DOT/FAA/TC-17/3

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

Integrated Domain Assessment of Future Systems—Taxonomy Development

October 2017

Final Report

This document is available to the U.S. public through the National Technical Information Services (NTIS), Springfield, Virginia 22161.

This document (when published) is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No.

DOT/FAA/TC-17/3

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

INTEGRATED DOMAIN ASSESSMENT OF FUTURE SYSTEMS—
TAXONOMY DEVELOPMENT

5. Report Date

October 2017

6. Performing Organization Code

ANG-E272

7. Author(s)

Nathan Girdner, Ed Snyder, Rod Squellati, and Jennifer Lamont

8. Performing Organization Report No.

9. Performing Organization Name and Address

Systems Enginuity, Inc.
8665 Sudley Rd #349
Manassas, VA 20110

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

DTFACT-11-D-00010

12. Sponsoring Agency Name and Address

U.S. Department of Transportation
Federal Aviation Administration
Aviation Safety – Air Traffic Safety Oversight Service
Washington, DC 20591

13. Type of Report and Period Covered

Final Report

14. Sponsoring Agency Code

AOV-300, Julia Pounds

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 provision of air traffic services. To support its mission, AOV initiated a research effort in fiscal year 2013 to develop a safety review support tool, the Integrated Domain Assessment of Future Systems (IDA-FS). The IDA-FS is intended 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) equipment given the introduction of multiple changes to the NAS. The foundation of the IDA-FS tool is a model and repository of data on NAS system architecture and related system safety hazards. Datasets and classifications for NAS systems and corresponding hazards must be compiled in preparation for defining the IDA-FS model. The purpose of this report is to describe the classification schemas defined for NAS systems, NAS change types, hazards, causes, and controls to enable IDA-FS tool functions. The IDA-FS classification schema maintains traceability to international aviation and FAA safety taxonomies where applicable and makes it possible to group and cross-reference “similar” safety data for comparison of SRMDs of interest to AOV analysts

17. Key Words

AOV, Risk control, Safety risk, NAS, NAS systems, NAS architecture, SMS, SRMD, Hazard, Hazard cause, Control, Taxonomy, Classification

18. Distribution Statement

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)

Unclassified

20. Security Classif. (of this page)

Unclassified

21. No. of Pages

55

22. Price

Reproduction of completed page authorized

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AAC	Approval, Acceptance, and Concurrence
ACCERS	Aviation Causal Contributors for Event Report Systems
ACT	AJI Common Taxonomy
ADS-B	Automatic Dependent Surveillance-Broadcast
AJI	Air Traffic Organization Office of Safety
ANSPS	Air Navigation Service Provider Systems
AOV	FAA Air Traffic Safety Oversight Service
ASAP	Aviation Safety Action Program
ASDE-X	Airport Surface Detection Equipment-Model X
ASR-11	Airport Surveillance Radar Model 11
ATC	Air traffic control
ATO	Air Traffic Organization
ATOP	Advanced Technologies & Oceanic Procedures
CARTS	Common Automated Radar Terminal System
CICTT	International Civil Aviation Organization Common Taxonomy Team
ERAM	En Route Automation Modernization
ETVS	Enhanced Terminal Voice Switch
FSEP	Facility, Service, and Equipment Profile
HMI	Human-machine interface
HW/SW	Hardware/software
ICAO	International Civil Aviation Organization
IDA-FS	Integrated Domain Assessment of Future Systems
JANUS	Joint Analysis System for Air Traffic Control
NAS	National Airspace System
NAS EA	National Airspace System Enterprise Architecture
NEC	Not Elsewhere Classified
NextGen	Next Generation Air Transportation System
NOI	National Airspace System Operational Inventory
NTSB	National Transportation Safety Board
RWSL	Runway Status Lights
SM ICG	Safety Management International Collaboration Group
SMS	Safety Management System
SOP	Safety Order of Precedence
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
STARS	Standard Terminal Automation Replacement System
TFM	Traffic flow management
WG	Working group

EXECUTIVE SUMMARY

Ensuring the safety of the flying public is the FAA's highest priority, and managing safety risks is increasingly important during the transition to the Next Generation Air Transportation System (NextGen). Multiple changes to the National Airspace System (NAS) will take place in the same timeframe as part of NextGen implementation, in which new systems are introduced and air traffic functions become more automated and distributed between ground and airborne systems. Efforts to sustain, replace, and integrate legacy systems with NextGen technologies are also a source of major change within the NAS. All of these changes, including the introduction of new systems and legacy system modifications, cumulatively interact to impact the safety of the NAS.

Whenever the Air Traffic Organization (ATO) proposes a change to the NAS with potential safety implications, a Safety Risk Management Document (SRMD) must be developed. In accordance with the ATO Safety Management System (SMS) Manual, NAS changes must be examined for system safety risk. Initial high risk and high risk discovered within legacy systems must be mitigated to an acceptable level. The ATO prepares SRMDs to describe the safety analysis for a proposed change to the NAS or corrective actions proposed for mitigating high risks.

The FAA Air Traffic Safety Oversight Service (AOV) is responsible for independent safety oversight of air traffic services provided by ATO. As part of AOV's responsibilities described in FAA Order 1100.161 Change 1, AOV reviews ATO SRMDs and approves or rejects controls that are proposed to mitigate high-risk safety hazards. The 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 SMS Manual compliance.

One of the major challenges that AOV faces is that the current ATO Safety Risk Management (SRM) process focuses on individual changes to the NAS, which means that an SRMD and associated risk controls do not always consider potential interactions among multiple NAS changes. Focusing only on individual changes increases the possibility that hazards due to unanticipated consequences of multiple system and NAS change interactions may not be identified before deployment.

To address this shortfall, AOV launched an Integrated Domain Assessment of Future Systems (IDA-FS) research effort. The primary goal of this effort is to develop a decision-making support tool to assist AOV with approving 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 and provide a basis for AOV's evaluation of SRMDs and high-risk hazard controls. Different from other SRM approaches, the IDA-FS is a model-based safety risk analysis tool. The model integrates NAS system and safety hazard information to identify and assess the impacts of changes on interfacing systems, service delivery points, and related hazards and risk controls that rely on specific NAS systems to effectively manage safety risk. The IDA-FS will notify AOV of potential SRMD discrepancies and NAS change impacts as areas of safety concern for further AOV review and oversight actions. In addition to supporting AOV's decision making on the approval of proposed controls to mitigate high-risk hazards, the IDA-FS tool will also support other AOV safety oversight processes, including audits, safety compliance monitoring, and Safety Management Action Review Team activities. The IDA-FS may

additionally be extended to support other AOV AAC activities in which AOV accepts (versus approves) controls spanning multiple FAA lines of business.

The foundation of the IDA-FS tool is a model and repository of data on NAS system architecture and related system safety hazards. Certain IDA-FS functions and outputs rely on this model and repository to cross-reference, compare, and filter NAS equipment (systems) and hazard information. As a result, it is necessary to define a classification scheme for grouping similar equipment and hazard information items within the IDA-FS dataset. The data items that need to be classified are the type of air traffic control (ATC) system equipment, NAS changes, hazards, hazard causes, and controls (both existing and recommended).

The FAA and international aviation groups have undertaken efforts to develop comprehensive safety taxonomies that meet the needs of the aviation community. The IDA-FS classification schema maintains traceability to applicable elements of the Safety Management International Collaboration Group (SM ICG) Hazard Taxonomy and the FAA Air Traffic Organization Office of Safety (AJI) Common Taxonomy. It should be noted that the SM ICG and AJI taxonomies are broad in scope, addressing accidents, incidents, and causal factors beyond ATC equipment hazards, which is the focus of the IDA-FS tool.

The purpose of this report is to describe the classification schemas defined for NAS systems, NAS change types, hazards, causes, and controls to enable IDA-FS tool functions. The IDA-FS classification schema maintains traceability to international aviation and FAA safety taxonomies where applicable, but is not intended to serve as a complete or universal taxonomy of safety data. Instead, the IDA-FS classification schema makes it possible to group and cross-reference "similar" safety data for comparison of SRMDs of interest to AOV analysts. This will enable further development of the IDA-FS model and analysis techniques. This taxonomy development report describes research on aviation safety taxonomies and their suitability for classifying and characterizing IDA-FS data. The proposed IDA-FS classification scheme is presented along with preliminary findings on applying the classification to a sample of 40 SRMDs and 8 systems captured in the IDA-FS dataset.

1. INTRODUCTION

1.1 BACKGROUND

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. The AOV's Approval, Acceptance, and Concurrence 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 (SRM) process focuses on individual changes to the National Airspace System (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 may 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 NAS air traffic control (ATC) equipment-related 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 controls.

The IDA-FS 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. Figure 1 provides an overview of the IDA-FS concept, which includes the following functional objectives:

- Identify Affected NAS Elements—Analyze the interactions among the NAS systems and identify the NAS elements affected by one or more changes to the NAS.
- Evaluate Hazards in SRMDs—Identify SRMDs, hazards, and controls that may be impacted (positively or negatively) by one or more NAS changes addressed in an SRMD.
- Evaluate Effectiveness of Controls—Assist AOV with determining whether proposed controls can be expected to reduce the risk as indicated in the SRMD.
- Maintain SRMD and Model Data—Manage and update the IDA-FS model in response to new or modified SRMDs and NAS changes.

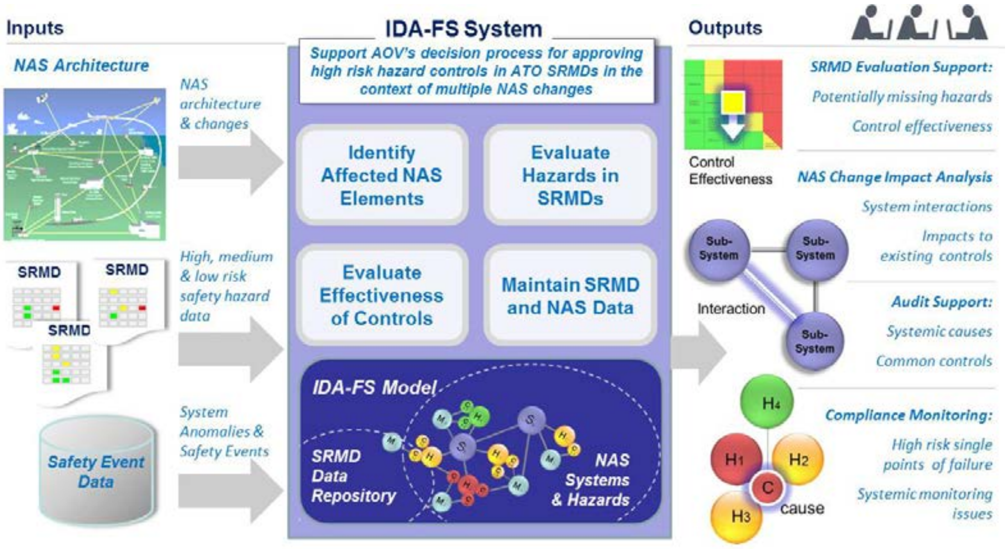
Inputs
NAS Architecture
NAS architecture & changes
SRMD
SRMD
SRMD
High, medium & low risk safety hazard data
Safety Event Data
System Anomalies & Safety Events
IDA-FS System
Support AOV's decision process for approving high risk hazard controls in ATO SRMDs in the context of multiple NAS changes
Identify Affected NAS Elements
Evaluate Hazards in SRMDs
Evaluate Effectiveness of Controls
Maintain SRMD and NAS Data
IDA-FS Model
SRMD Data Repository
NAS Systems & Hazards
Outputs
Control Effectiveness
SRMD Evaluation Support:
Potentially missing hazards
Control effectiveness
NAS Change Impact Analysis
System interactions
Impacts to existing controls
Sub-System
Sub-System
Sub-System
Interaction
Audit Support:
Systemic causes
Common controls
H4
H1
H2
C
H3
cause
Compliance Monitoring:
High risk single points of failure
Systemic monitoring issues

Figure 1. The IDA-FS concept overview

As shown in figure 1, the IDA-FS model constitutes the foundation of the tool, enabling functions to evaluate NAS change impacts, hazards, and risk-control effectiveness. The model includes a repository of SRMD data and NAS systems linked to hazards and corresponding causes and mitigations in a form that can be queried and analyzed. To establish and maintain this model, IDA-FS assembles NAS architecture information, system safety hazard data, and system anomalies and safety events in which NAS systems are identified as a contributing factor. As the NAS evolves, system architecture changes and supporting SRMDs are used to update the IDA-FS model.

