated with new and modified SRMD data over time to remain effective in assisting AOV with safety oversight actions, including SRMD evaluations. As NAS changes are proposed and implemented, the IDA-FS model must be updated accordingly. AOV obtains NAS change information through three primary mechanisms:

1. AAC requests–AOV receives SRMDs from the ATO based on AAC requests. This includes SRMDs with HRHs corresponding to a proposed NAS change as part of existing 1100.161 provisions. AOV also receives SRMDs with controls spanning multiple lines of business along with the corresponding proposed NAS change.
2. WebCM/NCPs–AOV will need to monitor the FAA's NAS configuration management data (currently maintained via WebCM) for proposed and implemented NAS changes and corresponding SRMDs and SRMDMs. This represents a change to AOV's existing practices by formalizing and institutionalizing a process for obtaining NCPs and accompanying SRMD/DMs.
3. NAS technical documents–AOV will need to monitor NAS technical documentation resources (i.e., the Logistics Center NAS Digital Library, the FAA NAS EA architecture diagrams, and NAS EA service roadmaps) for NAS architecture details and SRMD information. This also represents a new practice for AOV.

Because AOV will obtain NAS change information at various stages of pre-, on-going, and post-implementation, IDA-FS needs to provide a capability for classifying NAS changes over time. Accordingly, IDA-FS provides a mechanism for AOV to capture "pending" NAS changes (i.e., those new systems and system modifications that are proposed but not yet physically implemented in the NAS). The purpose of this capability is to enable the analysis and identification of impacts on proposed changes to other NAS systems and interrelated safety hazard data to support AOV's evaluation of ATO SRMDs. When proposed NAS changes are finally implemented, pending NAS changes in the IDA-FS model are also updated to reflect the "as-is" implementation and propagated as "implemented" changes in the tool.

AOV analysts will also interact with IDA-FS to evaluate SRMD-specific content. In particular, IDA-FS will support AOV review of ATO SRMDs as part of its AAC process. Analysts will use IDA-FS to find system and hazard data to assist with REW criteria evaluation. Each REW step focuses on a different aspect of the SRMD, including system description and scope, hazard identification, hazard cause identification, risk analysis (severity and likelihood), proposed hazard controls, and hazard monitoring plans. Figure 4 shows the process for using IDA-FS to assist with SRMD reviews.

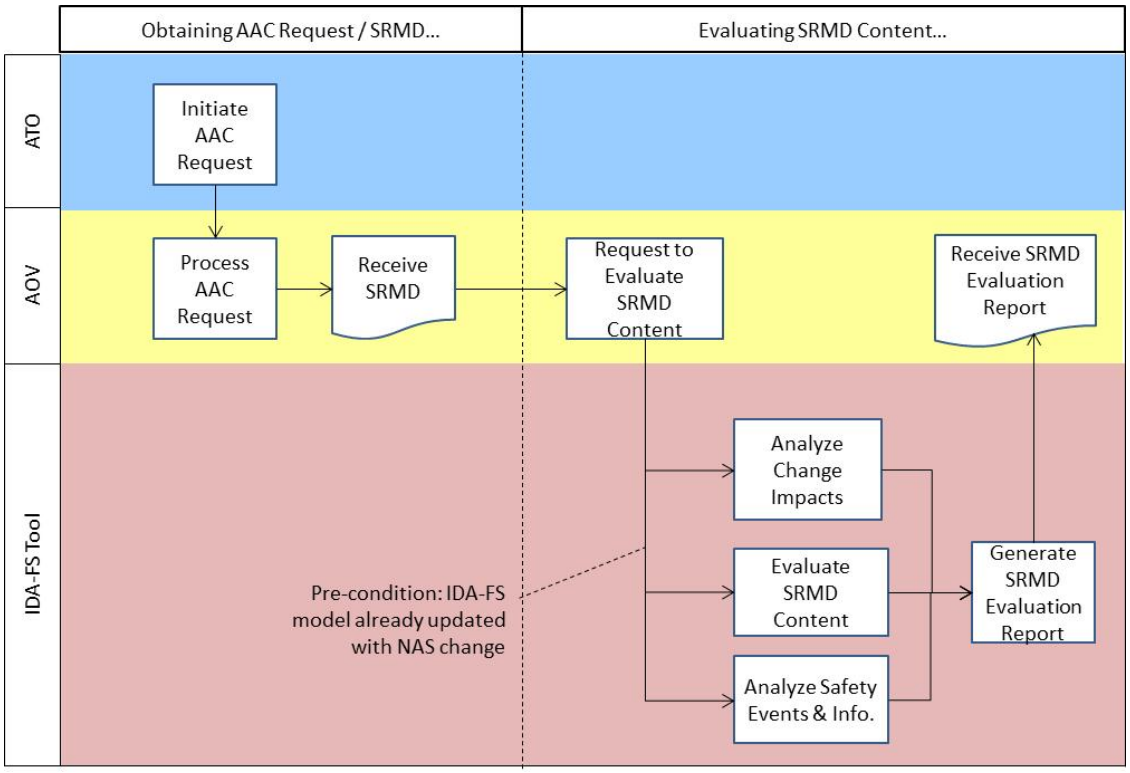

Figure 4. AAC process support swim lane

In addition to AOV review of a particular SRMD, IDA-FS also identifies and notifies AOV of NAS change impacts whenever the IDA-FS model is updated. As NAS architecture information or SRMD data is updated in the IDA-FS model, the tool may be configured to automatically analyze the change for impacts to other NAS systems and interrelated safety hazard data, causes, controls, and monitoring parameters. Based on the NAS change impacts, IDA-FS generates reports and notifications for AOV users. This process identifies potential areas of safety concern for AOV oversight attention regardless of whether or not AOV is conducting an SRMD review. For example, an AOV analyst may set up a notification to be generated whenever systems linked to control effectiveness are modified or whenever the frequency of reported system anomalies exceeds the predicted residual risk likelihood for a given hazard safety. Figure 5 shows the process for updating the IDA-FS model and generating appropriate notifications outside of the AAC process.

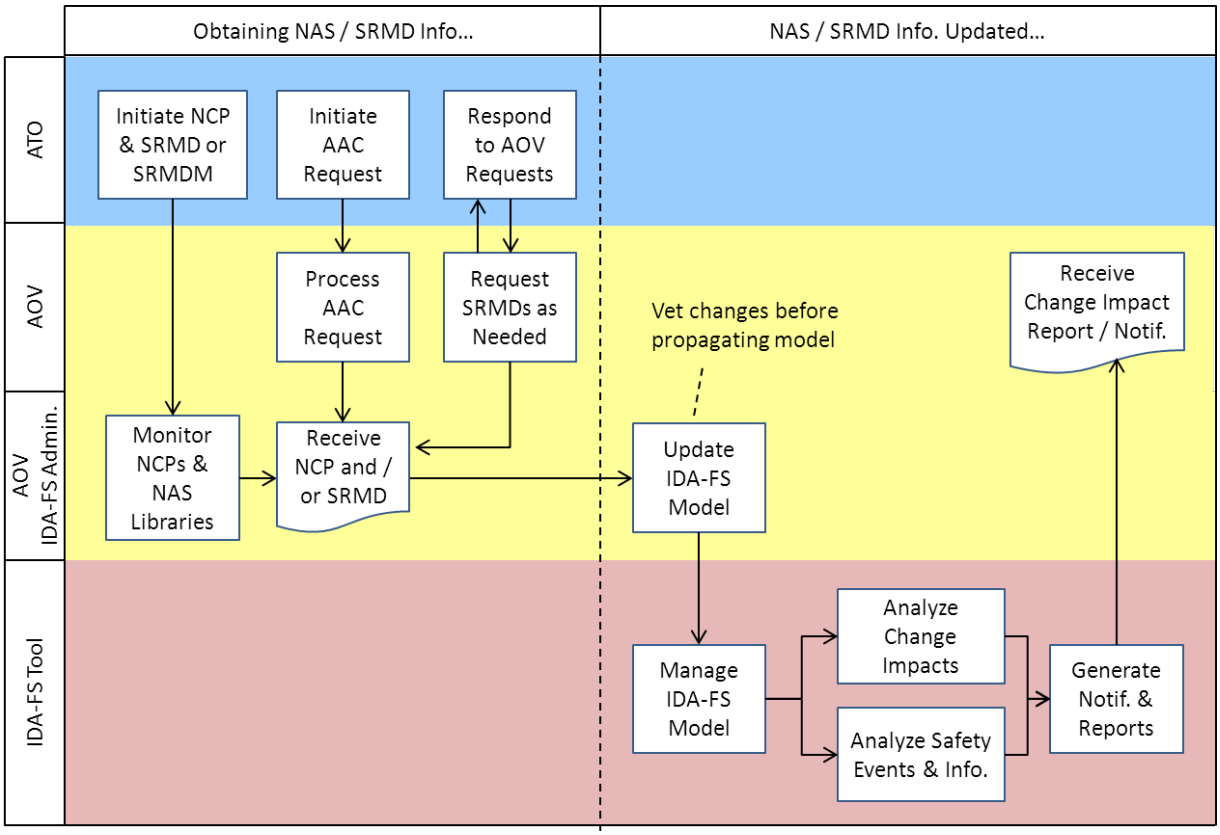

Figure 5. NAS model update swim lane

It should be noted that IDA-FS is a safety review support tool and not a decision-making tool. IDA-FS will support the AOV user by providing data and information on systems and relationships between hazards and systems. AOV will still be responsible for evaluating that data and information to confirm ATO safety analysis deficiencies and the criticality of those deficiencies in AOV's decision to approve or disapprove AAC requests.

5.6 OPERATIONAL ENVIRONMENT

Two specific operational needs were identified during the AOV needs analysis related to the operational environment for IDA-FS:

1. IDA-FS should support multiple and concurrent AOV users.
2. IDA-FS should provide a platform that can be accessed by remotely distributed users.

Based on these constraints, IDA-FS will be a Web-based software tool. It will be accessible to AOV users in the FAA headquarters and service areas. The tool will provide a secure environment for AOV users to investigate system and hazard interactions to support SRMD review and other safety oversight activities. IDA-FS is expected to be deployed on the FAA Intranet and will be subject to FAA information systems management policies. It will not be publically accessible, but access should be possible for authorized users on the FAA internal network.

IDA-FS is envisioned as a standalone software tool, meaning its operation is not directly dependent on any other AOV or FAA software/systems other than network and server systems. However, IDA-FS will contain data collected from external data sources and manual data inputs from AOV users. IDA-FS may also interface with AOV Web portals/knowledge management tools such as (but not limited to) AOV Connect.

5.7 USERS

The two types of IDA-FS users can be generally classified as Analysts and Administrators. Figure 6 shows the primary functions that each user class is expected to interact with.

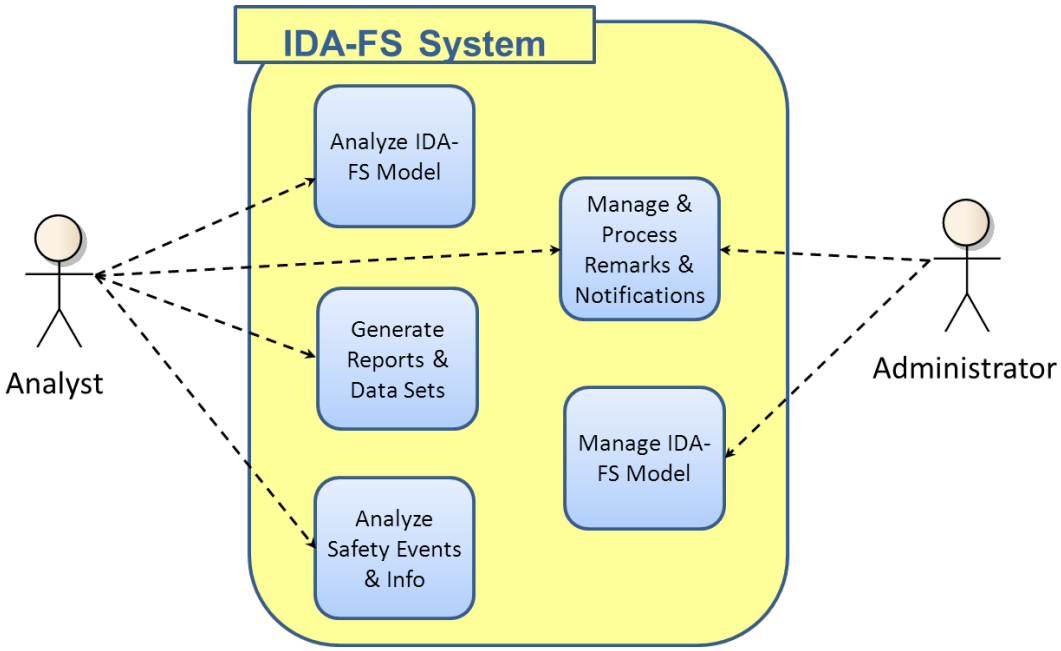

Figure 6. IDA-FS user class interactions

Analysts are primarily concerned with using IDA-FS to support their safety oversight role. They will use the functions related to identifying impacted NAS elements and evaluating SRMD content, as well as search, query, import, and export functions in IDA-FS. The majority of IDA-FS users are expected to be Analysts, including AOV RET members, primary maintenance inspectors, primary operations inspectors, operations research analysts, and service area and headquarters managers and analysts.

IDA-FS Administrators are primarily concerned with ensuring that IDA-FS is operating correctly and that the underlying IDA-FS model is up-to-date. IDA-FS Administrators may include IT specialists who ensure that the software is available via the FAA network and manage user access and privileges. Administrators may also include system safety specialists or SMEs who input/edit SRMD and NAS Architecture data.

Specific user roles and privileges will be defined along with the IDA-FS user interface (UI) requirements in future phases of IDA-FS development.

5.8 IDA-FS FUNCTIONS

The preliminary functional needs for IDA-FS described in section 4.2 were decomposed into tool functional capabilities. IDA-FS functional capabilities are organized into a functional hierarchy as shown in Figure 7. Sections 5.8.1–5.8.6 describe each first-tier and second-tier function.

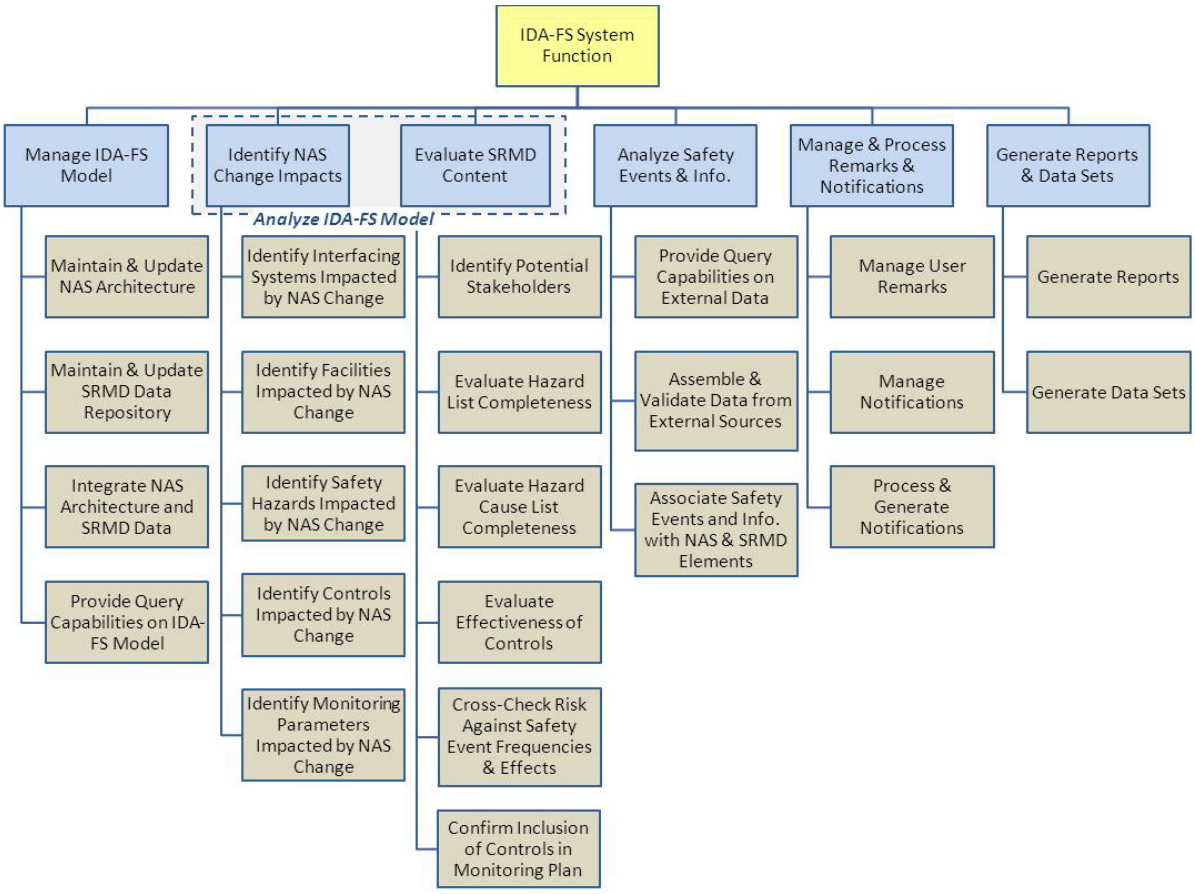

Figure 7. IDA-FS functional hierarchy

5.8.1 Manage IDA-FS Model

The first high-level function (i.e., Manage IDA-FS model) consists of sub-functions that will allow the AOV user to update the NAS architecture and safety hazard data elements of the IDA-FS model. The IDA-FS model establishes interdependencies among NAS systems, SRMDs, hazards, causes, and mitigations. Other IDA-FS functions (i.e., Identify NAS Change Impacts and Evaluate SRMD Content) rely upon the IDA-FS model to be accurate and up-to-date. The sub-functions of the Manage IDA-FS model function allow for the input, editing, and storage of NAS and SRMD data and the integration of that data into the IDA-FS model.

The second-tier functions that comprise this functional block are as follows:

- Maintain and Update NAS Architecture–This function manages changes to the NAS architecture data and provides mechanisms for users to confirm that systems, interfaces, and interactions are accurately captured in the IDA-FS model.
- Maintain and Update SRMD Data Repository–This function ensures that the SRMD data, including hazards, causes, risk ratings, and mitigations, are captured in the IDA-FS model.
- Integrate NAS Architecture and SRMD Data–This function manages the connections between NAS system data and ATO SRMD data.
- Provide Query Capabilities on IDA-FS Model–This function enables querying and sorting data from the IDA-FS model to support other IDA-FS functions.

5.8.2 Analyze IDA-FS Model

The second high-level functional block (i.e., Analyze IDA-FS model) consists of two sub-functions: Identify NAS Change Impacts and Evaluate SRMD Content.

The function (i.e., Identify NAS Change Impacts) examines NAS changes for potential impacts from and to other NAS systems. This set of functions may be used to evaluate the completeness of a safety analysis or to study system interactions in greater detail. The second-tier functions that comprise this functional block are as follows:

- Identify Interfacing Systems Impacted by NAS Change–This function identifies systems that directly interface with a given system of interest or NAS change and provides details about the interface and the systems.
- Identify Facilities Impacted by NAS Change–This function identifies air traffic facilities and service delivery points (e.g., ATC, flight crew, Tech Ops) that directly interface with a given system of interest or NAS change and provides details about the facilities and the systems used there.
- Identify Safety Hazards Impacted by NAS Change–This function allows for the identification of existing hazards that may be impacted (positively or negatively) by a given change to the NAS.
- Identify Controls Impacted by NAS Change–This function allows for the identification of existing or recommended controls that may be impacted (positively or negatively) by a given change to the NAS.
- Identify Monitoring Parameters Impacted by NAS Change–This function allows for the identification of hazard monitoring parameters that may be impacted by a given change to the NAS.

The function (i.e., Evaluate SRMD Content) supports the AOV user in evaluating the adequacy of SRMD content, including system (or NAS change) scope, hazard list, control effectiveness, and risk ratings, among other SRMD components. The second-tier functions that comprise this functional block are as follows:

- Identify Potential Stakeholders–This function enables identification of stakeholders that are associated with systems and facilities impacted by a given NAS change to cross-check the SRMP representation identified in the SRMD.
- Evaluate Hazard List Completeness–This function enables evaluation of the hazard list in an SRMD to ensure that no significant hazard or failures have been overlooked or improperly bounded out of the analysis.
- Evaluate Hazard Cause List Completeness–This function enables evaluation of the identified hazard causes in an SRMD to ensure that no significant failures, errors, or other anomalies have been overlooked or improperly bounded out of the analysis.
- Evaluate Effectiveness of Controls–This function enables evaluation of the proposed controls in an SRMD to ensure that the controls address the intended hazard/causes and that the controls can be expected to reduce the risk as indicated in the SRMD.
- Cross-Check Risk Against Safety-Event Frequencies and Effects–This function allows users to compare risk likelihoods and severities to historical reported system anomalies and their safety effects by querying external data sources and comparing observed event frequencies and effects to hazard-risk ratings.
- Confirm inclusion of controls in monitoring plan–This function supports AOV users in evaluating whether proposed controls are adequately addressed in the monitoring plan in an SRMD.

5.8.3 Analyze Safety Events and Information

The third functional block (i.e., Analyze Safety Events and Information) contains the set of functions that allow IDA-FS to search and analyze safety data in external databases. IDA-FS allows for searching and querying of external safety data sources. This will support the AOV user in finding and analyzing objective data that may pertain to the safety of NAS systems and changes.

The second-tier functions that comprise this functional block are as follows:

- Provide Query Capabilities on External Data–This function generates and tailors queries to search for reported NAS safety events and system anomalies related to IDA-FS model elements.
- Assemble and Validate Data From External Sources–This function collects the results of queries of external data sources and arranges the data into a form that can be sorted and analyzed by the user.
- Associate Safety Events and Info With NAS and SRMD Elements–This function enables the user to cross-check hazards and risk likelihoods against reported NAS safety event and system anomalies.

5.8.4 Manage and Process Remarks and Notifications

The fourth functional block (i.e., Manage and Process Remarks and Notifications) provides the capabilities to maintain user remarks and configure, process, and generate notifications on NAS and safety data requiring AOV attention.

The second-tier functions that comprise this functional block are as follows:

- Manage User Remarks–This function allows a user to create, edit, search, filter, and delete remarks regarding any element in the IDA-FS model. Remarks refer to AOV notes, observations, comments, questions, reminders, or action items that can be attached to any system, hazard, or other element of the IDA-FS model.
- Manage Notifications–This function allows a user to create, edit, search, filter, and delete notifications. Notifications are used to report IDA-FS model elements, NAS change impacts, and SRMD content evaluation findings needing AOV safety oversight attention based on user-defined rules.
- Process and Generate Notifications–This function is responsible for processing and managing the delivery of notifications to users according to the user-specified rules.

5.8.5 Generate Reports & Data Sets

The functional block (i.e., Generate Reports & Data Sets) contains the functions that govern IDA-FS presentation of NAS change impacts and SRMD content evaluation findings among other IDA-FS output data. This function assembles and outputs user-requested reports and reports triggered by notifications as well as user-requested data sets. Data export functions are also handled by this block, allowing AOV users to easily use the results of IDA-FS analysis in other parts of their workflow.

The second-tier functions that comprise this functional block are as follows:

- Generate Reports–This function is responsible for assembling and formatting data into a standardized report.
- Generate data sets–This function is responsible for assembling and outputting data in a format for import into external systems or software tools.

5.8.6 IDA-FS Functional Flow

Figure 8 shows the IDA-FS system level functions organized to illustrate the internal notional flow between functions.

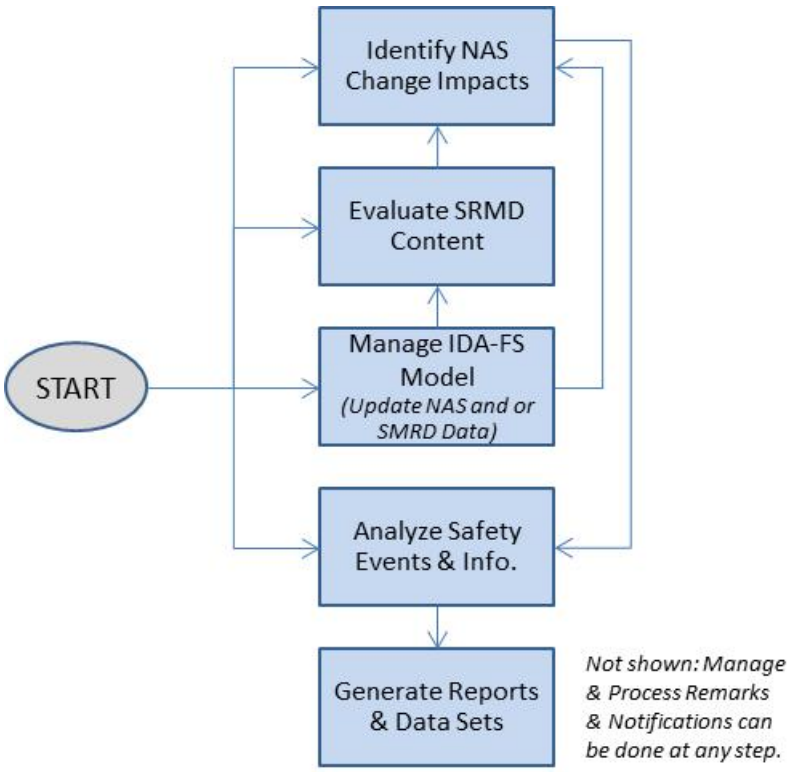

Figure 8. IDA-FS functional flow

From the Start state, the user can choose to identify NAS change impacts, evaluate SRMD content, manage the IDA-FS model, or analyze safety events and information. After identifying NAS change impacts, IDA-FS automatically proceeds to assemble and analyze safety events and information to determine whether any reported system anomalies are associated with the NAS change or changes. At the conclusion of that step, IDA-FS provides an option to generate reports and data sets upon user request. If the user first initiates an evaluation of SRMD content, the tool proceeds to the next step of identifying NAS change impacts to assist AOV with completing the SRMD review. If the user was interacting with the tool to manage the IDA-FS model (e.g., updating NAS architecture/SRMD data based on a NAS change), the tool provides the user with options to proceed to SRMD evaluation or identification of NAS changes. Though not shown in figure 8, the user may manage and process remarks and notifications at any point, because these items may be linked to any element in the IDA-FS model.

5.9 STANDARD TERMINAL AUTOMATION REPLACEMENT SYSTEM CASE STUDY

To better understand the AOV SRMD review process and to demonstrate the proposed capabilities of the IDA-FS tool, the development team chose a case study system and SRMDs. The team decided to focus on the Standard Terminal Automation Replacement System (STARS) as the primary system of interest for the IDA-FS case study. Because STARS is a terminal automation system, it interfaces with a number of different types of systems, including surveillance (such as radar and Automatic Dependent Surveillance–Broadcast [ADS-B]), other ATC facilities (including Air Route Traffic Control Centers and airport towers), and flight plan (FP) and

scheduling systems. It is also directly involved in enabling air traffic controllers to provide separation services.

Section 5.5 describes the IDA-FS capabilities that demonstrate operational scenarios for using the IDA-FS tool.

5.9.1 STARS System Overview

The STARS system provides continuous real-time support to air traffic controllers at terminal sites through the automation of certain functions. The primary automated functions are surveillance and tracking, controller data entry and display, aircraft separation assistance, FP processing, data recording, and system monitoring. The STARS system also provides support functions for data reduction, system evaluation, controller training, system administration, site and system adaptation data management, software development, and hardware and software maintenance.

STARS facilities consists of three basic site types: STARS Central Support Complex, the Operational Support Facility, and STARS Operational Site (SOS). In addition to these basic sites, local towers (LTs), remote towers (RTs), and RTs with direct radar feed provide for local ATC operations at airport sites. For the purposes of this case study, only the SOS is of interest. Each SOS accepts and processes surveillance and flight data information, providing ATC and system information to air traffic controllers and external systems. Typically the SOS includes an LT for local airport traffic control and may support one or more RTs.