Certain IDA-FS functions will require cross-referencing, comparing, and filtering NAS equipment (systems) and hazard information. For example, the IDA-FS function to "Evaluate Hazards in SRMDs" entails comparing one SRMD's hazards to similar hazards related to historical NAS changes to identify potentially missing hazards. To enable this comparison, NAS changes and hazards must be classified according to a common scheme. Another IDA-FS tool function identifies systemic hazard causes and the most prevalent or common controls. To do so, causes and controls must be grouped and sorted according to their respective types, particularly because SRMDs often express the same or similar hazard elements in different ways. The IDA-FS function to "Evaluate Effectiveness of Controls" also requires a standardized classification scheme for describing risk controls. Besides cross-referencing historical risk controls, a classification scheme that identifies controls according to their Safety Order of Precedence (SOP) may be used to characterize control effectiveness in mitigating risk. To enable these and other IDA-FS tool functions, a standardized classification scheme must be applied to the IDA-FS dataset to ensure that systems, NAS change types, hazards, causes, and controls are consistently described and grouped.

1.2 PURPOSE

The purpose of this report is to describe the research and selection of classifications for NAS system architecture and related SRMD information captured in the IDA-FS dataset. The classification scheme is intended to enable IDA-FS functions that require cross-referencing, comparing, and filtering NAS equipment (systems) and hazard information. The data items that need to be classified are the type of system, the type of NAS change, hazards, hazard causes, and both existing and recommended controls.

The purpose of the IDA-FS classification effort is to adequately describe and group data in SRMDs that have been captured in the IDA-FS dataset. This will allow for further development of the IDA-FS model and analysis techniques. It is anticipated that the data may be mapped to additional or alternative taxonomies at a later date to facilitate greater searching or analysis.

Note that this classification effort is not intended to serve as a common or universal taxonomy of safety data. The FAA and other international aviation groups have undertaken efforts to develop comprehensive, universal taxonomies that meet the broad needs of the aviation community, such as identifying accident causal factors and aviation safety trends. Instead, this IDA-FS classification effort is intended to fulfil the functional requirements of the IDA-FS tool.

1.3 DEFINITIONS

Definitions for the following terms used throughout this report are from FAA Order 1100.161 Change 1, Air Traffic Safety Oversight [1], unless otherwise noted:

- 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.
- Cause—Any events occurring independently or in combination that result in a hazard or failure. Causes include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.
- 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.
- NAS Change—Per the ATO SMS Manual, any change to or modification of airspace; airports; aircraft; pilots; air navigation facilities and ATC facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components. For IDA-FS purposes, NAS changes related to Air Traffic Organization (ATO) NAS equipment are the primary focus of this research effort.

1.4 DOCUMENT STRUCTURE

Section 2 describes existing research on aviation-safety taxonomies. The notable features of various taxonomical structures and their applicability to the IDA-FS effort are discussed. Section 3 describes the classification scheme for the IDA-FS model data. Each type of classified data is discussed, and the resultant classification schema is described. Section 4 discusses the application of the classification to the IDA-FS dataset compiled on NAS system equipment and related SRMDs. Section 5 summarizes issues and findings discovered during the classification development and possible refinements that may be made to the classes at a later date. Appendix A shows a case study on SRMD classification that demonstrates the application of the classification categories to data from an actual SRMD in the IDA-FS dataset.

2. OVERVIEW OF EXISTING TAXONOMIES

An overview of aviation safety taxonomies is presented in this section. Elements of these taxonomies that are applicable to IDA-FS are highlighted and discussed. Note that most of these taxonomies focus on aviation accident or incident event sequences and their primary causes and do not necessarily break down ATC equipment contributions to the event. The IDA-FS classification work is not intended to replace existing taxonomy work, but to adapt a framework to allow for consistent grouping of relevant safety data from SRMDs produced by ATO.

2.1 SAFETY MANAGEMENT INTERNATIONAL COLLABORATION GROUP HAZARD TAXONOMY

The Safety Management International Collaboration Group (SM ICG) includes representatives from the European Aviation Safety Agency, the U.S. FAA Aviation Safety Organization, the International Civil Aviation Organization (ICAO), and Transport Canada Civil Aviation. The purpose of the group is to promote a common understanding of SMS principles and requirements and to facilitate their application across the aviation community. To this end, the SM ICG began developing a common hazard taxonomy to promote improved analysis of hazards and to facilitate sharing of hazard information in the aviation community. [2]

The working group (WG) began their taxonomy-development process in 2009 by creating high-level categories of hazards. The categories were intended to capture the nature of hazards rather than specific impacts that hazards may have on aviation systems. According to the SM ICG Safety Management Terminology document, a hazard is defined as a “condition that could cause or contribute to an aircraft incident or accident.” [3]

The WG defines four broad hazard categories, including:

1. Organizational–Management or documentation, processes, and procedures.
2. Environmental–Weather, geography, or wildlife.
3. Human–Limitations of the human that, in the system, has the potential for causing harm:

    a. Medical condition
    b. Human performance limitations
    c. Human factors related to design, manufacturing, maintenance, and operations
    d. Psychological factors
    e. Cognitive tasks

4. Technical–Operations and processes involving personnel or equipment in each environment:

    a. Aerodrome
    b. Air Navigation
    c. Operations
    d. Maintenance
    e. Design & Manufacture

In 2013, the WG published a paper of examples to illustrate hazards that fit in each category [4]. Subcategories were described for each of the four categories to guide civil aviation authorities that are in the initial stages of safety management development and implementation. The hazard taxonomy developed by the SM ICG is not binding on any organization but is proposed as a way to improve sharing of hazard data among various organizations and entities involved in aviation safety around the world.

The classification schema developed for IDA-FS as described in section 3.2.3 is compliant with the broad hazard categories defined by the SRM ICG, as shown in table 1. The ATO equipment-related SRMDs include "Process" hazards that are related to the SM ICG's "Organizational" hazards. For example, ATO equipment-related SRMDs examined include hazards for system implementation, installation, and testing process and procedural faults. Though the ATO SMS scope does not include environmental hazards, system operating environment conditions, such as weather or traffic density, are recognized in the SMS as hazard causes or system state elements. Accordingly, the IDA-FS classification scheme includes weather among other environmental hazard causes. The SM ICG "Human" hazard category corresponds to the IDA-FS classifications for human-related hazards and hazard causes and risk controls involving training. Finally, the SM ICG's "Technical" hazard category is represented by equipment and process hazards and causes in the IDA-FS classification scheme.

Table 1. The SM ICG mapping to IDA-FS classifications

SM ICG Hazard Classes	IDA-FS Classifications		
	Hazard	Cause	Control
Organizational	Process	Process	Procedures
Environmental	N/A	Environmental	N/A
Human	Human	Human	Training
Technical	Equipment and Process	Equipment and Process	Design, Safety Devices, Warnings

2.2 NATIONAL TRANSPORTATION SAFETY BOARD CAUSAL CODE

The National Transportation Safety Board (NTSB) is tasked with investigating aviation accidents and incidents in the United States. Investigations are performed by the NTSB to determine the probable cause(s) for accidents and to make recommendations intended to reduce future accidents. The NTSB has developed a hierarchy of incident causal factors used to classify the results of their investigations. The NTSB accident investigation database [4] contains approximately 20,000 incidents classified by such parameters as event type, phase of flight, primary cause, and other contributing factors [5].

The causal code structure breaks down aircraft incident causes into the following five categories:

1. Aircraft
2. Personnel
3. Environmental

4. Organizational
5. Not Determined

Each category has subcategories, sections, subsections, and modifiers (descriptors).

A cross-database analysis of aviation incidents was performed by Nazeri in 2007 [6], including the NTSB accident database and associated accident cause taxonomy. The paper described the causal code structure as encoding accident causes in one of four categories:

1. Non-people oriented (e.g., aircraft, ATC, facility, terrain, weather)
2. People-oriented (e.g., human factors)
3. Direct underlying (e.g., fatigue, inadequate training)
4. Indirect underlying (e.g., insufficient standards/requirements)

This hierarchy of causal codes does not address any ground-based equipment but is instead focused on causal factors related to aircraft equipment, operators, and personnel. As a result, the taxonomy is not well-suited for classification of hazard causes in ATC equipment-related SRMDs. However, the IDA-FS classification scheme chosen for hazard causes, as described in section 3.2.4, approximately corresponds to the four top-level classes.

2.3 AVIATION SAFETY ACTION PROGRAM CAUSAL CONTRIBUTORS TAXONOMY

Krokos et al. [7] present a methodical approach to developing a taxonomy based on an exhaustive classification of Aviation Safety Action Program (ASAP) reports and expert inputs. The authors performed an extensive review of ASAP incident reports to develop a taxonomy of causal factors. The focus of this taxonomy is to classify and characterize incidents and accidents from a pilot/air carrier perspective. Causal factors were classified according to two levels. The first-level categories are:

- Policies or Procedures
- Human Error
- Human Factors
- Organizational Factors
- Hardware
- Weather or Environment
- Airspace or ATC

The formal name for the resultant taxonomy is Aviation Causal Contributors for Event Report Systems (ACCERS). All the top-level categories are addressed in the IDA-FS cause classification, except for “Organizational Factors.” Organizational hazards are not generally addressed in equipment-related SRMDs from ATO, and none of the causes in that category appear in any of the ATO SRMDs reviewed to date. Because the focus of ACCERS is on incidents and accidents from a pilot/air carrier perspective, it provides no detail on or granularity in its categorization of ATC equipment-related causes. The “Hardware” category addresses only aircraft equipment, and the “Airspace or ATC” category addresses only the clearances given by ATC, not the equipment-related causal factors that might produce incorrect clearances. For these reasons, it was not selected as a template for IDA-FS hazard-cause classification.