Figure 9 shows an overview of the subsystems that comprise STARS and the various systems that interface with STARS at an SOS. The figure also shows selected external systems that do not directly interface with STARS (e.g., runway status lights), but that may have interactions of interest to an AOV reviewer that could be identified by IDA-FS. The SRMDs chosen for the case study discuss the subsystems that comprise STARS and the interfacing systems in greater detail.

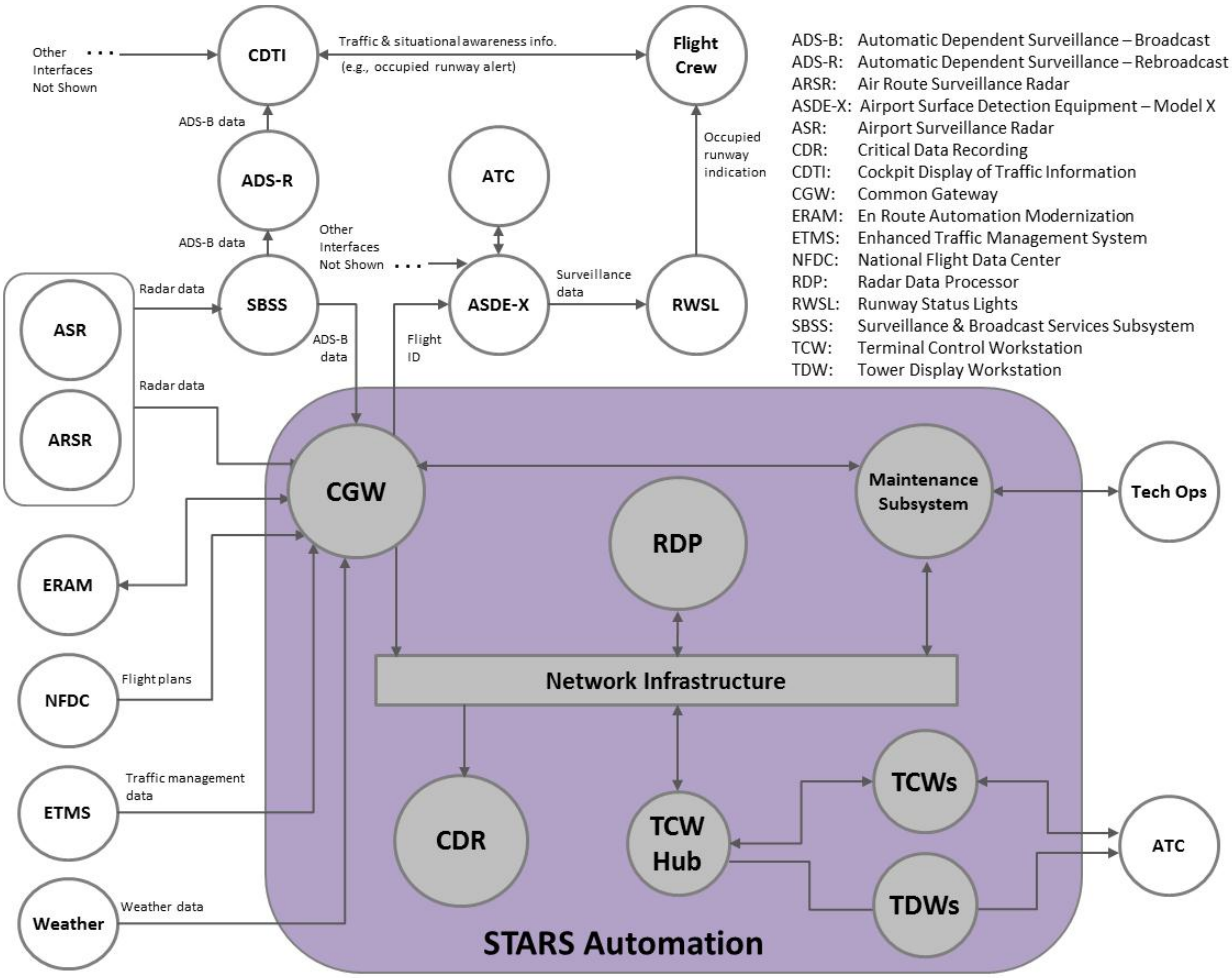

Figure 9. STARS system interfaces

5.9.2 Case Study SRMDs

The change to the NAS that was considered for this case study was the integration of ADS-B as a surveillance data source. To process ADS-B, changes were also made to the STARS processing subsystem and to the Terminal Control Workstation interface to display fused tracks and information about the ADS-B data and radar.

Two SRMDs were chosen for the case study that dealt with this change to the NAS. The first was entitled "Terminal ATC with ADS-B and STARS" and was approved on March 26, 2010 [8]. The SRMD describes the safety assessment of the end-to-end system from aircraft ADS-B avionics, the ADS-B ground surveillance system, and STARS modifications including surveillance tracker and ATC display processing. Eight medium-risk hazards were identified in the SRMD, and 16 recommended safety controls were documented to mitigate the assessed risks. The second SRMD was entitled "STARS FS-2+ Baseline Update to Include Additional ADS-B Initial Operating Capability (IOC) Requirements as Described in Engineering Change Proposal (ECP)-028" and was dated October 6, 2009 [9]. Two medium-risk hazards were identified in the SRMD, and four recommended safety requirements were documented to mitigate

the identified risks. Other hazards were identified in each of these SRMDs, but the IDA-FS development focused on the medium-risk hazards only for the purposes of this case study. Table 3 shows the identified hazards, causes, effects, and risks for each of the case study SRMDs.

Table 3. Case study hazards

Hazard ID	Hazard Title	Hazard Causes	Hazard Effects	Initial Risk	Residual Risk
SRMD: Terminal ATC with ADS-B and STARS					
CS6	Single Aircraft True Position Not Under Displayed Position in Fusion Display Mode	ADS-B Avionics fault Undetected GPS fault SBSS fault Automation fault	Based on incorrect position of aircraft, controller issues instructions to the aircraft resulting in converging aircraft Automation system does not provide conflict alert when one should be issued. Collision or controlled flight into terrain	1E (Medium)	1E (Medium)
CS7	Multiple Aircraft True Positions Not Under Displayed Position in Fusion Display Mode	GPS issues Avionics fault SBSS fault Automation fault	Based on incorrect position of aircraft, controller issues instructions to the aircraft resulting in converging aircraft Automation system does not provide conflict alert when one should be issued. Collision or controlled flight into terrain	1E (Medium)	1E (Medium)
CS8	All Aircraft True Positions are Not Under Displayed Positions While in Fusion Display Mode	GPS issues SBSS Fault Automation Fault	Increase in ATC workload due to verification of aircraft in sector Based on incorrect position of aircraft, controller issues instructions to the aircraft resulting in converging aircraft Automation system does not provide conflict alert when one should be issued. Collision or controlled flight into terrain	1E (Medium)	1E (Medium)

SBSS = Surveillance and Broadcast Services Subsystem

Table 3. Case study hazards (continued)

Hazard ID	Hazard Title	Hazard Causes	Hazard Effects	Initial Risk	Residual Risk
CS13	Failure to Display Emergency Mode for One Aircraft to ATC While in Fusion Display Mode	Avionics fault Human error SBSS fault Automation fault	Reduction in ATC services to the affected aircraft if communication is lost, and ATC does not have situational awareness of the nature of the emergency	1E (Medium)	1E (Medium)
CS16	Missed CA While in Fusion Display Mode	ADS-B and radar surveillance updates missing for same aircraft Single aircraft true position not under displayed position Persistent ADS-B position/altitude error for same aircraft Aural/visual alarms not provided to controller	Unresolved traffic conflict and subsequent collision Possible NMAC due to missed CA	1E (Medium)	1E (Medium)
CS17	MSAW While in Fusion Display Mode	ADS-B and radar surveillance updates missing for same aircraft Single aircraft true position not under displayed position Persistent ADS-B position/altitude error for same aircraft Aural/visual alarms not provided to controller	Controlled flight into terrain due to unresolved MSAW	1E (Medium)	1E (Medium)
CS18	Unnecessary Conflict Alerts in Fusion Display Mode	Persistent ADS-B position/altitude error for same aircraft Track split due to SSR & ADSB beacon code mismatch	Increase in ATC workload due to verification of CA conditions ATC fails to respond to valid CA in a timely manner due to desensitization	2D (Medium)	2D (Medium)

SBSS = Surveillance and Broadcast Services Subsystem
CA = Conflict Alert
MSAW = Missed Minimum Safe Altitude Warning;

Table 3. Case study hazards (continued)

Hazard ID	Hazard Title	Hazard Causes	Hazard Effects	Initial Risk	Residual Risk
CS19	Unnecessary MSAWs in Fusion Display Mode	Persistent ADS-B position/altitude error for same aircraft	Increase in ATC workload due to verification of MSAW conditions ATC fails to respond to valid MSAW in a timely manner due to desensitization.	2D (Medium)	2D (Medium)
STARS FS-2+ Baseline update to include additional ADS-B IOC requirements as described in ECP-028SRMD					
19731(a)	TRK displayed in the data block when not warranted and target symbol not displayed when it should be	Erroneous software calculation Understated confidence that the target is under the target symbol	Increased controller workload in either providing non-sensor separation for single TRK target, or going to single or multi sensor mode for pervasive TRK problem (all or most targets)	3C (Medium)	3D (Low)
19731(b)	TRK not displayed in the data block when warranted and the target symbol is displayed when it shouldn't be	Erroneous software calculation Understated confidence that the target is under the target symbol	Separation decreases and participants take extreme action to narrowly avoid a collision.	2D (Medium)	2E (Low)

MSAW = Missed Minimum Safe Altitude Warning; TRK = System track mode

Table 4 shows the controls proposed in each of the case study SRMDs to address the hazards. If these were HRHs, AOV would be tasked with approving these controls as part of its SRMD review.

Table 4. Case study proposed controls

Controls	Responsible Org.	Applicable Hazards
SRMD: Terminal ATC with ADS-B and STARS		
Warnings and cautions shall be developed instructing pilots using UAT transponders to change beacon codes on radar transponder before changing the UAT beacon code.	AFS	CS 13
The number of unnecessary CAs issued in STARS Fused Display Mode with ADS-B data per operational hour shall not exceed the unnecessary CA rate in single-sensor display mode by more than 10%.	STARS PO	CS 18
Controllers shall be trained to anticipate possible CAs when issuing instructions for an ADS-B equipped aircraft to change beacon code.	ATO-T SOS	CS 18
The number of unnecessary MSAWSs issued in STARS Fused Display Mode with ADS-B data per operational hour shall not exceed the unnecessary CA rate in single-sensor display mode by more than 10%.	STARS PO	CS 19
STARS FS-2+ Baseline update to include additional ADS-B IOC requirements as described in ECP-028SRMD		
Separation Standards Study (that includes multiple flight checks)	John Hopkins	19731(a) 19731(b)
Integration Phase 2 (IP2) Live Feed Testing that includes multiple flight checks	STARS Engineering and Raytheon	19731(a) 19731(b)
Independent evaluation of tracker and sensor input	ARCON Corp.	19731(a) 19731(b)
Install and run live ADSB feed through small STARS test system at target site (PHL)	STARS TFOS	19731(a) 19731(b)

UAT = Universal Access Transceiver; MSAW = Missed Minimum Safe Altitude Warning

As part of the ConOps development process, the IDA-FS team independently evaluated the SRMDs using the AOV REW criteria to better understand the information that would be of value to AOV analysts. The capability descriptions in section 5.10 include discussions of how each IDA-FS capability might be applied to AAC review of the case study SRMDs to illustrate the tool's benefit to AOV.

5.10 IDA-FS CAPABILITY DESCRIPTIONS

A set of operational capabilities for IDA-FS has been developed that provide examples of the tasks IDA-FS will support and enable for AOV users. These operational capabilities illustrate the IDA-FS functions listed in figure 7 and are grouped by system level function. This is not an exhaustive list of capabilities or functions, but demonstrates the major operations and benefits that IDA-FS

will provide to the AOV user. The list of capabilities and the system functions is provided in table 5. The table indicates what IDA-FS functions a given capability demonstrates and exercises.

Table 5. IDA-FS capabilities

ID	Capability Name	IDA-FS Functions Exercised
1	Identify change impacts	Identify interfacing systems impacted by NAS change. Identify facilities impacted by NAS change. Identify safety hazards impacted by NAS change. Identify controls impacted by NAS change. Identify monitoring parameters impacted by NAS change. Evaluate hazard list completeness. Evaluate hazard cause list completeness. Evaluate effectiveness of controls. Provide query capabilities on IDA-FS model.
2	Identify operational interactions	Identify interfacing systems impacted by NAS change. Identify safety hazards impacted by NAS change. Identify controls impacted by NAS change. Identify monitoring parameters impacted by NAS change. Evaluate hazard list completeness. Evaluate hazard cause list completeness. Evaluate effectiveness of controls. Provide query capabilities on IDA-FS model.
3	Identify potential stakeholders	Identify potential stakeholders. Provide query capabilities on IDA-FS model.
4	Identify interfacing systems not addressed in the hazard cause list.	Identify interfacing systems impacted by NAS Change. Evaluate hazard cause list completeness. Provide query capabilities on IDA-FS model.
5	Compare similar SRMDs and content	Evaluate hazard list completeness. Evaluate hazard cause list completeness. Evaluate effectiveness of controls. Provide query capabilities on IDA-FS model.
6	Query SRMDs	Evaluate hazard list completeness. Evaluate hazard cause list completeness. Evaluate effectiveness of controls. Provide query capabilities on IDA-FS model.
7	Identify hazard cause issues	Evaluate hazard list completeness. Evaluate hazard cause list completeness. Evaluate effectiveness of controls. Provide query capabilities on IDA-FS model.
8	Identify inconsistent controls	Identify controls impacted by NAS change. Evaluate effectiveness of controls. Provide query capabilities on IDA-FS model.
9	Compare monitoring plan to similar SRMDs	Identify monitoring parameters impacted by NAS change. Confirm inclusion of controls in monitoring plan. Provide query capabilities on IDA-FS model.
10	Investigate prior incidents and effects	Evaluate effectiveness of controls. Cross-check risk against safety event frequencies and effects. Provide query capabilities on External data. Assemble and validate data from external sources. Associate safety events and info with NAS and SRMD elements.
11	Capture remarks from reviewers	Manage user remarks.
12	Query remarks	Manage user remarks.
13	Manage notifications	Manage notifications. Process and generate notifications.
14	Generate a report of relevant IDA-FS data	Generate reports. Generate data sets.
15	Enter SRMD Data	Maintain and update SRMD Data Repository.
16	Enter NAS system data	Maintain and update NAS Architecture.
17	Edit IDA-FS model elements	Maintain and update NAS Architecture. Maintain and update SRMD Data Repository.