2.4 THE FAA ATO OFFICE OF SAFETY COMMON TAXONOMY

The FAA ATO Office of Safety (AJI) is developing a common taxonomy to describe and classify a wide range of data related to aircraft accidents, incidents, and loss of separation events. Similar to NTSB Cause taxonomy, the AJI Common Taxonomy (ACT) breaks down and describes incidents and events that are of interest to ATO (i.e., occurrences). The occurrences and events that were analyzed to produce the AJI-specific taxonomy are based on the Mandatory Occurrence Reporting types. The occurrence categories in the ACT are:

- Airborne Separation
- Surface Separation
- Terrain/Obstruction
- Airspace/Altitude/Route/Speed
- Airport Environment
- Communication
- Emergency
- Inquiry

These occurrence categories describe incidents and events, but not the causal factors and contributors to the event. This led to the classification of aviation occurrence causes into the following Domains and Disciplines (elements and sub-elements are not shown for brevity):

- Individual/Human Factors (an individual's performance related to their environment):

  – Experience/Knowledge
  – Perceptual
  – Physical/Sensory
  – Procedural/Task Performance
  – Psychological
  – Fatigue
  – Human/Individual Not Elsewhere Classified (NEC)

- Organizational Factors (oversight, support, and monitoring of programs, policies, personnel):

  – Oversight
  – Operational Planning/Scheduling/Resource Management
  – Policy/Procedures
  – Culture
  – Training Program
  – Documentation/Record Keeping
  – Enforcement
  – Safety Program
  – Organizational Factors NEC

- Equipment Factors (malfunctions, flaws, or inoperative equipment)
  - Aircraft
  - Air Navigation Service Provider Systems (ANSPS)
  - Equipment Factors NEC

- Operating Environment Factors (system states and circumstances influencing flight and ATC)
  - Infrastructure
  - Weather
  - Special Events
  - Emergencies
  - Operating Equipment NEC

Certain elements of the ACT are applicable to the IDA-FS tool, which is focused on ATC equipment-related safety hazards. Specifically, the ACT describes ANSPS equipment factors that identify hazard or failure conditions associated with air traffic equipment. Table 2 outlines the ACT elements and definitions applicable to the IDA-FS research scope. Other elements in the ACT related to Human and Environmental factors also apply to air traffic equipment-related SRMDs and are captured at a broad level in the IDA-FS classification scheme.

Table 2 The ACT mapping to IDA-FS classifications

ACT1 No. & Description	AJI's Definition	IDA-FS Classifications
10.01 Installation	Installation of ATC equipment contributes to an undesired outcome.	Installation faults
10.02 Malfunction	Unscheduled or unexpected equipment malfunction contributes to an undesired outcome. Note that AJI's lower-tier subcategories for 10.02 cite failure-hardware, failure-software, corruption-hardware, incorrect adaptation, system failure, etc.	Partial loss or failure of system functions Total loss or failure of system Missing or incomplete data Inaccurate or misleading data or function HW/SW/function failure HW/SW/function fault Interface failure/fault
10.03 Outage	Scheduled shutdown or scheduled maintenance contributing to an undesired outcome. Equipment was unavailable because of a pre-coordinated outage.	<No examples identified in initial IDA-FS dataset. May be added in the future.>
10.04 Coverage	Equipment coverage that does not meet operational needs, which contributes to an undesired outcome.	System design/development flaw Installation fault Adaptation/configuration errors Note that coverage and other system performance characteristics are treated as an aspect of system design and implementation.
10.05 Equipment / Automation Type	Type of equipment/automation that caused/contributed to an undesired outcome.	Note that NAS system equipment is classified according to the NAS Enterprise Architecture and Facility Service and Equipment Profile, which includes Automation equipment.
10.06 Automation Anomaly	Automation deviation that is outside the expected norm, which contributes to an undesired outcome.	See note above.

HW/SW = hardware/software

Table 2 The ACT mapping to IDA-FS classifications (continued)

ACT1 No. & Description	AJI's Definition	IDA-FS Classifications
10.07 Layout/Placement	Equipment's physical arrangement within the operation contributes to an undesired outcome.	Installation fault
10.08 Design	Physical construction of an equipment interface to a human contributes to an undesired outcome.	System design/development flaw
10.09 Access/Availability	Inability to use an existing piece of equipment because of temporary physical location, or conflicting use contributes to an undesired outcome.	System interoperability flaw Installation fault
10.10 Safety Alert Malfunction	Unscheduled or unexpected safety alert malfunction contributing to an undesired outcome.	Note that NAS system equipment is classified according to the NAS Enterprise Architecture and Facility Service and Equipment Profile, which includes Safety Alerting equipment.
10.11 Safety Alert Equipment	Specific safety alerting equipment that causes or contributes to an undesired outcome.	See note above.
10.12 Testing	Equipment testing causes or contributes to an undesired outcome.	Testing issues
10.13 Not Used	N/A	N/A
10.14 HMI & Support Systems	HMI problems contributes to an undesired outcome.	System design/development flaw HW/SW/function failure HW/SW/function fault Interface failure / fault
10.15 Adaptation	Not defined.	Adaptation/configuration errors

HW/SW = hardware/software; HMI = human-machine interface

2.5 THE ICAO AVIATION COMMON TAXONOMIES

The Commercial Aviation Safety Team/International Civil Aviation Organization Common Taxonomy Team (CICTT) developed common taxonomies and definitions for aviation-accident and incident-reporting systems. The CICTT includes experts from several air carriers, aircraft manufacturers, engine manufacturers, pilot associations, regulatory authorities, transportation safety boards, ICAO, and members from Canada, the European Union, France, Italy, the Netherlands, the United Kingdom, and the United States.

To accomplish its objectives, CICTT developed and maintains the following standard taxonomies [8]:

- International standard for aircraft make, model, and series groupings
- International standard for engine make, model, and sub-model groupings
- Human factors classifies human factors causal factors in incidents/accidents
- Aviation occurrence categories (taxonomy of incident/accident/events)
- System/Component Failure or Malfunction (Powerplant) subcategory
- Phase of flight
- Positive taxonomy (corrective actions taken to address hazards)

The taxonomies being developed by CICTT may be made available on their completion. The majority of these taxonomies do not apply directly to the data being classified in IDA-FS. The "Positive" taxonomy of corrective actions might be of use to IDA-FS in the future, but it was unavailable for review during the preparation of this report.

2.6 THE NAS ENTERPRISE ARCHITECTURE MID-TERM AND FAR-TERM SAFETY OVERLAYS

As part of the National Airspace System Enterprise Architecture (NAS EA) modeling effort, the FAA Next Generation Air Transportation System (NextGen) Office has developed safety overlays to characterize the primary hazard categories of concern during NextGen transition and implementation. Seven categories of catastrophic hazards are identified in these overlays:

- Separation Assurance
- Flight Planning
- Navigation
- ATC Advisories-Weather
- Aeronautical Information
- ATC Advisories-NAS Status
- Emergency & Alerting

The focus of these safety overlays is on catastrophic hazards and the types of systems and anomalies that are most likely to produce those hazards. This scope is more limited than that of IDA-FS, because the IDA-FS tool is intended to capture NAS equipment-related hazards at all identified risk levels. The categories identified by the NAS EA safety overlays will fit into the hazard classification categories developed for IDA-FS.

2.7 JOINT ANALYSIS SYSTEM FOR ATC

The Joint Analysis System for Air Traffic Control (JANUS) is an integrated approach to identify human error risk factors in ATC incidents. JANUS was developed jointly by the FAA and EUROCONTROL and is intended to harmonize the Human Factors Analysis and Classification System and the Human Error Reduction in Air Traffic Management techniques [9]. It gives a classification of conditions and contributing factors to incidents and hazards from an ATC perspective. The broad categories of causes are as follows:

- Contributing Conditions:

  - Organization
  - Management
  - Supervision

- Contextual conditions:

  - Team/relational interactions
  - System state/environmental conditions

- Controller Performance:

  - Task descriptions
  - Mental processes
  - Non-compliance issues

JANUS is particularly focused on human factors and incident causes related to human performance. As such, it is not broad enough to classify the range of hazards and hazard causes captured in ATC equipment-related SRMDs. There is, however, a “Human factors” class in the IDA-FS hazard-cause schema. This class could later be decomposed according to the JANUS taxonomy for IDA-FS searching, sorting, and querying. The hazard causes identified as “Human factors” could be sub-categorized according to the JANUS classes, though subject matter expert input might be required to ensure completeness and accuracy.

2.8 THE ATO SMS MANUAL

The ATO SMS manual is the handbook that provides guidance to ATO personnel on the process of identifying hazards and mitigating risk in the NAS. The current version of the SMS manual is 2.1, though version 4.0 is in development and expected to be released in 2014 [10, 11]. The ATO SMS manual does not provide any taxonomies or classifications of safety data or specific guidance regarding the selection of taxonomies. It does, however, provide a process and framework for identification and analysis of hazards related to NAS changes. Because SRMDs must comply with SMS manual provisions, the SMS framework for hazard identification is suitable for classifying hazards in the IDA-FS dataset.

In developing a framework to classify hazards and hazard causes for IDA-FS, guidance from the ATO SMS manual version 2.1 and draft version 4.0 were reviewed and considered. The ATO SMS manual recommends that safety practitioners use the “5M model” to describe the system and NAS change. The 5 M’s are:

1. Mission–The clearly defined and detailed purpose of the change proposal or system/operation being assessed.
2. (hu)Man/Person–The human operators, maintainers, and affected stakeholders.
3. Machine–The equipment used in the system, including hardware, firmware, software, human-to-system interfaces, system-to-system interfaces, and avionics.

4. Management–The procedures and policies that govern the system's behavior.
5. Media–The environment in which the system is operated and maintained.

The 5M model is used to fully describe the change and to identify elements that are part of or affected by the proposed change. These elements are used by the Safety Risk Management Panels to help identify hazards, hazard causes, and mitigations. Therefore, it is logical to consider the 5M model as a framework for classifying the hazards, hazard causes, and mitigations identified in SRMDs.

A hazard is defined as 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 prerequisite to an accident or incident. Hazards often arise from/are propagated by deficiencies or failures in one or more of the parts of the 5M model. Because of this, IDA-FS may use the 5M model to classify both hazards and hazard causes identified in ATO SRMDs.

The draft ATO SMS Manual 4.0 Section 3.4.6 describes potential sources of hazards. It states, "The hazard identification stage considers all possible causes of hazards. Depending on the nature and size of the system under consideration, these could include:

- NAS equipment failure/malfunction,
- Operating environment (including physical conditions, airspace, and air route design),
- Human operator failure/error,
- Human-machine interface (HMI) problems,
- Operational procedures limitations/design,
- Maintenance procedures limitations/design, and
- External services

This guidance provides a starting point for classifying hazard causes. Each of these types of hazard causes also fit within the 5M model. "Machine" encompasses equipment failures; malfunctions both within the system and from external services; and some aspects of HMI. "Man" encompasses human operator and HMI issues. "Media" encompasses causes related to the operating environment and some external services, and "Management" addresses operational and maintenance procedure limitations and design issues.

The ATO SMS Manual (and other generally accepted SMS guidance) describes hazard controls according to the SOP. The SOP describes four categories of safety risk mitigations by order of effectiveness and desirability. The four levels of the SOP are:

1. Design for Minimum Risk—Eliminate hazards wherever possible/incorporate design choices that minimize the likelihood of hazards occurring.
2. Incorporate Safety Devices—Design and incorporate devices to prevent, interrupt, or detect a hazard
3. Provide Warnings—Provide alerts, alarms, announcements, and reminders of unsafe conditions to minimize the likelihood of inappropriate human reaction and response.
4. Procedures or Training—Develop processes to minimize human errors and ensure that users are trained in their application and execution.

These four categories provide a high-level framework for classifying hazard mitigations, both existing and recommended controls. These categories can be further decomposed for greater granularity, as described in section 3.2.5.

These mitigation classes could also be mapped to the 5M model, as shown below:

- Mission → Design
- (hu)Man/Person → Training
- Machine → Design, Safety Devices
- Management → Training
- Media → Warnings

3. CLASSIFICATION DEVELOPMENT APPROACH

3.1 THE IDA-FS DATASET

Datasets for NAS systems and corresponding hazards have been developed in preparation for defining the IDA-FS model. The NAS system architecture and related SRMD information for selected systems has been collected from a variety of sources to thoroughly characterize the systems. The eight systems selected for initial IDA-FS study are the Standard Terminal Automation Replacement System (STARS), Common Automated Radar Terminal System (CARTS), En Route Automation Modernization (ERAM), Advanced Technologies & Oceanic Procedures (ATOP), Airport Surface Detection Equipment-Model X (ASDE-X), Enhanced Terminal Voice Switch (ETVS), Airport Surveillance Radar Model 11 (ASR-11), and Runway Status Lights (RWSL).

The IDA-FS dataset compiles information on NAS systems and ATC equipment-related SRMDs, including:

- System Architecture—System descriptions, first-tier subsystems, and internal and external system interfaces.
- Safety Analysis Information—System hazard descriptions, causes, existing and recommended controls, initial and predicted residual risk (severity and likelihood), and control monitoring activities.
- SRMD Attributes—NAS system(s) addressed in the SRMD (i.e., the scope of the NAS change), applicable Safety Management System (SMS) Manual version, and SRMD reference information (i.e., title, version, date).

The results of the initial IDA-FS dataset development effort are summarized in the previously submitted report titled "IDA-FS Model Dataset Development Report." Since the completion of the IDA-FS Dataset report on December 15, 2013, work has continued to capture and characterize safety and system data on the eight key systems selected for the IDA-FS prototype. The data captured on these systems and addressed in the IDA-FS classification scheme for this report include 40 SRMDs, 226 hazards, 604 hazard causes, 1003 existing controls, and 339 recommended controls. Table 3 shows the distribution of data items across the eight systems selected for IDA-FS Phase II research.

Table 3. The IDA-FS dataset summary

System	SRMDs	Hazards	Causes	Existing Controls	Recommended Controls
ASDE-X	3	12	25	34	4
ASR-11	8	32	50	96	60
ATOP	4	8	10	15	4
CARTS	6	16	22	101	36
ERAM	7	48	144	204	42
ETVS	1	3	3	4	0
RWSL	4	72	198	213	158
STARS	8	35	152	336	35
Totals	40	226	604	1003	339

The IDA-FS dataset was used to guide the development of classification categories and to validate that the classes selected for the IDA-FS tool adequately describe the actual system and safety data. Analysis of this data provided the initial groupings for the IDA-FS data classes. These initial groups were defined, consolidated, and refined to produce the classes reported in Section 3.2.

3.2 DATA ITEMS NEEDING CLASSIFICATION

3.2.1 NAS Systems

The NAS EA reports define a multilevel hierarchy of the NAS so that the total NAS system can be examined and functional interrelationships can be followed. The NAS EA Systems Interface Description (SV-1) describes the NAS in terms of elements, sub-elements, and sub-systems. Figure 2 shows the partitioning of the NAS into element and sub-element levels [12].

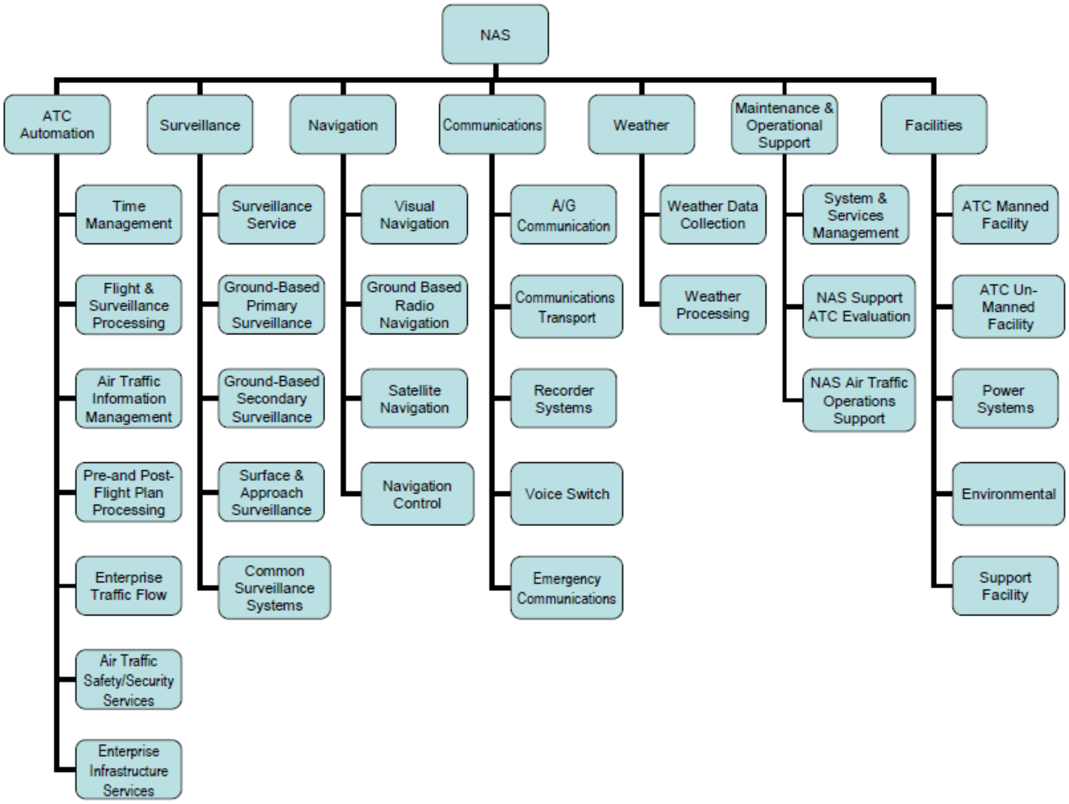
NAS
ATC Automation
Surveillance
Navigation
Communications
Weather
Maintenance & Operational Support
Facilities
Time Management
Flight & Surveillance Processing
Air Traffic Information Management
Pre-and Post-Flight Plan Processing
Enterprise Traffic Flow
Air Traffic Safety/Security Services
Enterprise Infrastructure Services
Surveillance Service
Ground-Based Primary Surveillance
Ground-Based Secondary Surveillance
Surface & Approach Surveillance
Common Surveillance Systems
Visual Navigation
Ground Based Radio Navigation
Satellite Navigation
Navigation Control
A/G Communication
Communications Transport
Recorder Systems
Voice Switch
Emergency Communications
Weather Data Collection
Weather Processing
System & Services Management
NAS Support ATC Evaluation
NAS Air Traffic Operations Support
ATC Manned Facility
ATC Un-Manned Facility
Power Systems
Environmental
Support Facility

Figure 2. Basic NAS hierarchy structure

According to this structure, the NAS is broken into seven high-level categories (elements): ATC Automation, Surveillance, Navigation, Communications, Weather, Maintenance & Operational Support, and Facilities. Each element contains sub-elements that further refine the purpose or function within the NAS Element. All NAS systems, equipment, and facilities under the purview of ATO can then be classified under one of these sub-element headings.

The NAS EA hierarchy closely parallels the structure used by the Facility, Service, and Equipment Profile (FSEP) program. The FSEP is a standardized profile and inventory of the physical components of the NAS and is governed by FAA Order 6000.5D [13]. The FSEP order defines the National Airspace System Operational Inventory (NOI), which clarifies the NAS operational infrastructure. The NOI is organized into seven capabilities and five categories. The capabilities are Automation, Communication, Navigation, Surveillance, Weather, Infrastructure, and Mission Support. The categories tracked by NOI are Facilities, Systems, Subsystems, Equipment, and National Airspace Performance Reporting System Services.

Each facility and service in the NAS is assigned an FSEP code that describes key pieces of data, including its capability and category; location; and status. These codes can be used to look up monitoring data via the FAA’s Technet website (http://technet.faa.gov). Mapping these codes to systems in the IDA-FS dataset may allow the IDA-FS tool to use the monitoring data to extrapolate system issues or reliability statistics as part of its analysis.

Table 4 shows the NAS EA element and Sub-element classifications and the FSEP codes for each of the systems captured in the initial IDA-FS dataset. The range of codes is captured and described where multiple variants of a system are tracked in FSEP..

Table 4. The FSEP classification codes

System	NAS EA Element; Sub-Element	FSEP Code	FSEP Code Description
CARTS	ATC Automation; Flight & surveillance processing	AA01A	ARTS IIIE with AP-1
		AA02A	ARTS IIIE with PPC
		AA04A	ARTS IIIE with AP-2–N90 only
ASR-11	Surveillance; Ground-based primary surveillance	53AHA	ASR-11 Digital
		SC00A	ASR-11 Military GPN-30
ATOP	ATC Automation; Flight & surveillance processing	AC00 (A / B / C)	ATOP Hardware
ERAM	ATC Automation; Flight & surveillance processing	AK00A	ECG-U
ETVS	Communication; Voice switch	48HB (A-H, J-L)	ETVS
RWSL	Navigation; Visual navigation	NJ00A	RWSL System
STARS	ATC Automation; Flight & surveillance processing	02FV(E, F)	STARS w/G1
		AX00(E, F)	STARS w/G2
		AX01(E, F)	STARS w/G4
		AX02D	STARS LITE
		AX03(E, F)	STARS ELITE
ASDE-X	Navigation; Surface and approach surveillance	SA04(K-N, Q-T)	ASDE-X with Data Distribution
		SA06N	ASDE-X with Data Distribution and PRM-A

ARTS IIIE = Automated Radar Terminal System Model IIIE; AP = ARTS Processor; ECG = EnRoute Communication Gateway Upgrade; ELITE = Enhanced Local Integrated Tower Equipment; LITE = Local Integrated Tower Equipment; PRM-A = Precision Runway Monitor – Advanced; PPC = Power PC

3.2.2 The NAS Change Types

SRMDs are written in response to a change to the NAS, which may include a new system, the expanded deployment of a system, a system modification, or the removal of a system. These NAS changes take place over various system life-cycle phases, as shown in figure 3 from the FAA's Acquisition System Toolset [14]. Table 5 maps each life-cycle phase to one or more NAS change types applicable to the SRMDs sampled for the IDA-FS dataset that includes eight NAS systems.

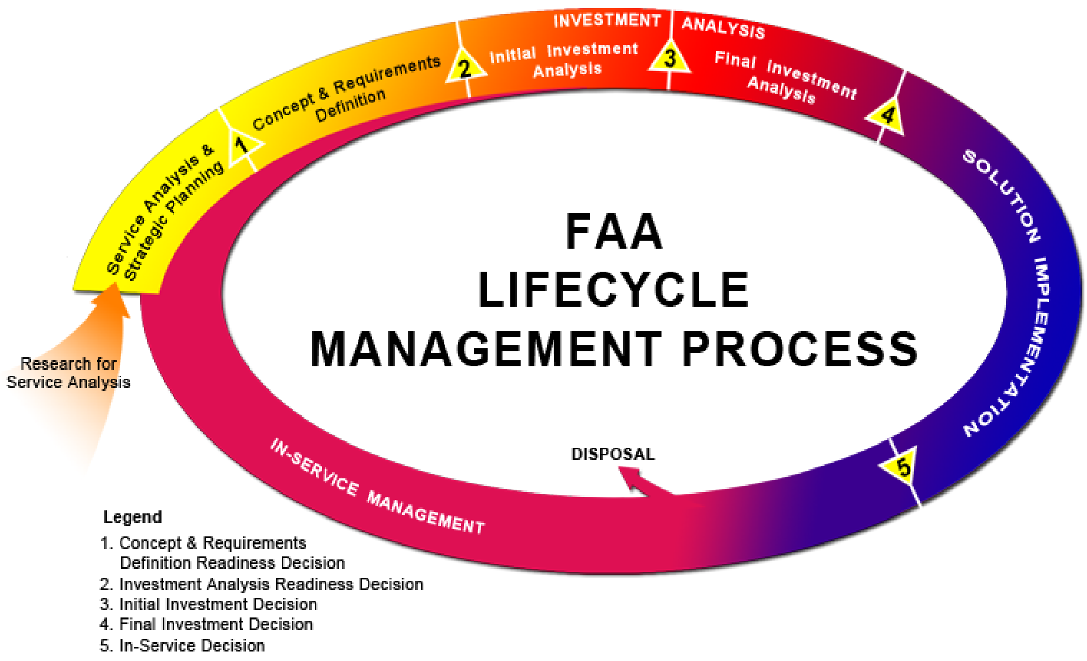
INVESTMENT
ANALYSIS
Service Analysis & Strategic Planning
1
Concept & Requirements Definition
2
Initial Investment Analysis
3
Final Investment Analysis
4
SOLUTION IMPLEMENTATION
5
FAA LIFECYCLE MANAGEMENT PROCESS
DISPOSAL
IN-SERVICE MANAGEMENT
Research for Service Analysis
Legend
1. Concept & Requirements Definition Readiness Decision
2. Investment Analysis Readiness Decision
3. Initial Investment Decision
4. Final Investment Decision
5. In-Service Decision

Figure 3. The FAA life-cycle phases

Table 5. The NAS change types by FAA lifecycle phase

Change Type Lifecycle Phase	New System Acquisition/Development	Modification	Deployment/Installation	Decommissioning/Removal	Deviation	New/Modified Mission or Application
Service Analysis & Strategic Planning	X					
Concept & Requirements Definition	X				X	X
Initial-Final Investment Analysis	X				X	
Solution Implementation	X	X	X		X	X
In-Service Management		X	X		X	X
Disposal				X		

Using the system life-cycle phases as a framework, SRMDs were grouped by the type of NAS change described and mapped to one or more life-cycle phases. Based on this approach, six classes were identified. Table 6 shows the classes selected to describe the NAS change types for IDA-FS.