The following sections provide additional details about the IDA-FS operational capabilities. Many of these capabilities are described in terms of their application to RET review of an SRMD, but these capabilities are also expected to be of use to other AOV personnel in planning audits, evaluating overall NAS safety, and other AOV tasks.

Most of the capability descriptions below include an example based on the STARS case study presented in section 5.9.2. The examples are based on AOV review of an SRMD submitted by ATO for HRH control approval. Unless otherwise specified, the use case examples based on the STARS case study assume that the AOV user is a member of the RET tasked with reviewing the SRMD.

References to the UI and selections made by the user are generic and merely illustrative of the IDA-FS ConOps. Design details will be improved in a future development phase.

5.10.1 Identify Change Impacts

The purpose of this capability is to identify systems and subsystems that may be impacted by a proposed change to the NAS. The SMS process requires change proponents to identify and describe all systems affected by a change. Part of AOV's REW criteria includes ensuring that the system and NAS change have been properly scoped and adequately described, which means independently evaluating whether all applicable system interfaces were captured and described.

Using this capability begins with the AOV user identifying primary system(s) being changed. IDA-FS queries its internal NAS Model to identify potential interfacing systems and then displays a list of the interfacing systems to the user. The AOV user compares the list of interfacing systems to the system description in the SRMD under review. The user can get additional details on the interfacing system and data exchanged. Similarly, a user may wish to see facilities impacted by a system change. In this case, the analyst identifies the primary system(s) being changed and the facility affected by the change. IDA-FS queries its internal NAS Model to identify potential interfacing facilities and displays a list of interfacing facilities and the systems installed at those facilities. Finally, the AOV user compares the list of interfacing systems and facilities to the system description in the SRMD under review. Figure 10 shows the event sequence diagram (ESD) for this capability.

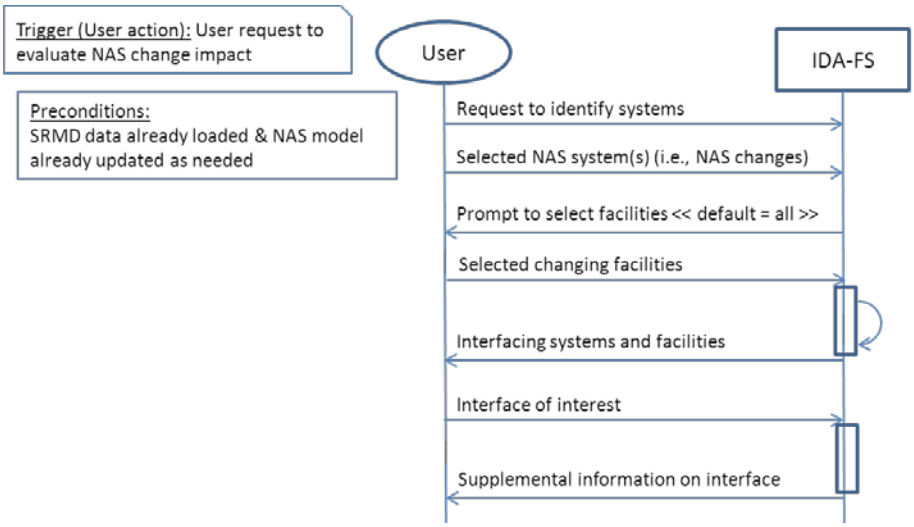

Figure 10. Identify change impacts ESD

The information on system interactions and change impacts can be used by an AOV analyst in several ways:

1. Ensure that the system description in the SRMD under review adequately addresses all affected systems, interfaces, and facilities, and that no relevant interactions have been missed or scoped out.
2. Ensure that the change to the NAS section of the SRMD under review adequately describes the proposed change and interactions with existing systems and facilities.
3. Ensure that the hazard list accounts for all systems impacted by the proposed change.
4. Ensure that all impacted systems, users, and facilities that can contribute to a hazard are correctly identified as hazard causes.

It should be noted that IDA-FS identification of an interface may or may not be an indication of a deficiency in the SRMD under review. The AOV user may need to do further research/coordination with ATO to determine if the system or facility interface was appropriately or inappropriately scoped out of the analysis.

5.10.1.1 Case Study Demonstration

The AOV user identifies STARS and ADS-B as the systems of interest in IDA-FS. The tool returns a list of systems that may interface with STARS in the NAS. The list includes:

- Airport Surveillance Radar (ASR) systems
- ADS-B surveillance
- National Flight Data Center for FPs
- Enhanced Traffic Management System for traffic management
- Weather systems
- Airport Surface Detection Equipment–Model X (ASDE-X)
- En Route Automation Modernization (ERAM)

The analyst then compares the list to the SRMD under review to assess whether all of the systems were specifically addressed/scoped in the analysis. The AOV user may request additional information on the ERAM system interface. IDA-FS returns a brief description of the ERAM system and the ERAM/STARS interface, including the type of data exchanged between the systems.

Next, the AOV user identifies the key site facility as the PHL airport. IDA-FS returns a list of systems and facilities that directly interface with STARS at PHL. The analyst notices that the PHL airport uses ASDE-X for surface surveillance. Selecting the ASDE-X/STARS interface in IDA-FS brings up additional information about the ASDE-X system and the one-way FP data output from STARS to ASDE-X. Because ASDE-X is not addressed in the ADS-B/STARS SRMD, the analyst creates a remark in IDA-FS (see section 5.10.11) as a reminder to follow up with ATO to determine why impacts to ASDE-X were not considered.

The AOV analyst uses the information provided by IDA-FS to ensure that the SRMD system description and change to the NAS descriptions correctly and adequately address all relevant system interfaces. The information may also assist the analyst in considering whether the identified hazard list includes hazards and causes related to these external system interactions.

5.10.2 Identify Operational Interactions

The purpose of this capability is to allow AOV users to investigate interactions between systems that do not necessarily interface directly. Two (or more) systems at a facility may serve similar functions or create similar hazards without directly interfacing or interacting. Analysis of identified hazards associated with each independent system may reveal interactions that are not addressed in a standalone SRMD. IDA-FS will allow AOV users to identify systems that may have operational or functional interactions not captured by direct interfaces by identifying similar hazards in SRMDs associated with the systems.

First, the AOV user selects a hazard of interest from the SRMD under review. IDA-FS queries its NAS model and SRMD data repository for similar hazards in systems at the same facility. IDA-FS returns a list of systems with similar identified hazards at the facility of interest. The AOV user can select a system from the list for additional details about the system. The AOV user can also select the hazard title for additional details for comparison to the SRMD under review. Figure 11 shows the ESD for this capability.

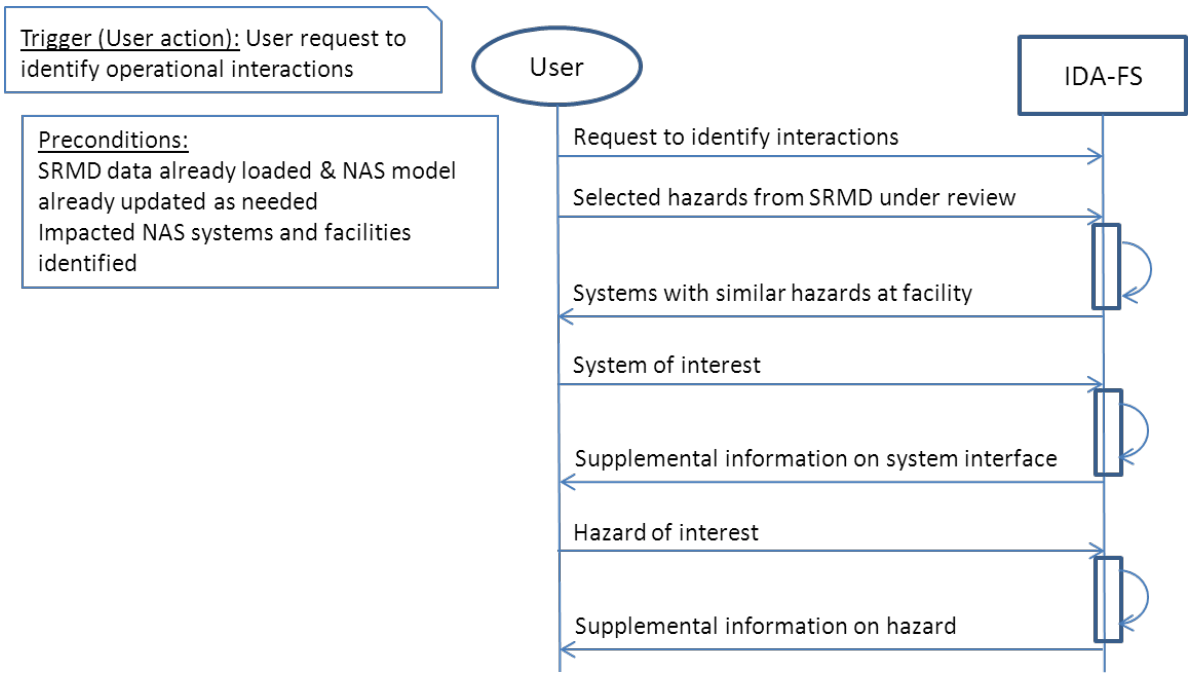

Figure 11. Identify operational interactions ESD

The information presented by IDA-FS can be used in one of two ways. First, it can support the AOV user in evaluating whether all relevant impacted systems were identified in the SRMD under review. Second, it can support the AOV user in identifying whether the identified hazard list is complete/if all relevant hazard causes (e.g., those due to operational interactions) have been identified. It should be noted that IDA-FS identification of a hazard or operational interaction may or may not be an indication of a deficiency in the SRMD under review. The AOV user may need to do further research/coordination with ATO to determine if the system or facility interface was appropriately or inappropriately scoped out of the analysis.

5.10.2.1 Case Study Demonstration

As discussed in section 5.10.1, the AOV user has identified the ADS-B/STARS systems and the associated interfacing systems that were impacted by the change and has identified PHL as the key site. IDA-FS presents the list of the hazards identified in the SRMD under review to the user. The user selects the hazard CS16: "Missed Conflict Alert While in Fusion Display Mode." IDA-FS queries other SRMDs to identify hazards dealing with missed alerting. IDA-FS returns a list of similar hazards from the ASDE-X SRMD and from an SRMD addressing the Enhanced Traffic Situational Awareness on the Airport Surface with Indications and Alerts (SURF-IA) system.

In this example, ASDE-X has been identified as an interfacing system, but SURF-IA, which is a cockpit application for flight crews that uses ADS-B data, has not. In addition, none of the hazards in the ASDE-X or the ADS-B/STARS SRMD address whether a unique hazard is created if a conflict alert is given by one system but not the other. The AOV user enters a remark (see section 5.10.12) in IDA-FS, reminding the RET to follow up with ATO and investigate whether this indicates a hazardous interaction.

5.10.3 Identify Potential Stakeholders

The purpose of this capability is to support AOV users in identifying the stakeholders who should be represented on the SRMP convened to analyze the proposed change to the NAS. One of the steps in the REW is to determine whether the SRMP included all impacted stakeholders. IDA-FS can support this process.

First, the AOV user selects the system and facility (or facilities) being changed into IDA-FS. The user may also select the impacted systems/facilities identified in Capability 1. IDA-FS queries its internal model and presents a list of proposed stakeholder organizations based on the set of impacted systems and facilities. The AOV user then compares the list of proposed stakeholders to the representatives identified in the SRMD under review. Figure 12 shows the ESD for this capability.

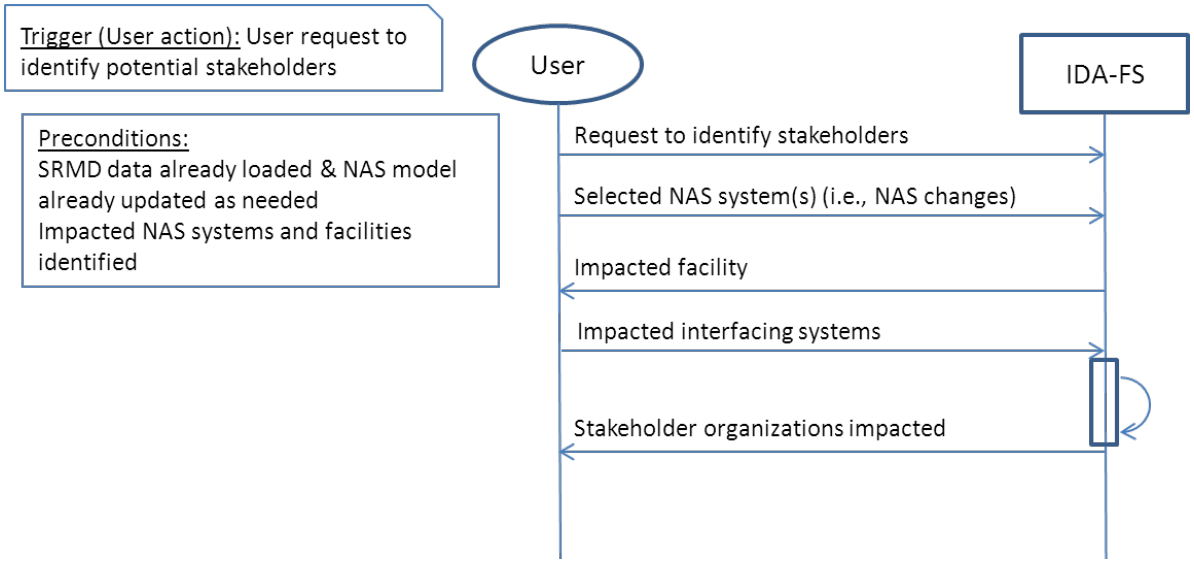

Figure 12. Identify potential stakeholders ESD

The information presented by IDA-FS can be used to support AOV evaluation of the SRMP membership identified in the SRMD under review. The report of potential stakeholders is based on the systems and facilities identified by the analyst, and will reduce the time and reviewer background knowledge required to ensure that all impacted stakeholders were represented. Note that that IDA-FS identification of a potential stakeholder may or may not be an indication of a deficiency in the SRMD under review. The AOV user may need to do further research/coordination with ATO to determine if the system stakeholder or representative was appropriately or inappropriately excluded from the SRMP.