Table 6. The NAS change classification

NAS Change Type	Definition	Example
New system acquisition/development	NAS changes related to the development/acquisition of a new NAS system. May include key site activities, testing, system integration, etc.	SRMD ATO0T-CARTS-1065 assesses the safety of adding Automatic Dependent Surveillance-Broadcast functionality to CARTS at Louisville International (SDF) Airport via a future CARTS revision.
System modification	NAS changes related to system improvements, updates, corrective actions, technology refreshes, upgrades, or addition or removal of system interfaces. Subclasses include: • Hardware or software modifications • Adaptation changes • New or modified system interfaces • Integration of systems • Upgrades • Technology refresh • Form-fit-function replacement	ASR-11_TR2_OSA SRMD assesses the safety of the ASR-11 Tech Refresh Phase 2 program to address shortfalls created by part obsolescence issues; unreliable or incomplete fault monitoring/fault isolation results; stability; and site Uninterruptable Power Supply maintenance issues.
System deployment/installation	NAS changes related to the installation of a system/ the deployment of an existing system to additional locations beyond baseline plans.	Los Angeles International Airport (LAX) RWSL Final version 3.0 assesses safety of installing RWSL, including Runway Entrance Lights and Takeoff Hold Lights at LAX, based on more than 3 years of extensive testing at the Dallas Fort Worth (DFW) Airport.
System decommissioning/removal	NAS changes related to the decommissioning of a system, including removal of a system from a facility or the entire NAS.	Not applicable.

Table 6. The NAS change classification (continued)

NAS Change Type	Definition	Example
System deviation from equipment safety standards	NAS changes requesting approval to deviate or waive FAA safety standards for equipment design, development, installation, test, operation, and/or maintenance. Not a change to the system, but a change or waiver in technical/safety standards.	ASDE-X FAA-STD-19E Deviation SRMD Version 1.4–Deviation from grounding requirements by placing ASDE-X multilateration System Remote Unit antennas on low impact resistant fiberglass masts.
New/modified mission or application for existing system	NAS changes requesting approval to modify the way that a system is used; expanding or reducing its mission; or the environment in which it may be used. Not a change to equipment, but may include adaptation/procedural changes.	ASR-11 SRMD v1.0 to allow 3 NM separation between the specified limit of 40 NM limit of the radar antenna and 60 NM. Changes make ASR-11 standards consistent with standards for ASR-9 with a Mode Select (Mode S) secondary radar system, which allows, as per paragraph 5-5-4 in 7110.65, for the application of Terminal Area Separation Minima of 3 NM out to a range of 60 NM from its antenna.

3.2.3 Hazards

The classification of hazards for IDA-FS began with a thorough review of all hazards captured to date in the IDA-FS dataset. Through manual review and grouping, a number of potential classes emerged. At the broadest level, potential system failures or hazards related to new systems can be broken down into the following categories:

- Failure or loss of system functionality
- System malfunction
- Human factors in understanding or using a system
- Errors in system testing and evaluation
- Air traffic environment disruption (e.g., due to equipment installation)

These potential classes were then grouped according to their best fit within the 5M model described in section 2.8. Table 7 shows the proposed hazard classifications for IDA-FS. There are three high-level classes consistent with elements of the SM ICG Hazard Taxonomy and FAA ACT: “Equipment,” “Process,” and “Human.” The definition for each sub-class and an example from the IDA-FS dataset are also provided.

Table 7. Hazard classification

Hazard Class Name	Definition	Example
Equipment		
Partial loss or failure of system functions	One or more functions of the system are lost or unavailable, but the overall system is operating.	CARTS malfunction results in complete loss of Primary Surveillance Radar to controller, but Secondary Surveillance Radar, which operates of the aircraft transponder, remains available.
Total loss or failure of system	More than one functions of the system fail or are unavailable such that the system is inoperative or unavailable.	Hardware or software failure that renders ATOP inoperative.
Missing or incomplete data	Data inputs or outputs are missing or incomplete, though the system continues to operate. The missing or incomplete data may or may not be detected through automated means or manual human observation.	The displayed ERAM flight data block has missing fields.
Inaccurate or misleading data or function	Source data or processing produces incorrect, confusing, or misleading data to the user. Includes mis-timed functions and latency issues that do not result in function/system failure.	False activation of Runway Entrance Lights component of RWSL.
System interoperability fault	Flaw or inconsistency in the planning or implementation of systems such that those systems may not work together correctly to safely carry out their intended functions. Addresses inconsistencies between systems that provide similar functions or that use the same data with different processing.	Misalignment of radar with ASDE-X causes target jump on short final for the runway affecting RWSL light activations.

Table 7. Hazard classification (continued)

Hazard Class Name	Definition	Example
Process		
Testing faults	Hazards related to or caused by improper, incorrect, and/or insufficient testing.	Software update not properly tested causing radar failure when installed.
Installation/implementation faults	Hazardous conditions and faults caused by or related to system installation, construction, and implementation. Includes ATC environment disruption, airport traffic-flow disruption, and other equipment disruption due to system implementation activities.	Installation of RWSL at approach end of runway requires all aircraft to back taxi causing significant increase in runway occupancy time for departures.
Human		
Human factors	Hazards related to human error, confusion, or understanding.	Numerous false Collision Avoidance alarms cause controller to become complacent and ignore legitimate alarms.

3.2.4 Hazard Causes

The definition of a hazard cause according to the ATO SMS Manual is “the origin of a hazard.”[10, 11] That is, it is a specific event that triggers the hazard. An incident causal factor is typically the presenting problem that occurred just prior to the incident. Often, a hazard is a condition brought about by a combination or intersection of multiple system failures and human errors and results in the adverse effect.

In new systems, causes can generally be classified as flaws, failures, or malfunctions of internal and external system components, including hardware or software. Causes may also be classified by human factors, such as human limitations and human errors, due to improper training. Process errors associated with system implementation and testing also contribute to hazard causes and, in turn, may lead to system failures and malfunctions. Similarly, environmental factors such as climate and traffic loading may impact system operation and contribute to system failure and malfunction.

Table 8 shows the hazard cause classification proposed for IDA-FS. There are four high-level classes consistent with elements of the SM ICG Hazard Taxonomy and ACT: “Equipment,” “Process,” “Human,” and “Environment.” The definition for each sub-class and an example from the IDA-FS dataset are also provided.

Table 8. Hazard cause classification

Cause Class Name	Definition	Example
Equipment		
System design/development flaw	Flaw or weakness in design requirements or development processes that leads to bugs, faults, or system limitations.	STARS software coded incorrectly causing good ADS-B sensor input to be filtered out.
HW/SW/function failure	Failure of system or subsystem hardware or software leading to a loss of function. Includes power system failures.	RWSL LED heater fails allowing snow/ice build-up on LED lights, thereby reducing the visibility distance of lights.
HW/SW/function fault	Fault or error in system or subsystem hardware or software leading to a loss or degradation of function. Includes power-system faults.	Defective ETVS monitor assembly improperly identifies normal interface activity as a fault condition.
Interface failure/fault	Failure or fault of hardware or equipment that connects systems or subsystems. Includes failure of network systems and equipment.	Commercial telco connection between ERAM components (Circuit Switched to Multiprotocol Label Switching) fails.
Interoperability flaw	Flaw or inconsistency in the planning or implementation of systems such that those systems may not work together correctly to safely carry out their intended functions.	ASDE-X software upgrade causes increase in false illuminations of RWSLs.
Latency/timing fault	Data or a function is presented later or earlier than expected by a recipient or user.	ASR-11 software fault causes weather messages to be delayed.
Data corruption	Data errors that occur during reading, writing, storage, transmission, or processing that introduce unintended changes to the original data.	<No examples of this class in the initial IDA-FS dataset>

ADS-B = Automatic Dependent Surveillance-Broadcast; HW/SW = hardware/software; LED = light-emitting diode

Table 8. Hazard cause classification (continued)

Cause Class Name	Definition	Example
Process		
Installation fault	Construction or installation operation that does not comply with relevant processes, requirements, guidance, or restrictions.	Improper installation of RWSL lighting hardware causes light angle to be difficult for pilot to view.
Adaptation/configuration errors	Adaptation/configuration parameters incorrectly set, changed, or deleted.	ASR-11 radar adjusted to reduce clutter causes loss of primary radar targets.
Testing issues	Incorrect/insufficient testing to locate and correct system anomalies or deficiencies.	Insufficient regression testing in ATOP software resulting in undetected errors.
Human		
Human errors	Incorrect action or inaction on the part of a human operator, user, or maintenance support.	Pilot files flight plan indicating aircraft is ADS-B equipped when it is not.
Human limitations	Physical or psychological limitations on human performance in the system state.	Pilot visual limitations in seeing RWSL LED lights from certain angle and distances.
Training issues	Insufficient, out-of-date, and/or incorrect training in relevant operations, procedures, and/or conditions.	ATC specialists not fully trained to understand new ERAM reroute tool capabilities.
Environmental		
Weather	Climate, weather conditions, or natural disasters that affect a system or operation.	Excessive heat causes RWSL relay failure.
Interference and Loading	Radio frequency interference, heavy traffic, or other conditions that overload an operational environment.	ERAM Surveillance and Broadcast Services system failure because of inability for test messages to be delivered in high-interference environment.
Operating environment conditions	The physical conditions in which equipment operates, excluding weather. May include physical configuration and conditions of the facility in which the equipment is installed.	Failure to control and eliminate dust from entering the control room when tiles and equipment are moved during ATOP equipment installation causes ATC disruption.

ADS-B = Automatic Dependent Surveillance-Broadcast; LED = light-emitting diode;

Note that the ACT under development by AJI, as discussed in section 2.4, already includes classification codes that describe various human, management, and equipment-related causal factors. These codes address a number of system failures; functional and operational faults and errors; and human actions, both ATC and pilot. The reason that the ACT codes were not chosen to classify hazard causes in IDA-FS is twofold: first, although a large number of system faults and failures are coded in ACT, the codes do not address the causes and sources of those faults and failures. As a result, particular failure modes and issues identified in ATO SRMDs may not be captured. By grouping hazard causes in terms of the 5M model categories and also capturing the associated system data in the IDA-FS model, the same traceability to system faults can be achieved while also distinguishing between faults and failures in hardware, software, interfaces, or other sources. Second, the ACT definition spans hundreds of individual causal codes across the four domains. At this point in IDA-FS development, the ACT causal codes are much more detailed than is necessary or practical for the IDA-FS model. It should be emphasized, however, that the ACT classes and codes can be mapped onto the IDA-FS data at a future time.

3.2.5 Mitigations

There are two broad types of mitigations identified in SRMDs: existing controls and recommended safety controls. The fundamental difference between these two categories, however, is only their validation and verification status. Existing controls are those that are validated and verified to be in existence in the baseline system or NAS environment. Recommended controls are those that are proposed to mitigate identified hazards but have not yet been validated and verified as implemented. Both types of mitigations can be categorized according to SOP, as described in section 2.8.

Like the classes for hazards and hazard causes, the classification categories for mitigations were assembled after review and analysis of all of the existing and recommended controls in the IDA-FS dataset. The initial groupings were consolidated and refined and then organized according to their classification within the SOP. Definitions were written for each class, and the dataset was re-classified according to the final schema.

Table 9 shows the control classifications that IDA-FS will use, including five high-level classes: “Design,” “Safety Devices,” “Warnings,” “Procedures,” and “Training.” The definition for each sub-class and an example from the dataset are provided in the table.

Table 9. Control classes

Control Class Name	Definition	Example
Design		
System performance	Requirements, specifications, or historical performance for system or function availability; latency; error tolerance; and false-alert rates.	ASR-9 operational availability performance.
HW/SW design	HW/SW design features intended to minimize risk. Example hardware-related design mitigations, including grounding, shielding, environmental, and other physical design criteria. Example software design-related mitigations include fault/failure control detection logic, timing controls, etc.	ASDE-X remote unit cabinet design requirements for lightning protection.
Redundancies and backups	Systems/equipment that mitigate a failed or faulted system; subsystem; or function allowing the impacted system or service to continue to operate.	ASR-11 requirement for independent, redundant radar channels.
Safety Devices		
Automatic backup or bypass	Automatic switchover or failover of a system or function to an alternate.	Existing ARTS IIIE software available in standby mode.
Automatic shutdown or disabling	Automatic shutoff of a system or function when fault or failure conditions are detected.	If ASDE-X goes offline, RWSL system is automatically shut down.
Automated fault/failure detection	System condition and performance monitoring, including self-monitoring, self-test, data verification, and system status checks. May support automatic safety devices or warning devices.	ERAM automatically discards an ADS-B report if the content of the validation field is invalid.

ASR-9 = Airport Surveillance Radar Model 9; HW/SW = hardware/software; ARTS IIIE = Automated Radar Terminal System Model IIIE; ADS-B = Automatic Dependent Surveillance-Broadcast

Table 9. Control classes (continued)

Control Class Name	Definition	Example
Warnings (see note that follows table)		
Operational alarms and alerts	Audible or visual alarms, alerts, and warnings that inform a user of a condition requiring action or attention.	STARS Collision Avoidance alert sounds alarm and gives visual indication of two aircraft in close proximity with potential for collision.
Maintenance alerts	Alarms and notifications indicating a condition potentially requiring maintenance, repair, or attention from system maintainers.	The RWSL system monitors key performance relative to key operational performance requirements and notifies the maintainer when they are not met.
Information systems	Systems that provide supplemental information regarding potential hazards to users but do not provide real-time indications of conditions or resolutions. May include NOTAMs ATIS information, or other notification of conditions.	ATIS broadcast includes advisory that RWSLs are in use. Pilot is required to listen to ATIS prior to taxi and ATC must verify receipt of the ATIS.
System status indications	Visual indications of data or conditions of potential interest to users (e.g., radar target reliability indicators).	STARS diamonds give controller an indication of target reliability.
Signage	Signs and labels notifying users of potential hazards/providing reminders or instructions.	Caution labels (e.g., High Voltage) on applicable components of ERAM.

ATIS = Automatic Terminal Information Service; NOTAM = Notice to Airmen

Table 9. Control classes (continued)

Control Class Name	Definition	Example
Procedures		
System development and test	Procedures and standards for system development and testing processes to minimize errors, faults, and failures.	Adherence to FAA T&E Gold Standard testing for NAS HW/SW Modifications to STARS.
System installation procedures	Procedures and standards for system installation and construction processes to minimize errors, faults, and failures.	Procedure to fall back to previous version of software on backup channel when installing new ATOP software.
System operating procedures	Manuals and procedures that give guidance on the operation of equipment to accomplish the user tasks.	Procedure to switch to single-sensor mode or turn functionality off if ADSB track is lost in CARTS.
ATC procedures	National or local procedures and guidance governing ATC operations and responsibilities.	ATCT use of 7110.65 procedures for validating aircraft identification, position, and altitude to verify ERAM information display.
Pilot procedures	Procedures and guidance governing pilot operations and responsibilities.	Procedures mandated by Title 14 Code of Federal Regulations Part 91 gives pilot requirements for weather minimums, cloud separation, and see and avoid.
Maintenance procedures	National or local procedures and guidance governing system maintenance, certification, and adaptation operations and personnel responsibilities.	FAA Order 6191.3X STARS Maintenance Technical Handbook specifies Tech Ops maintenance and certification procedures to ensure accurate SBS service certification.
Airport procedures	National or local procedures and guidance governing airport operations/personnel. Includes FAA Advisory Circulars, airport policy, and Letters of Agreement with local ATC.	Procedures specified in AC 150/5370 for the airport to establish predetermined mobilization and haul routes to avoid runway crossings for the installation of RWSL.

ATCT = Air Traffic Control Tower; HW/SW = hardware/software; SBS = Surveillance and Broadcast services; T&E = Test & Evaluation

Table 9. Control classes (continued)

Control Class Name	Definition	Example
Training		
ATC training	Training for ATC personnel in procedures and operations to minimize the risk of an ATC error.	Training of ATC personnel on the ERAM system operating procedures prior to implementation of system changes.
Tech Ops training	Training for Tech Ops personnel in procedures and operations to minimize the risk of a maintenance or certification error.	Training of Tech Ops personnel on the playback feature of RWSL including ATC coordination requirements.
Pilot/vehicle operator training	Training for pilots or ground vehicle operators. Includes air crew, airport, or contractor personnel procedures and operations to minimize the risk of an operational error by the pilot or driver.	Training of pilots and persons driving vehicles in the airport operating area on the functions of RWSL.

Note: Draft version 4.0 of the ATO SMS Manual gives the following definition for "Providing Warning:"

> **"**When alternatives and safety devices do not effectively eliminate or reduce risk, warning devices or procedures are used to detect the condition and to produce an adequate warning. The warning is designed to minimize the likelihood of inappropriate human reaction and response, and must be provided in time to avert the hazard's effects" [11].

The examples given in the ATO SMS Manual for warnings include aural and visual indicators of hazardous conditions that prompt a user to take action. These types of warnings were classified as "Operational Alarms and Alerts" and "Maintenance Alerts," depending on the intended recipient of the warning. Less clear, however, was how to classify safety controls that provide warnings that were more passive in nature. These could include information systems such as Automatic Terminal Information Service broadcasts alerting pilots of new or unusual conditions at the airport, or signs and labels that provide supplemental reminders to users of potential hazards related to the equipment or its operation. Because these are more passive in their operation, it is difficult to assess whether they are provided in time to avert the hazard's effects. Nevertheless, these are examples of both existing and recommended controls that are cited in SRMDs as mitigating identified hazards, and they more closely fit the profile of a warning than any of the other classes. Additional research indicates that other industry guidance does classify signage and other passive hazard information under the heading of "Warnings." In the end, the decision was made to classify "Information Systems" and "Signage" as sub-classes of "Warnings," with the understanding that these types of warnings are likely to be less effective risk controls because of their increased dependence on user behavior (reading or listening to information and comprehending its intent).

4. FINDINGS

Since the completion of the IDA-FS Dataset report in December 2013, work has continued to capture and characterize SRMD data on eight systems selected for the IDA-FS Phase II research. The data captured on these systems so far include 40 SRMDs with 226 hazards, 604 hazard causes, 1003 existing controls, and 339 recommended controls. To be included in the IDA-FS dataset, SRMDs must meet the following criteria:

- The document must be an SRMD and not an SRM Decision Memo (SRMDM).
- The SRMD must be approved by all required parties.
- The change to the NAS addressed in the SRMD must be focused on NAS equipment; this excludes air traffic procedural waivers.
- The SRMD must be available via the FAA's Web Configuration Management, the ATO NAS Digital Library, or AOV Connect, because these sources are accessible for the IDA-FS research effort and do not require special permission for AOV to obtain an ATO SRMD.
- The SRMD must be developed in accordance with ATO SMS Manual version 2.1 or a subsequent version

    – Note 1: SMS Manual version 2.1 has an effective date of May 2008. However, some SRMDs dated prior to May 2008 may still reference SMS Manual version 2.1.

    – Note 2: No SRMDs were found for the ETVS system that met all of the criteria above. To include SRMD data for this system, an SRMD was selected that was developed in accordance with ATO SMS Manual version 1.1.

Table 10 lists the SRMDs that have been characterized as of the date of this report. The focus of each SRMD is indicated as the "Primary System" in table 10, though certain SRMDs address system integration or interface development and more than one NAS system. Besides these 40 SRMDs, 20 additional SRMDs have been obtained for the eight systems selected for IDA-FS Phase II research and will be added to the IDA-FS dataset.

Table 10. SRMDs included in current IDA-FS dataset

No.	SRMD Title	Date	Primary System	Number of Hazards
1	Airport Surface Detection Equipment Model X (ASDE-X) Replacement of ASDE-X Antenna and Upgrade to Surface Movement Radar Improved (SMRi) at SEA	1-Aug-09	ASDE-X	2
2	Airport Surface Detection Equipment Model X (ASDE-X) Change Order 6 (CO6) National Software Build	18-Mar-10	ASDE-X	8
3	Airport Surface Detection Equipment Model X (ASDE-X) Deviation from FAA-STD-19E: Air Terminal Installation atop ASDE-X Low Impact Resistant Fiberglass Masts housing ASDE-X Multilateration System Remote Unit Antennas	26-Mar-10	ASDE-X	1
4	Airport Surface Detection Equipment Model X (ASDE-X) SAN ASDE-X Interface to ASR-8	26-Jul-10	ASDE-X	1
5	Anchorage International Airport–Optimization of ASR-8 and ASR-11	1-Jan-11	ASR-11	2
6	Application of 3-NM Terminal Area Separation Standards for Air Surveillance Radar-11	1-Sep-11	ASR-11	2
7	SRMD for ASR-11 Anchorage Build 2 Software Upgrade SSM-ASR11-026	25-Feb-08	ASR-11	3
8	STARS ELITE Connection to Existing ASR-11 TRACON UPS at TAMRp3s2 Sites	13-Sep-13	STARS	1
9	Advanced Signal Data Processor Technical Refresh for ASR-11	30-Nov-07	ASR-11	15

Table 10. SRMDs included in current IDA-FS dataset (continued)