5.10.3.1 Case Study Demonstration

As discussed in section 5.10.1, the AOV user has identified the ADS-B/STARS systems as the primary systems being changed and ERAM and ASDE-X as interfacing systems potentially impacted by the change. The user has identified PHL as the key site. Based on these systems, IDA-

FS returns a list of stakeholder organizations that should be considered as part of the SRMP. It includes:

- Surveillance and Broadcast Services (SBS) program office
- SBS system vendor
- STARS program office
- STARS system vendor
- Terminal ATC SME
- Tech Ops SME
- PHL Terminal Radar Approach Control (TRACON) manager
- PHL TRACON ATC representative
- PHL Tech Ops representative
- FAA flight standards
- ASDE-X program office
- ERAM program office

The AOV user compares the list of suggested stakeholders to the representation on the SRMP documented in the SRMD and confirms that all necessary stakeholders (as well as others) were represented on the panel.

5.10.4 Identify Interfacing Systems Not Addressed in the Hazard Cause List

The purpose of this capability is to support AOV users in identifying whether all hazard causes were identified. This capability is an extension of Operational Capability 1, as it provides additional supporting data to AOV analysts regarding the scope and impacts of the proposed change to the NAS.

The AOV user selects the SRMD of interest in IDA-FS. The user then selects the system being changed, the relevant facility (or facilities), and the interfacing systems/facilities identified in Capability 1 in IDA-FS. IDA-FS queries its NAS model to identify systems that do not have any identified hazard causes associated with them. IDA-FS returns a list of interfacing systems that are not identified as hazard causes. The AOV user evaluates whether these interfacing systems could contribute to the hazards identified in the SRMD. Figure 13 shows the ESD for this use case.

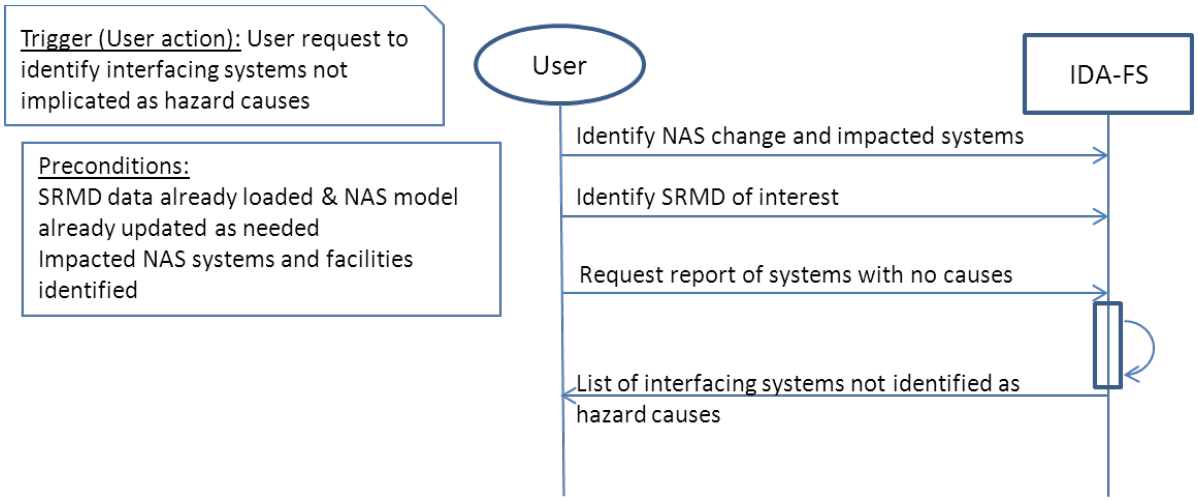

Figure 13. Identify interfacing systems ESD

The information presented by IDA-FS can be used by AOV analysts to support the evaluation of whether all possible hazard causes were identified in the SRMD under review. It can also support evaluation of the hazard controls and resultant risk ratings of the hazard. If a system or system interface that is impacted by the change to the NAS is identified during the review process, then the AOV analyst can further investigate whether that system or interface might contribute to or help to mitigate an identified hazard. It should be noted that that IDA-FS identification of a system or system interface with no associated hazard cause is not necessarily an indication of a deficiency in the SRMD under review. The AOV user may need to do further research/coordination with ATO to determine if there are credible causes or mitigations related to the interfacing system.

5.10.4.1 Case Study Demonstration

As discussed in section 5.10.1, the AOV user has identified the ADS-B/STARS systems as the primary systems being changed, and ERAM and ASDE-X as interfacing systems impacted by the change. The user has identified PHL as the key site. The AOV user selects the ADS-B STARS SRMD being reviewed in IDA-FS. IDA-FS queries its NAS model to determine if any of the identified interfacing systems are associated with hazard causes in the SRMD. IDA-FS returns a list highlighting the fact that ASDE-X and ERAM are not implicated as causes of any of the identified hazard in the SRMD. Upon further investigation, the AOV user determines that this is a consistent conclusion, because these systems are downstream from the proposed NAS change and therefore not contributing causes to any of the identified hazards.

5.10.5 Compare Similar SRMDs and Content

The purpose of this capability is to support AOV users in identifying and comparing SRMDs related to a proposed NAS change. Prior and related SRMDs can help to shed light on proposed changes, hazards, causes, risk evaluations, and proposed controls. Guidance given at several points in the REW instructs reviewers to compare the details of hazards to similar hazards in related SRMDs. IDA-FS can support this process by automating and accelerating the identification of related SRMDs and presenting the hazards for easy comparison.

This capability consists of two main tasks: identifying similar SRMDs and comparing SRMD data. First, the AOV user selects the SRMD under review. IDA-FS queries its NAS model and SRMD data repository to identify related SRMDs. The AOV user may filter the SRMDs by various criteria, including type of system, date range, system, and facility. IDA-FS generates a list of potential SRMDs of interest, and the AOV user can select one or more SRMDs from the list. Figure 14 shows the ESD for this portion of the capability.

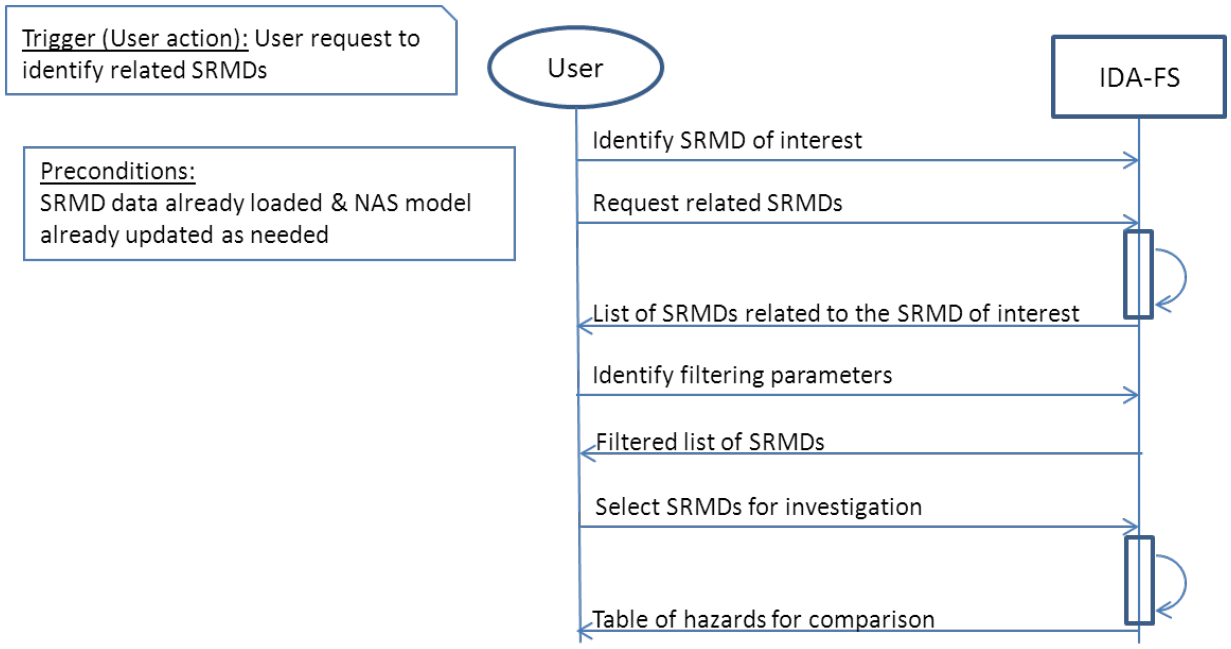

Figure 14. Identify related SRMDs

Once a set of similar SRMDs is identified, IDA-FS will allow for comparisons between the SRMD under review and the identified SRMDs. The AOV user may choose to compare hazard lists between SRMDs, causes between two or more hazards, risk ratings among identified hazards, or hazard controls and mitigations. IDA-FS will query the selected SRMDs and format the results to facilitate comparison and analysis by the AOV user. The AOV user can select a hazard and receive additional details from its SRMD. Figure 15 shows the ESD for this use case.

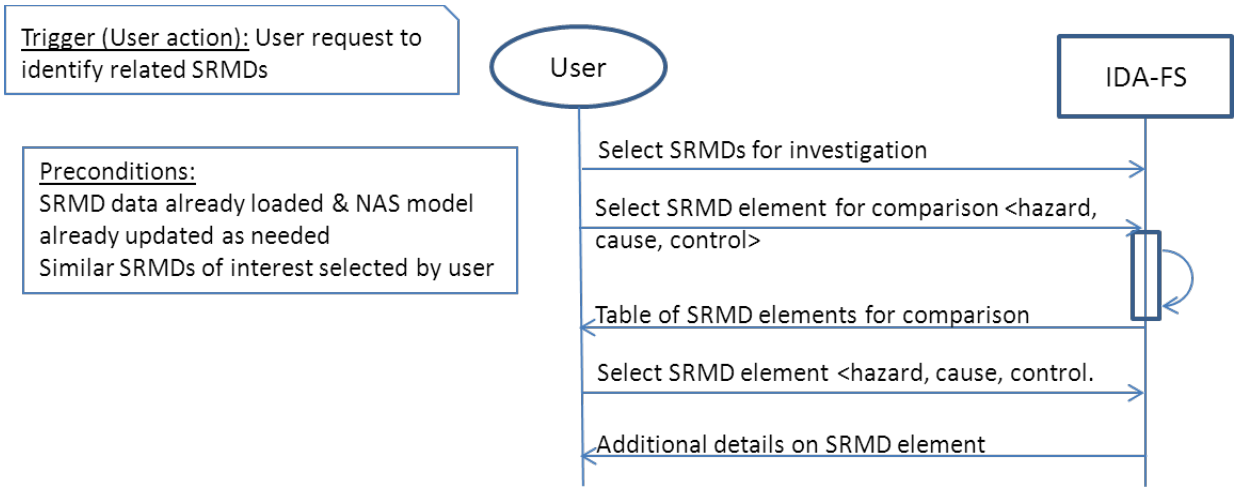

Figure 15. Compare SRMD data elements

The information presented by IDA-FS can be used by the AOV user to:

1. Evaluate whether the hazard list in the SRMD under review is complete.
2. Evaluate whether the hazard severities in the SRMD under review are consistent with prior/related SRMDs.
3. Evaluate whether the hazard likelihoods in the SRMD under review are consistent with prior/related SRMDs.
4. Evaluate whether hazard controls and mitigations in the SRMD under review are consistent with prior/related SRMDs.

The information presented by IDA-FS can be used by the AOV user to compare the hazard causes identified in the SRMD under review to prior related SRMDs. This function is currently done manually by reviewers, but IDA-FS can automate and streamline the process, providing a significant time savings. If hazard causes or controls are missed in the SRMD under review, or new ones are identified, the reviewer can examine the details to ensure that the resultant cause list is complete and that controls adequately address the identified causes.

It should be noted that that IDA-FS identification of related SRMDs and hazard lists may or may not be exhaustive. In addition, identification of a different severity or likelihood for a similar hazard may or may not be an indication of a deficiency in the SRMD under review. The AOV user may need to do further research/coordination with ATO to determine if inconsistencies between the SRMD under review and prior safety analyses are appropriate and justifiable. IDA-FS will support AOV by automating the process of searching for related SRMDs and comparing them to the SRMD under review.

5.10.5.1 Case Study Demonstration

As discussed in section 5.10.1, the AOV user has identified the ADS-B/STARS systems as the primary systems being changed and ERAM and ASDE-X as interfacing systems impacted by the change. The user has identified PHL as the key site. The AOV user selects the ADS-B STARS

SRMD being reviewed in the IDA-FS interface. IDA-FS queries its NAS model to find other related SRMDs of interest. IDA-FS returns a list of related SRMDs including:

- ADS-B/Common Automated Radar Terminal System (CARTS) SRMD–This describes a similar change to a different terminal automation platform (CARTS rather than STARS).
- SRMD for STARS FS-2+ Baseline Update to Include Additional ADS-B IOC Requirements as Described in ECP-028–This SRMD was prepared by the STARS Acquisition team as part of the development of the STARS R21 development life cycle.

The AOV user selects the STARS FS-2+ SRMD, and IDA-FS returns a formatted list of the identified hazards and their risk ratings, for comparison to the current SRMD. The AOV user can quickly see and compare the hazard CS6: "Single Aircraft True Position Not Under Displayed Position in Fusion Display Mode" from the ADS-B/STARS SRMD to the hazard "Single Aircraft True Position Not Under Displayed Position" from the ADS-B/CARTS SRMD. The AOV user can quickly see that the identified causes are similar and that the current and residual risk ratings are both 1E (Medium). This lends credibility to the analysis found in the SRMD under review.

5.10.6 Query SRMDs

The purpose of this capability is to support AOV users in searching SRMDs for topics or data of interest. The guidance given in the REW instructs AOV reviewers to research related SRMDs to compare hazards, causes, risk ratings, and proposed controls. IDA-FS can search for SRMD elements based on user-selected keywords.

First, the AOV user identifies the keywords they wish to search for. These may be related to systems, hazards, causes, controls, or some combination thereof. IDA-FS queries its NAS model and SRMD data repository to identify SRMDs that match the search terms. The AOV user may filter the SRMDs by various criteria, including type of system, date range, system, and facility. IDA-FS generates a list of potential SRMDs of interest, and the AOV user can select one or more SRMDs from the list to obtain additional information. Figure 16 shows the ESD for this capability.

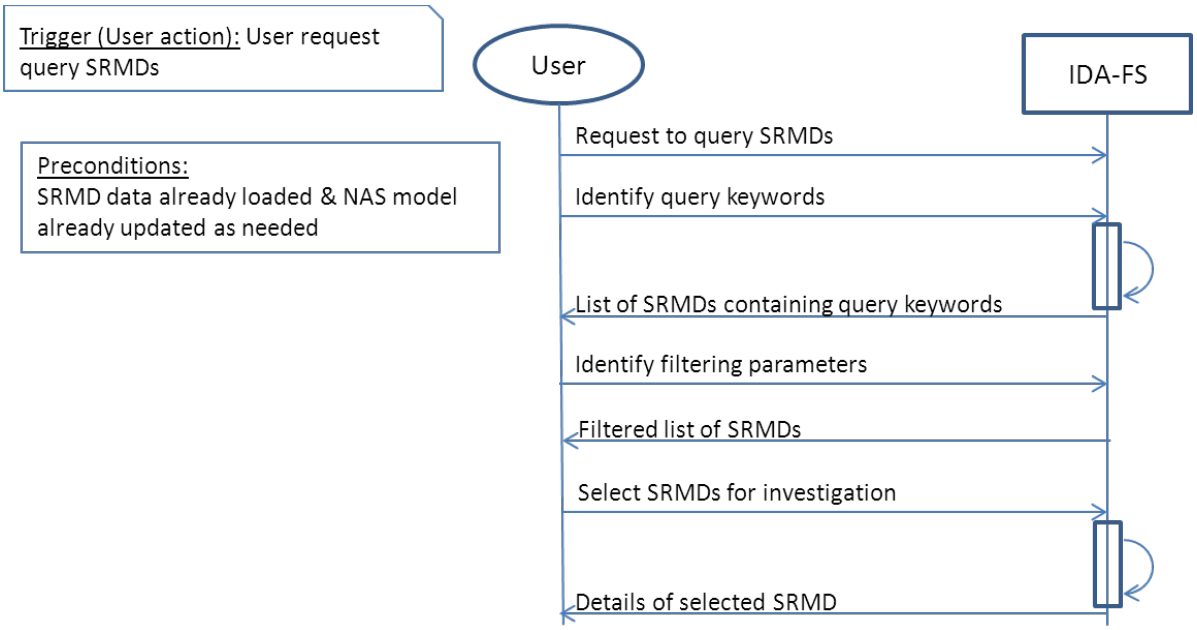

Figure 16. Query SRMDs ESD

The information presented by IDA-FS can be used by the AOV user to aid in investigating control effectiveness and sufficiency. It should be noted that that IDA-FS may not identify any proposed controls similar to the ones in the SRMD under review. If the proposed controls are not similar to those implemented in prior NAS changes, the AOV user may need to do further research/coordination with ATO to assess proposed control effectiveness.

5.10.7 Identify Hazard Cause Issues

The purpose of this capability is to support AOV users in identifying common issues related to hazard causes in SRMDs under review. IDA-FS can support the identification of single points of failure, common causes across multiple hazards identified in an SRMD, and identified hazard causes that do not have any mitigations. Single points of failure are of significant concern in hazard analyses, and one of the REW criteria is to check for single points of failure. Common causes are hazard causes that may produce or contribute to several separate hazards and may indicate a particular system vulnerability. A similar approach can be taken to identify common causes to hazards identified in a system or facility across multiple SRMDs. Unmitigated hazard causes are potential holes in the "Swiss cheese model." Identifying hazard causes with no existing or proposed controls will assist AOV users in evaluating the assessed hazard risks. IDA-FS automates the process of searching for common hazard causes, hazards with only one identified cause, and hazard causes with no identified controls, greatly speeding that aspect of AOV review.

This capability requires that the hazard data from the SRMD under review has been inputted, including the identified hazards and hazard causes. IDA-FS links hazard causes to hazards and to systems in its internal NAS model. The AOV user requests a report of single and common cause issues in the SRMD of interest. IDA-FS then queries the hazards in the SRMD under review to identify causes that are identified with multiple hazards. IDA-FS flags the hazards with single

causes for review by the AOV user. IDA-FS also returns a list of common causes and the associated hazards to the AOV user. The AOV user can expand the search to find common causes across all tracked hazards in the selected system, not just the ones in the SRMD under review. Finally, IDA-FS returns a list of hazard causes that do not have any controls identified to mitigate them. Figure 17 shows the ESD for this use case.

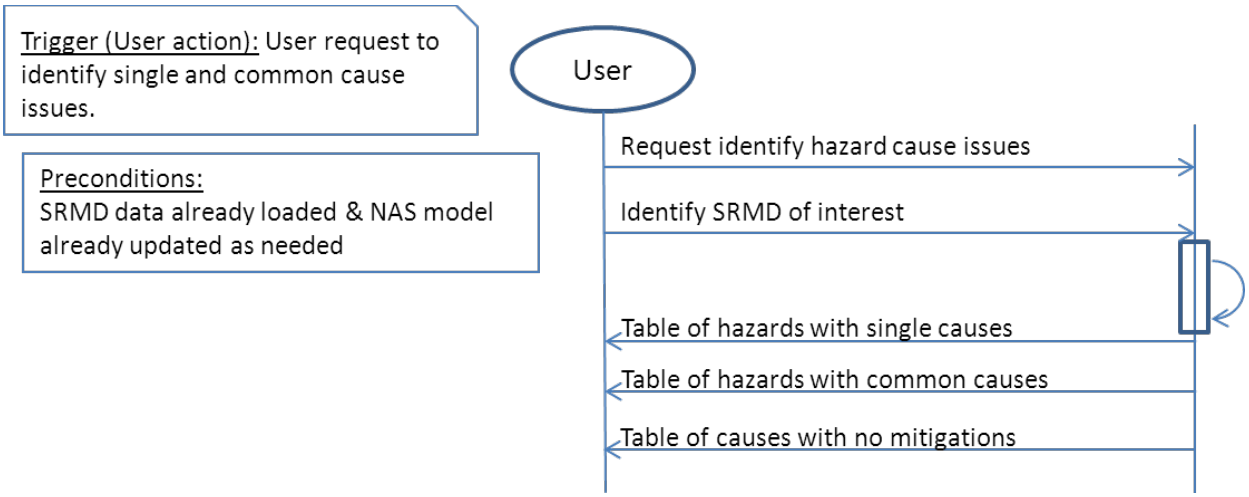

Figure 17. Identify hazard cause issues ESD

The information presented by IDA-FS can be used to identify causes that are implicated in multiple hazards. Though these causes may not be the primary hazard pathway for the system, they may still merit additional examination, research, and/or coordination with ATO to determine if the common hazard causes have sufficiently treated. This capability can also be used to identify a partial set of hazards with single point failures. It should be noted that IDA-FS can identify and flag hazards with only one cause identified, but it will not necessarily identify a single point of failure if other causes are identified in addition to the single point cause. The AOV user may need to do further research, SRMD review, and/or coordination with ATO to determine if single points of failure exist for any hazard. Finally, the information presented by IDA-FS can be used to evaluate the assessed risk of hazards in the SRMD under review. It may also be of use in evaluating proposed controls. It should be noted that that IDA-FS identification of an unmitigated hazard cause may or may not be a direct indication of a deficiency in the SRMD under review. The AOV user may need to do further research/coordination with ATO to determine if controls exist to mitigate the identified cause or if proposed controls are sufficient to manage the assessed risk.

5.10.7.1 Case Study Demonstration

The AOV user wants to investigate whether any of the hazards in the ADS-B/STARS SRMD are due to a common cause. The user selects the SRMD and requests a report of common causes. IDA-FS queries its internal model and finds four hazards that share a common cause, "Track processing fault." The hazards that identify this common cause are:

1. CS1–Loss of surveillance for one aircraft on ATC display while in fusion display mode
2. CS2–Loss of surveillance for multiple aircraft on ATC display while in fusion display mode
3. CS4–Single aircraft not acquired or displayed to ATC while in fusion display mode
4. CS5–Multiple aircraft not acquired or displayed to ATC while in fusion display mode

The user can then focus their review on the four hazards that share the cause to assess whether this represents a significant risk.

Next, the AOV user also wants to investigate whether any of the hazards in the related STARS FS-2+ SRMD contain single points of failure. The user selects the SRMD in the IDA-FS interface and then requests a report of single point failures. IDA-FS queries its internal model and reports that two of the hazards identified in the SRMD have only a single cause identified, "Erroneous software calculation." The user then adds a remark/notification to follow up with ATO regarding this single point of failure for hazards.

5.10.8 Identify Inconsistent Controls

The purpose of this capability is to support AOV users in identifying controls in SRMDs that are not consistent with controls and mitigations cited in other SRMDs. This is accomplished by querying the IDA-FS internal model to match similar identified hazard controls linked to systems of interest.

The AOV user imports or inputs the hazard data from the SRMD under review, including the identified hazards and hazard causes. IDA-FS links hazard causes to hazards and to systems in its internal NAS model. The AOV user requests IDA-FS to analyze inconsistent controls. IDA-FS queries the controls cited in the SRMD under review. Control titles, linked systems, and control metadata are used to identify each hazard control. IDA-FS queries hazard controls linked to the same system(s) from other SRMDs to find matching controls to those cited in the SRMD under review. IDA-FS compares cited performance values for sets of matching hazard controls to identify discrepancies. IDA-FS flags the controls with inconsistent performance data for review by the AOV user. Figure 18 shows the ESD for this IDA-FS capability.

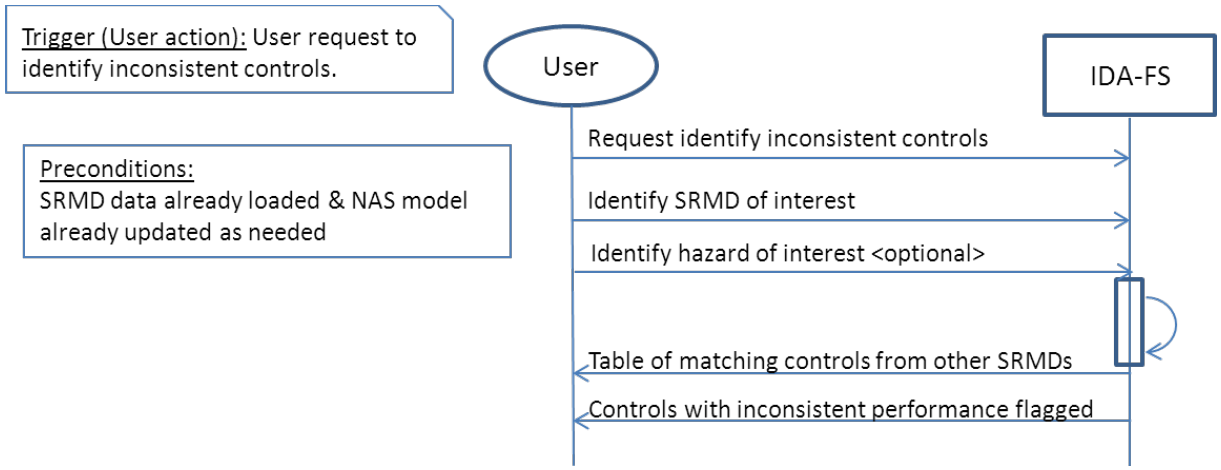

Figure 18. Identify inconsistent controls ESD

The information presented by IDA-FS can be used by AOV users to evaluate whether controls cited or proposed to mitigate a hazard are reasonable to address the hazard or cause. If a cited control has a likelihood or other performance value on a different order of magnitude than the same control in a prior approved SRMD, the AOV user may need to do further research/coordination with ATO to determine if the rationale for changing the performance value is appropriate.

5.10.8.1 Case Study Demonstration

The ADS-B/STARS SRMD contains a hazard titled "Loss of surveillance for all aircraft on ATC display." One of the causes listed is secondary radar failure, and it has an associated likelihood of 1e-5/hr. The AOV user reviewing the ADS-B/STARS SRMD identifies the SRMD in IDA-FS and requests a report of inconsistent controls. IDA-FS queries its NAS model and finds a separate SRMD—the ASR-11 Technical Refresh SRMD. That SRMD cites unavailability for the radar at 1e-3. No additional explanation is given in the ADS-B/STARS SRMD regarding the source of the availability value used.

IDA-FS flags this discrepancy for the user, who then follows up with ATO to ascertain why the ADS-B/STARS value is 2 orders of magnitude less likely.

5.10.9 Compare Monitoring Plan to Similar SRMDs

The purpose of this capability is to support AOV users in comparing the hazard and control monitoring parameters in an SRMD to those identified in prior related SRMDs. This comparison helps AOV reviewers to evaluate the adequacy of the continuous monitoring plan. Guidance given in the REW instructs reviewers to compare the details of hazards to similar hazards in related SRMDs. IDA-FS can automate and accelerate this process for reviewers.

The AOV user imports or inputs the hazard data from the SRMD under review, including the identified hazards, proposed controls, and monitoring parameters. IDA-FS links monitoring parameters to hazards and proposed controls in its internal NAS model. Next, the AOV user selects the similar SRMDs identified in Capability 5. The AOV user selects the hazards of interest to

compare from the SRMD under review and from the historical SRMDs. IDA-FS queries the monitoring parameters cited in the SRMD under review. IDA-FS queries the monitoring parameters linked to the similar hazards from other SRMDs to find matching causes as those cited in the SRMD under review. Finally, IDA-FS generates a table of monitoring parameters for each hazard for comparison by AOV user. Figure 19 shows the ESD for this capability.