No.	SRMD Title	Date	Primary System	Number of Hazards
10	Airport Surveillance Radar-11 Technology Refresh Segment 2 Operational Safety Assessment	7-Aug-12	ASR-11	5
11	Airport Surveillance Radar Model 11 Terminal Radar Approach Control (TRACON) Mini-Uninterruptible Power Supply SSM-ASR11-034, SSM-ASR11-036 and ATO0W-ASR11-1094	7-May-09	ASR-11	1
12	ASR-11 Kpsf-1 build C test SSM-ASR-11-031 ATO0W-ASR11-1090	19-Feb-09	ASR-11	1
13	Advanced Technologies and Oceanic Procedures (ATOP) NAS Change Proposal 34118 Safety Risk Management Document (SRMD)	7-Mar-11	ATOP	1
14	Advanced Technologies and Oceanic Procedures (ATOP) NAS Change Proposal 32386	1-Apr-09	ATOP	2
15	Advanced Technologies and Oceanic Procedures (ATOP) NAS Change Proposal 31815	30-May-08	ATOP	1
16	Relocation of ATOP Control Room, Installation of a Supervisory Quad Workstation, Installation of an ATOP Local Area Network (LAN) Rack - 2010	18-May-10	ATOP	4
17	Terminal Automation Modernization Replacement (TAMR) ARTS IIIE Revision 33b Transition Software And Common ARTS Generation Five Upgrade For Minneapolis TRACON And Associated Tower Facilities Safety Risk Management Document	1-Jan-08	CARTS	4
18	SRMD-ATO-T-CARTS-1030-PHA Case File ATO0T-CARTS-1030 Remove Obsolete Equipment from the Common Automated Radar Terminal System (CARTS) Inventory and Documentation	23-Nov-09	CARTS	2

Table 10. SRMDs included in current IDA-FS dataset (continued)

No.	SRMD Title	Date	Primary System	Number of Hazards
19	Common Automated Radar Terminal System (CARTS) Case File ATO0T-CARTS-1041	3-Sep-09	CARTS	1
20	SRMD-ATO-T-CARTS-1065-PHA Case File ATO-0T-CARTS-1065 Automatic Dependent Surveillance-Broadcast (ADS-B)	5-Oct-09	CARTS	2
21	SRMD-JT132-CARTS-1004-PHA Modify CARTS Software to Allow SBS DO-260B/282B Interface and to Include Updated SBS ADS-B Requirements	24-Jun-11	CARTS	4
22	SRMD-ATO-T-CARTS-R37A-PHA Common Automated Radar Terminal System (CARTS) Software Release Revision 37a	17-Apr-13	CARTS	3
23	En Route Automation Modernization (ERAM) CR 961 / SIG 1359 Additional ICAO 2012 Changes (Pt. 2)	29-Nov-12	ERAM	1
24	Enhanced Backup Surveillance System (EBUS) Case File JE122-DARC-1001 (NCP 33135) ERAM and EBUS Displays Are Not In Synch	22-Jun-10	ERAM	3
25	ICAO 2012 Flight Plan Changes-Amendment 1 SRMD	6-Jun-12	ERAM	20
26	Safety Risk Management Document (SRMD) Addendum for Critical Services: ATC Surveillance Services in the Gulf Of Mexico With Automatic Dependent Surveillance Broadcast (ADS-B) And ERAM R2	29-Apr-11	ERAM	6
27	Safety Risk Management Document (SRMD) for Test Runway Status Light (RWSL) Installations Boston Logan International Airport (BOS)	3-Mar-09	RWSL	4
28	Runway Status Lights Los Angeles International Airport Local Safety Risk Management Document	24-Oct-08	RWSL	37

Table 10. SRMDs included in current IDA-FS dataset (continued)

No.	SRMD Title	Date	Primary System	Number of Hazards
29	Runway Status Lights (RWSL) Safety Risk Management Document (SRMD) SRMD-ATO-T-RWSL-ISM-2010-001	10-Mar-10	RWSL	15
30	Runway Status Lights (RWSL) Safety Risk Management Document (SRMD) SRMD-ATO-T-RWSL-ISM-2010-001	30-Aug-12	RWSL	16
31	Critical Services: Terminal Air Traffic Control with ADS-B and STARS	23-Feb-10	STARS	16
32	Radar-Pairwise Registration Enhancements	3-Feb-12	STARS	3
33	STARS FS-2+ Baseline Update to include requirements to support LCM Build E1	19-Dec-12	STARS	3
34	STARS FS-2+ Baseline Update to include requirements to support Life Cycle Maintenance (LCM) Build R1a	9-Apr-13	STARS	2
35	STARS FS-2+ Baseline update to include additional Automation Dependent Surveillance-Broadcast (ADS-B) Initial Operating Capability (IOC) requirements as described in Engineering Change Proposal (ECP)-028	6-Oct-09	STARS	4
36	Safety Risk Management Document (SRMD) SRMD-T1311-STARS-1009-PHA STARS FS-2+ Baseline Update to include requirements to support LCM Build R22	13-Dec-10	STARS	5
37	Safety Risk Management Document (SRMD) SRMD-T1311-STARS-1052-PHA STARS FS-2+ Baseline Update to include new requirements to support the STARS G4 system architecture	18-Apr-12	STARS	1

Table 10. SRMDs included in current IDA-FS dataset (continued)

No.	SRMD Title	Date	Primary System	Number of Hazards
38	Safety Risk Management Document (SRMD) for Enhanced Terminal Voice Switch (ETVS) ETVS Operator Processor Enhancement SSM-ETVS-012	7-Nov-07	ETVS	3
39	En Route Automation Modernization (ERAM) CR 484/SIG 609 Pre-departure Traffic Flow Management (TFM) reroute amendments with preferential route override	7-Mar-12	ERAM	2
40	En Route Automation Modernization (ERAM) Flight Plan (FP) Updates not output to Flight Data Input/Output (FDIO) when Strip Printing Fails (PR57238) Safety Risk Management Document (SRMD)	12-Apr-12	ERAM	1

Sections 4.1 through 4.4present an initial distribution of SRMD data according to the classification scheme for IDA-FS discussed in Section 3.2.

4.1 THE NAS CHANGES

Figure 4 shows the number of SRMDs according to the NAS change types defined in table 5. Approximately 73% of SRMDs (29 out of 40) are classified as "System Modifications," consistent with the "In-Service Management" life-cycle phase for 6 of the 8 systems. Two (2) of the 8 systems (namely, RWSL and Automatic Dependent Surveillance-Broadcast [ADS-B]) have sites in "Solution Implementation" and provide a sample of SRMDs for the NAS Change Types involving "New System Acquisition/Development" and "System Deployment/Installation." The ASR-11 system, which is in the "In-Service Management" life-cycle phase, provides an example for a NAS change type involving a modified mission or application for an existing system, although the system had no actual physical or functional change. In this case, the ASR-11 SRMD sought approval to apply 3 NM terminal separation standards at a range of 60 NM from the ASR-11 antenna versus the originally approved 40 NM range. For the NAS change type involving a "Deviation from equipment/safety standards," one ASDE-X SRMD sought approval to deviate from FAA-STD-19E, "Lightning and Surge Protection, Grounding, Bonding and Shielding Requirements for Facilities and Electronic Equipment." None of the 40 SRMDs sampled involved "System Decommissioning/Removal," although a CARTS SRMD did address a system modification to remove obsolete equipment. It is anticipated that ETVS, which is to be replaced by the FAA's NAS Voice Switch system, will eventually be addressed in an SRMD for the "Decommissioning/Removal" NAS change type.

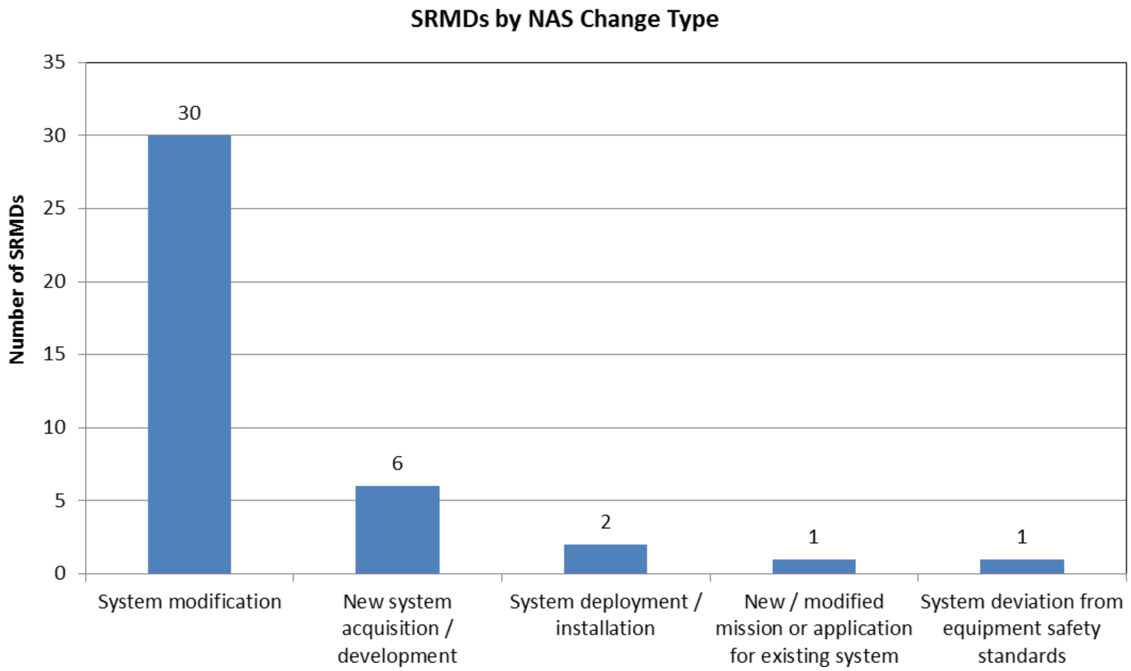

Figure 4. The SRMDs by NAS change type

4.2 HAZARDS

Figure 5 shows the distribution of 226 hazards by their assigned hazard classification. Of these hazards, 74% (167 out of 226) are directly related to equipment failure, malfunction, or error. The remaining 26% are comprised of human factors and process hazards that relate to system implementation, operation, test, or maintenance.

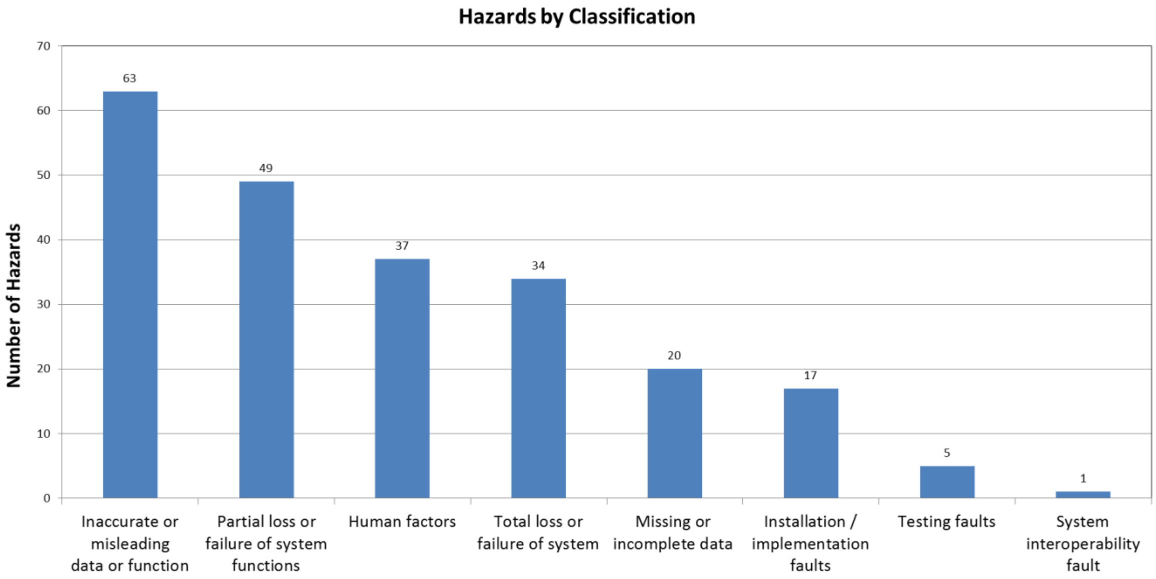

Figure 5. Hazards by classification

4.3 HAZARD CAUSES

Figure 6 shows the distribution of the 604 hazard causes by cause classification. Approximately 40% of causes (245 out of 604) are related to hardware, software, or function faults. All other cause classifications individually represent less than 10% of the total number of causes sampled. This distribution suggests that hardware/software function faults may benefit from further decomposition into types of faults, such as data input faults, processing faults, and output faults. The sub-categorization of equipment malfunctions presented in AJI's Common Taxonomy may offer another approach for breaking down hazard causes related to faults.