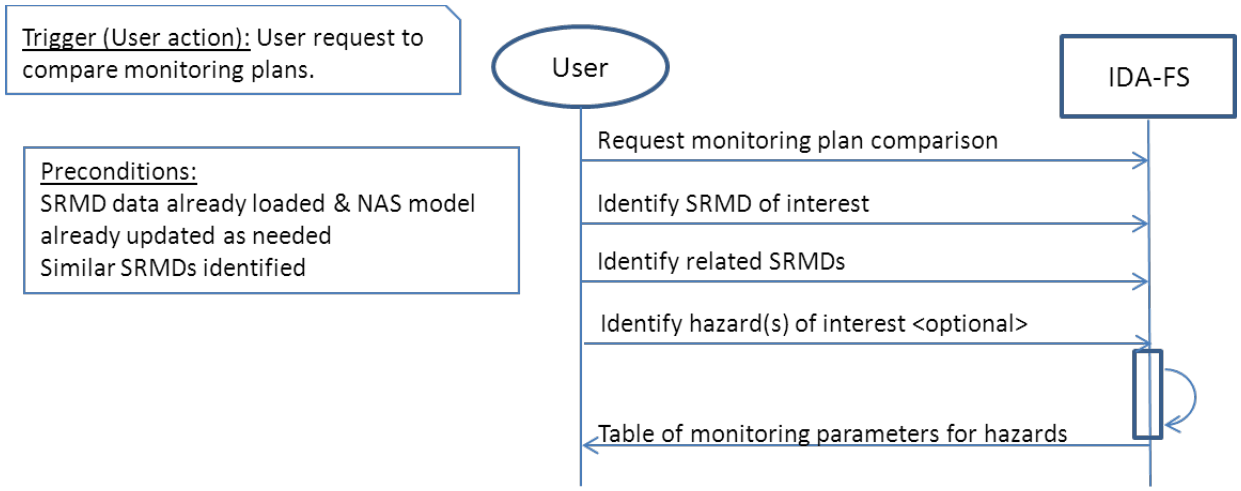

Figure 19. Compare monitoring plan ESD

The information presented by IDA-FS can be used by the AOV user to compare the monitoring parameters identified in the SRMD under review to prior related SRMDs. This function is currently done manually by reviewers, but IDA-FS can automate and streamline the process, providing a significant time savings. If monitoring parameters for a hazard or control are inconsistent with identified monitoring parameters in prior approved SRMDs, the AOV reviewer can investigate further to determine whether this represents a deficiency in the monitoring plan.

5.10.9.1 Case Study Demonstration

To assess the hazard monitoring plan, the AOV user selects the ADS-B STARS SRMD being reviewed in the IDA-FS interface. IDA-FS queries its NAS model to find other related SRMDs of interest. IDA-FS returns a list of related SRMDs including the ADS-B/CARTS SRMD. This SRMD describes a similar change to a different terminal automation platform (CARTS rather than STARS).

The AOV user selects the ADS-B/CARTS SRMD for monitoring plan comparison, and IDA-FS returns a formatted list of the monitoring plan parameters from each SRMD. The AOV user can quickly see that the monitoring parameters dealing with performance and reliability are comparable between the two SRMDs. This lends credibility to the analysis found in the SRMD under review.

5.10.10 Investigate Prior Incidents and Effects

The purpose of this capability is to support AOV users by providing a single interface point to search multiple databases of aviation safety and event reports. This will enhance AOV user's

ability to investigate the details, severity, and frequency of incidents related to hazards of interest. Several REW criteria instruct AOV analysts to evaluate hazards and controls in the SRMD under review in light of findings from external incident and reporting databases. IDA-FS will support searching, filtering, and compiling data from multiple queries of external safety reporting databases to collect potential evidence related to the hazards in the SRMD.

The AOV user identifies query keywords of interest, which may be based on identified hazards, causes, effects, and/or controls in the SRMD under review. IDA-FS formats the keyword(s) into a query of external safety and event reporting databases. The AOV user may filter the query by parameters including date range, database, and/or additional keywords. IDA-FS presents the query results in a report of incidents that may be related to the proposed change to the NAS. Figure 20 shows the ESD for this capability.

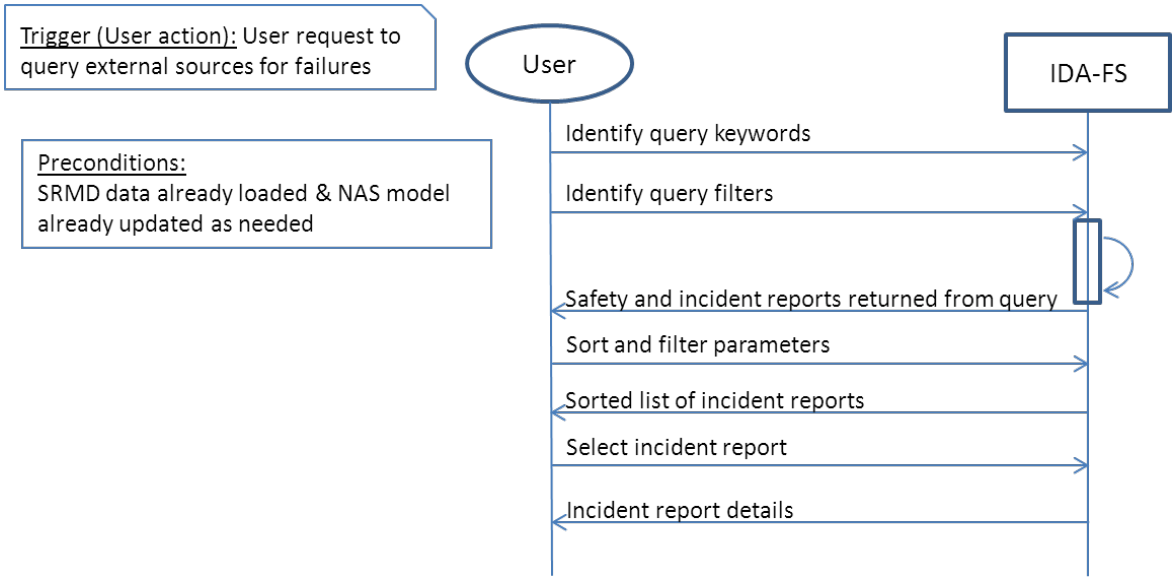

Figure 20. Investigate prior incidents ESD

The query results presented by IDA-FS can be used to:

1. Evaluate whether all hazard causes were considered and documented in the SRMD under review.
2. Evaluate whether all observed hazard effects in similar/historical systems were considered in the SRMD under review.
3. Evaluate whether assessed hazard severities and likelihoods are in accordance with historical system incidents.
4. Investigate incidents and events related to proposed hazard controls.

It should be noted that the safety incident reports identified by queries via IDA-FS may or may not correspond directly with the specifics of the safety analysis in the SRMD under review. It will be necessary for the AOV user to investigate particular reports of interest to determine their applicability to the hazard being reviewed. Examination of historical incidents and performance may help to shed light on relevant safety concerns in light of the proposed change to the NAS.

5.10.10.1 Case Study Demonstration

The AOV user wants to investigate the residual likelihood cited for the hazard "Loss of Surveillance for Multiple Aircraft on ATC Display While in Fusion Display Mode." The user selects the keywords "STARS Error OR failure AND fusion mode." The user also selects filter criteria that restrict the search to STARS sites and a date range in the last 3 years. IDA-FS queries the ASRS and ASIAS databases and returns the matching reports in a consistent format for user review.

Based on the query results, the user is able to determine that six incidents of target loss have been reported in STARS in the last 3 years, which indicates a more frequent rate of hazard occurrence than the extremely remote frequency cited in the SRMD. The AOV user then creates a remark/notification as a reminder to follow up with ATO for further investigation.

5.10.11 Capture Remarks from Reviewers

The purpose of this capability is to support AOV users in their review of SRMDs by capturing remarks during the review process. AOV users may enter additional information on SRMDs, systems, hazards, causes, controls, and risks. The notes may include questions, concerns, supplemental information, lessons learned, or objections. The notes need not be formally submitted for adjudication or comment, but they may be exported, queried, amended, edited, or deleted (by the AOV user who owns the note).

To add a remark, the AOV user first selects an entity from the IDA-FS interface. An entity can be an SRMD, a system, hazard, hazard cause, hazard control/mitigation, a proposed control, or a monitoring parameter. The AOV user selects the option to add a remark to the entity in the IDA-FS interface. The AOV user enters textual information in the notes field. If desired, the AOV user may create notification rules that will notify the user or some other party of required follow up activities. IDA-FS saves the remark and links it to the entity in the IDA-FS internal NAS model. IDA-FS also gives confirmation to the AOV user that the remark has been saved. Figure 21 shows the ESD for this capability.

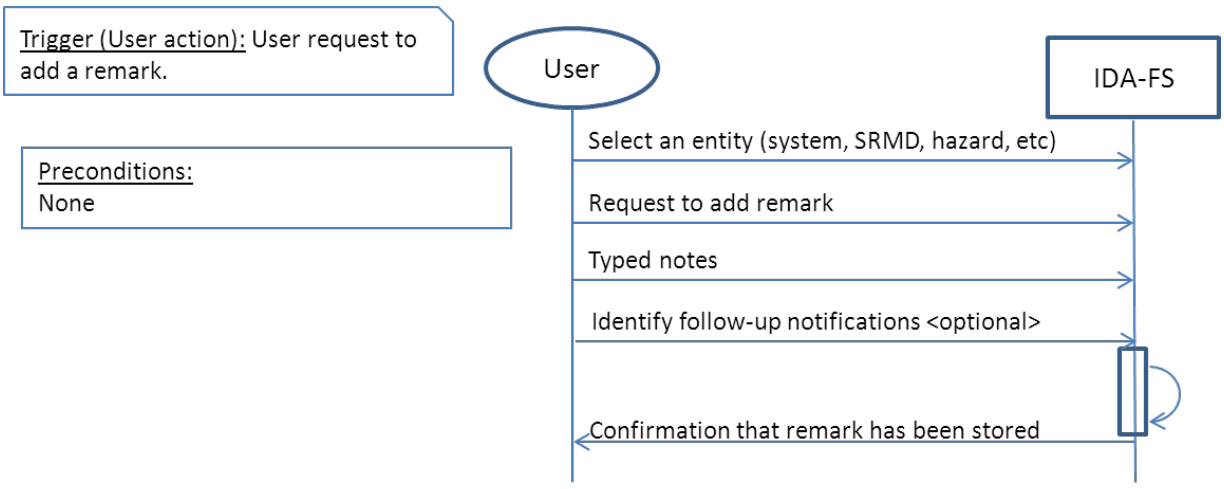

Figure 21. Capture remarks ESD

The remarks field can be used to record a variety of different types of information, both to support the current review of the SRMD and to support reviewers and auditors searching for additional information uncovered by other IDA-FS users. Remarks may also be linked to notifications, which are used to automatically inform or remind a user of information contained in a remark.

5.10.12 Query Remarks

The purpose of this capability is to support AOV users by querying and presenting remarks captured during earlier AOV activities. AOV users of IDA-FS may enter additional information on SRMDs, systems, hazards, causes, controls, and risks. The remarks may include questions, concerns, supplemental information, lessons learned, or objections. These notes may be of benefit to AOV users at a later point, so IDA-FS will allow users to query the remarks for additional information.

Figure 22 shows an ESD for this capability. The AOV user identifies query keywords of interest, which may be based on identified hazards, causes, effects, and/or controls in the SRMD under review. IDA-FS formats the keyword(s) into a query of user remarks in its internal database. The AOV user may filter the query by parameters including date range, SRMD, facility, and/or additional keywords. IDA-FS presents the query results in a report of user remarks that may be related to the item being investigated. The AOV user may sort the remarks by factors including date, system, or owner. The AOV user may select one or more remarks to view their details.

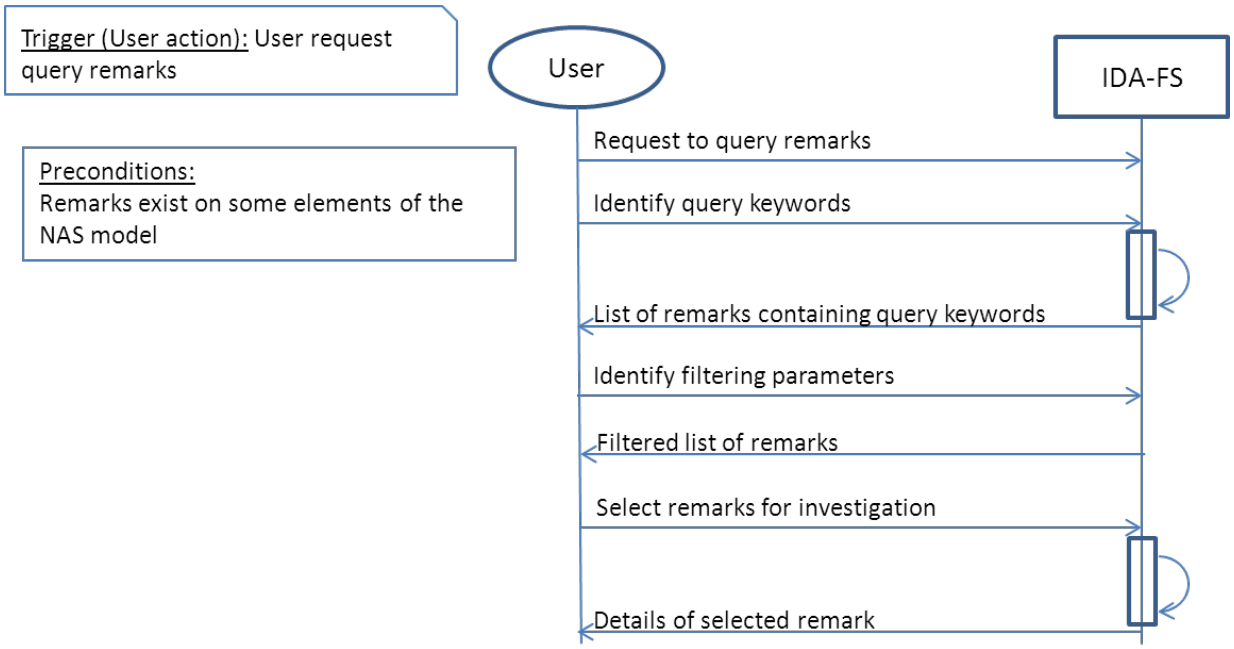

Figure 22. Query remarks ESD

The query results presented by IDA-FS can be used by the AOV user to incorporate lessons learned, clarifying supplemental information and other recorded data into the AOV workflow. The notes field can be used to record a variety of different types of information, both to support the current review of the SRMD and also to support reviewers and auditors searching for additional information uncovered by other IDA-FS users.

5.10.13 Manage Notifications

The purpose of this capability is to support AOV users by creating and delivering notifications and reminders to users. AOV users of IDA-FS may create notifications on SRMDs, systems, hazards, causes, controls, and risks. These notifications are a type of remark, but involve a follow-up or action component. IDA-FS will deliver notifications to specified users according to user-generated rules.

Figure 23 shows an ESD for this capability. The AOV user creates a notification remark in IDA-FS. The user specifies who is to receive the notification, when (or at what interval), the method by which they will be notified, and text describing what the recipient is expected to do. The user may also specify rules for notifications under particular conditions (e.g., when IDA-FS analysis uncovers a common cause or when an SRMD regarding a particular system is entered). IDA-FS will store the notification and deliver the reminder to the specified user when the conditions are met.

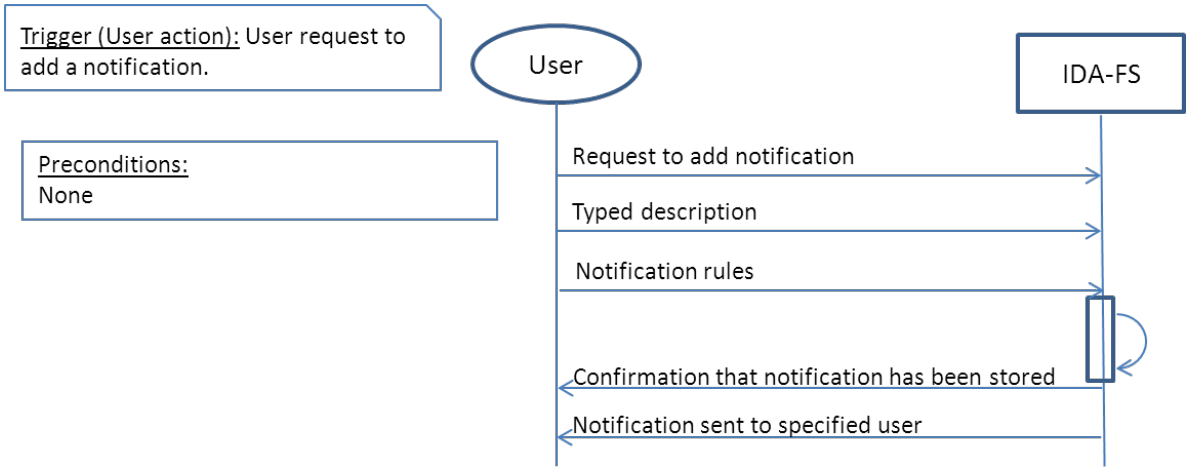

Figure 23. Manage notifications ESD

The notifications delivered by IDA-FS can be used by the AOV user to remind themselves or a colleague of follow-up actions related to proposed controls or safety monitoring. Notifications can also be set up to notify users when system changes with potential safety impacts are implemented or when safety issues are flagged by IDA-FS.

5.10.14 Generate a Report of Relevant IDA-FS Data

The purpose of this capability is to support AOV users in reporting the findings of their review of an SRMD. The REW guidance instructs AOV reviewers to document comments on the SRMD, review findings, and lessons learned during the review. IDA-FS will, at user request, generate a summary of notes and safety event statistics that can be used to complete or supplement this report.

Figure 24 shows the ESD for this capability. The AOV user requests a summary report from IDA-FS. The AOV user selects the SRMD of interest, and IDA-FS presents a list of notes and findings generated during the review of that SRMD. The AOV user chooses the elements desired in the

summary report. IDA-FS generates a formatted report of the selected information. If requested by the AOV user, IDA-FS may also export the report to a file for use in other programs.

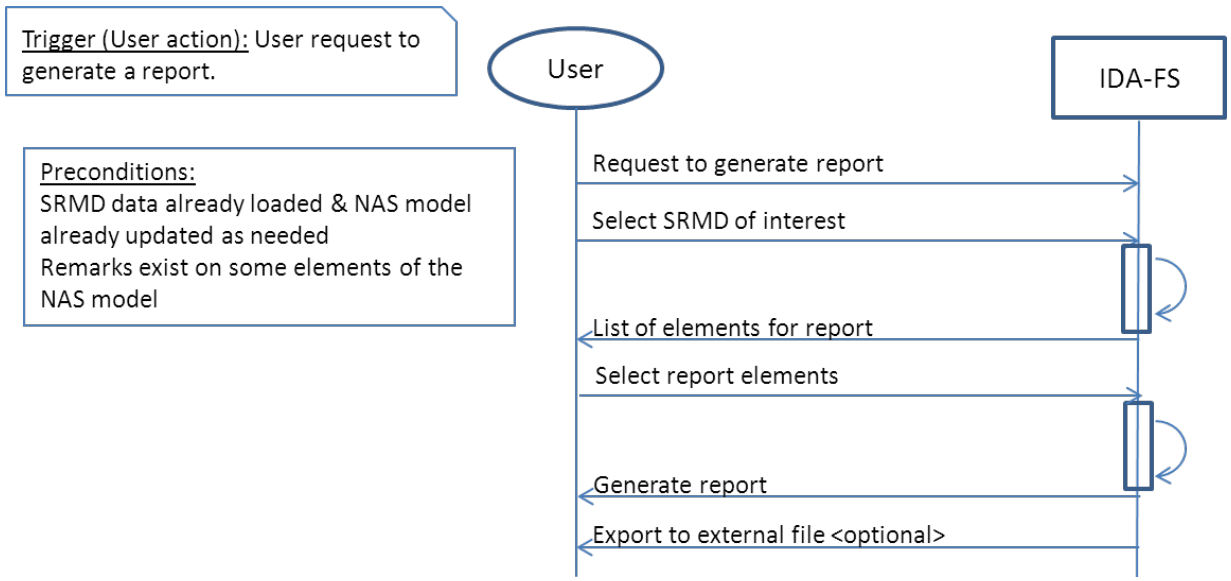

Figure 24. Generate report ESD

The resultant report can be used as a summary of RET findings during the SRMD review, it can collect findings on a particular system or control, or summarize lessons learned during a review. It may also be used by AOV auditors or other AOV users in planning additional safety activities.

5.10.15 Enter SRMD Data

To perform the evaluation tasks in IDA-FS, it is necessary to first import data from and about the SRMD under review into IDA-FS.

Entering SRMD data serves two basic purposes: first, it allows for the comparison and evaluation functions for that SRMD within IDA-FS. Second, the SRMD data is used to update and maintain the internal IDA-FS model. The change to the NAS and associated hazards and controls documented in the SRMD may be added to the model if the change is implemented to track the current state of the NAS over time. Entering SRMD data is a task that will be primarily performed by IDA-FS administrators.

The AOV user begins by performing a search for the SRMD in the digital library (SRM Tracking System or similar). If the SRMD data is available in the electronic form, the user selects import function. IDA-FS imports system data, hazards, causes, controls, risk ratings, and monitoring parameters. Finally, the AOV user reviews imported data for completeness and correctness, making corrections as required.

If SRMD is not available in an automatically importable format, the AOV user must manually import the SRMD data. The user must identify the system being changed, identify the interface changes (if any), input hazard data, including description, causes, controls, current/residual risks, and proposed controls, and input hazard monitoring plan details. IDA-FS will present the SRMD

data and NAS model changes for review, and the AOV user will edit the data as necessary. Finally, changes to the NAS model are committed.

Once the SRMD data has been imported or entered by the AOV administrator user, other IDA-FS capabilities will be enabled, including analysis of hazards, causes, and controls, as described in other operational capability descriptions above.

5.10.16 Enter NAS System Data

To ensure that the SRMD evaluation tasks in IDA-FS function correctly, it is necessary to regularly import data about NAS systems, facilities, and interfaces into IDA-FS.

Entering NAS system data ensures that the internal IDA-FS model is complete and up-to-date. New NAS system data must be entered when a system is implemented in the NAS, whether NAS-wide or at a single site. The change to the NAS and associated hazards and controls documented in the SRMD are added to the NAS model to track the current state of the NAS over time. Entering SRMD data is a task that will be primarily performed by IDA-FS administrators.

The AOV user begins by performing a search for NAS system in the appropriate digital library(s), including the NAS EA website. The user must identify the system being added or changed, identify and characterize the physical and logical interfaces, and identify the facilities where this system is to be used. The user should also identify any SRMDs that address the NAS system to link them in the model. IDA-FS will present the NAS model elements and changes for review, and the AOV user will edit the data as necessary. Finally, changes to the NAS model will be committed.

Once the NAS system data has been imported or entered by the AOV administrator user, other IDA-FS capabilities will be enabled, including analysis of hazards, causes, and controls, as described in other operational capability descriptions above.

5.10.17 Edit IDA-FS Model Elements

To ensure that the SRMD evaluation tasks in IDA-FS function correctly, it is necessary to regularly update data about NAS systems, facilities, and interfaces into IDA-FS.

Editing and updating NAS system and SRMD data ensures that the internal IDA-FS model is complete and up-to-date. Updates to NAS systems may come in the form of new system acquisitions that impact existing systems, updates to existing systems to extend their life or fix identified issues, or decommissioning of a system at a facility or NAS-wide. Each change to the NAS must have an accompanying SRMD or SRMDM, and the safety analysis data must be added to the IDA-FS model to track the current state of the NAS over time. In addition, editing IDA-FS model elements will be necessary at times to correct errors that are identified in the model or supporting model data. Editing SRMD data is a task that will be primarily performed by IDA-FS administrators.

The AOV user begins by performing a search for the model element, whether it is a system, interface description, SRMD, hazard, cause, control, or monitoring parameter. IDA-FS will present the model element and its properties to the user. The user will edit the properties that must be

updated. IDA-FS will present the updated NAS model elements for review, and the AOV user will edit the data as necessary. Finally, changes to the NAS model will be committed.

Once the NAS model has been updated by the AOV administrator user, other IDA-FS capabilities will continue to function correctly, including analysis of hazards, causes, and controls, as described in other operational capability descriptions above.

5.11 UI

The IDA-FS UI is the system that will permit interaction between the AOV user and the IDA-FS tool. IDA-FS will make use of a Web-based graphical user interface (GUI) to access the tool functions. Specific details and requirements governing the IDA-FS GUI are not defined at the ConOps level; however, general requirements for IDA-FS inputs and outputs have been defined through the operational scenarios. GUI requirements and development will be addressed in later phases of tool development.

The IDA-FS UI must be capable at a minimum of accepting and correctly processing the following inputs from users:

- Select desired IDA-FS function
- Select items of interest
- Select database(s) to query
- Input query keywords
- Input query filters
- Select result sort parameters
- Input remarks
- Edit remarks
- Input NAS system data
- Input SRMD data

The IDA-FS UI must be capable at a minimum of correctly processing and displaying the following outputs to users:

- Display NAS system and interface details
- Display SRMD details
- Display possible stakeholder organizations
- Display results of external database queries
- Display details of query results
- Display monitoring parameters
- Format selected data for reporting

The IDA-FS UI will also allow administrative and maintenance tasks to be performed by authorized users. These tasks include (but are not limited to) managing user accounts and permissions, managing connections to data sources, maintaining internal models and data, and maintaining the IDA-FS software.

6. CONCLUSION

Integrated Domain Assessment of Future Systems (IDA-FS) is intended to support the Air Traffic Safety Oversight Service's (AOV's) decision-making process for Safety Risk Management Document (SRMD) review and high-risk hazard (HRH) control approval in the context of multiple National Airspace System (NAS) changes. IDA-FS uses a model-based approach to pinpoint areas of safety concern attributed to NAS change impacts on other systems, hazards, and risk controls. By identifying interactions and interdependencies among NAS systems and system safety hazards, IDA-FS provides a basis for AOV's evaluation of SRMDs and HRH control approval decisions.

Because current Air Traffic Organization (ATO) Safety Risk Management practices focus on individual NAS changes, SRMDs and associated risk controls do not necessarily consider potential interactions with other changes in the NAS. Examining NAS changes on an individual basis increases the possibility that hazards due to unanticipated consequences of NAS change interactions will not be identified before system deployment. IDA-FS is intended to assist AOV with identifying whether hazards and risks are overlooked or insufficiently mitigated given multiple, overlapping changes in the context of the dynamic and complex NAS environment.

This concept of operations (ConOps) describes AOV user needs for IDA-FS, proposed functional capabilities aligned to AOV needs, and scenarios for user interaction with the tool to accomplish specific objectives when evaluating SRMDs. The ConOps also demonstrates how the tool will allow AOV users to more effectively and efficiently evaluate SRMDs and NAS change impacts by integrating multiple sources of system and safety data into a single platform. Besides AOV's Approval, Acceptance, and Concurrence process, IDA-FS is also expected to support AOV safety oversight activities for audits and safety compliance monitoring. IDA-FS will assist AOV with audit topic planning by identifying systemic hazard causes and critical controls spanning multiple systems and facilities. AOV's compliance monitoring activities are also expected to benefit from the IDA-FS tool that identifies potential ATO Safety Management System compliance deficiencies in terms of high-risk single points of failure and systemic lack of control monitoring.

The ConOps provides a foundation for future IDA-FS research activities to define system requirements and a technical approach for implementing the IDA-FS model and functional capabilities.

7. REFERENCES

1. FAA Order 1100.161, Air Traffic Safety Oversight, Change 1 (2006).

2. FAA Order JO 1000.37, Air Traffic Organization Safety Management System (2007).

3. Air Traffic Organization. (2008). *Safety Management System (SMS) Manual Version 2.1*. Washington, D.C: Department of Transportation.

4. Draft AOV-002-002-WI, AOV Approval, Acceptance, and Concurrence Request Evaluation Work Instruction, March 2013.
5. Approval, Acceptance, and Concurrence (AAC) Enhancements. (2013). AOV Employee Familiarization Briefing. [PowerPoint slides].

6. AOV Connect. (2013). Advanced Knowledge Management Infrastructure. [PowerPoint slides].

7. FAA Report. (2017). Integrated Domain Assessment of Future Systems (DOT/FAA/TC-17/4).

8. SRMD. (2010, March). Terminal ATC with ADS-B and STARS.

9. SRMD. (2009, October). STARS FS-2+ Baseline Update to Include Additional ADS-B IOC Requirements as Described in ECP-028.