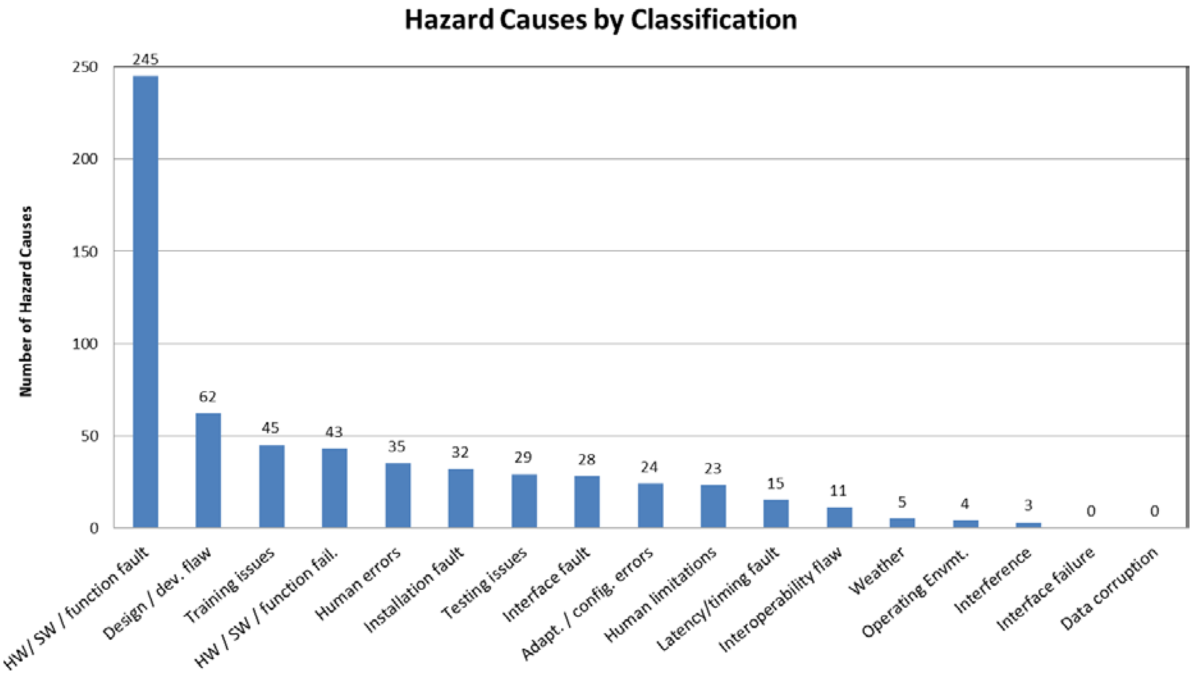

Figure 6. Hazard causes by classification

Some proposed classifications yielded few, if any, hazard causes in the initial IDA-FS dataset. It is expected that, as additional SRMDs and systems are captured in the IDA-FS dataset, the distribution of data items in each class may shift from what is depicted at this time.

4.4 CONTROLS

Figure 7 shows the distribution of the 1003 existing controls by control classification. Approximately 43% of existing controls (435 out of 1003) entail system design provisions, safety devices, or warnings that are validated and verified as already implemented at the time of the proposed NAS change. Most of these controls are attributed to: (1) STARS and ERAM updates to support the ADS-B acquisition and (2) the RWSL acquisition. In the case of STARS and ERAM, many existing controls cite external requirements for radar system and ADS-B avionics performance, whereas RWSL cites mostly internal system existing controls. Procedural controls in the form of system development and testing standards and ATC procedures also comprise a large percentage of existing controls at 40% (394 out of 1003).

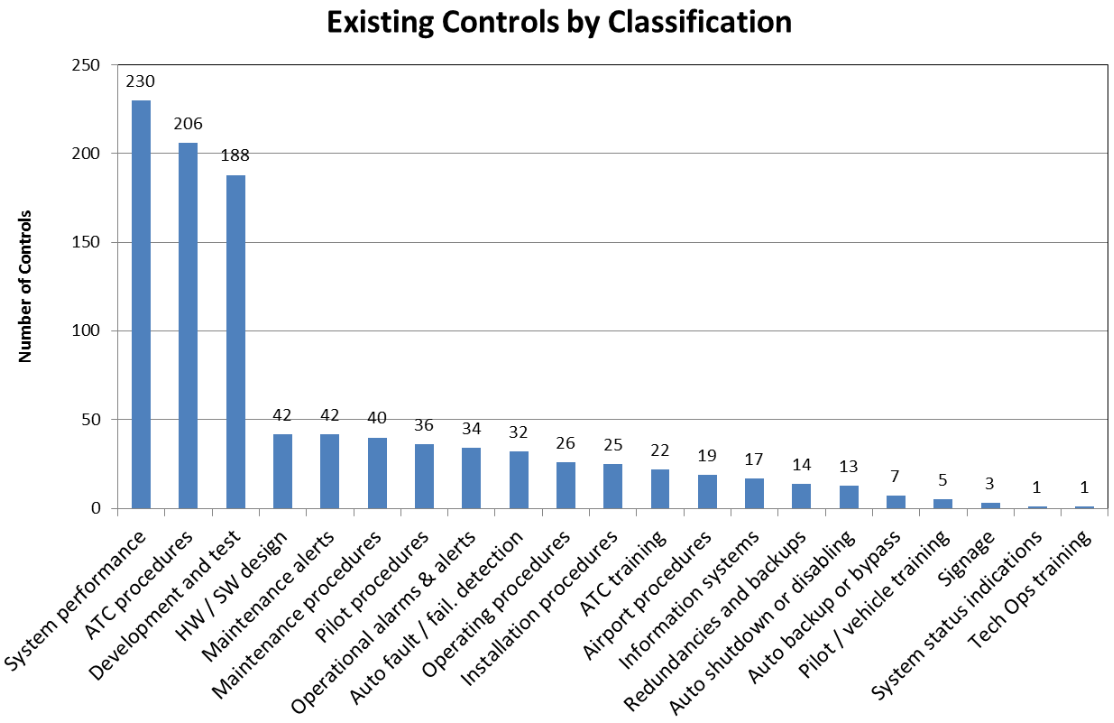

Figure 7. Existing controls by classification

Figure 8 shows the distribution of the 339 recommended controls by the same classifications applied to existing controls. The sample of SRMDs in the IDA-FS dataset indicates that 74% of recommended controls (250 out of 339) entail procedures or training. Because the SRMDs examined consist mostly of NAS system modifications in the “In-Service Management” life-cycle phase, it follows that most recommended controls do not impose system-design requirements that have yet to be validated and verified. For the 19% of recommended controls that entail design requirements, most are attributed to SRMDs for RWSL and ADS-B/STARS-related system acquisitions, during which recommended controls undergo validation and verification.

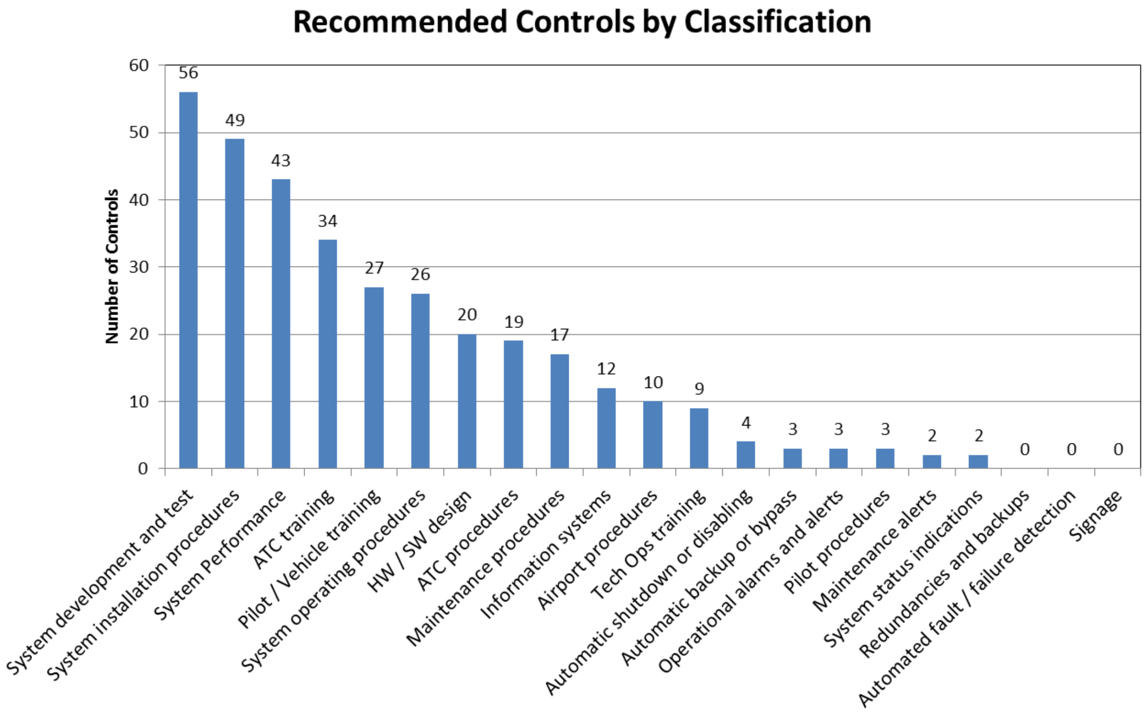

Figure 8. Recommended controls by classification

5. CONCLUSIONS

The Integrated Domain Assessment of Future Systems (IDA-FS) classification schemas described in this report will be used to enable IDA-FS tool functions that cross-reference and compare similar systems, National Airspace System (NAS) changes, and hazard information. Classifications are defined for NAS systems, NAS change types, hazards, causes, and controls based on a sample of 40 Safety Risk Management Documents (SRMDs) compiled for the initial IDA-FS dataset.

The IDA-FS classification schema maintains traceability to international aviation and FAA safety taxonomies where applicable but is not intended to serve as a complete or universal taxonomy of safety data. The International Civil Aviation Organization (ICAO) and the FAA have undertaken efforts to develop comprehensive safety taxonomies that meet the broad needs of the aviation community, whereas IDA-FS is focused on air traffic control equipment-related hazard information. Nevertheless, the proposed IDA-FS classification schema is traceable to applicable elements of the Safety Management International Collaboration Group Hazard Taxonomy and the FAA Air Traffic Organization Office of Safety (AJI) Common Taxonomy to support potential future collaboration.

It is anticipated that the IDA-FS data may be mapped to additional or alternative taxonomies at a later date as needed. If one or more of these taxonomies is chosen by the FAA or by the FAA Air Traffic Safety Oversight Service (AOV) as a standard for future safety efforts, it should be possible to align IDA-FS with that taxonomy. Because IDA-FS data will be stored in a database, the process of mapping that data onto a new or alternative classification schema is a matter of subject matter expertise, not IDA-FS system architecture. In addition, the classifications proposed in this report are not envisioned as schema for AOV analysts to tag IDA-FS data for later querying. Tagging data items with keywords and running searches on those tags will be a separate use case for IDA-FS and will be addressed later in the IDA-FS prototype development.

The classification schemas proposed in this document will be used by the IDA-FS tool to group similar systems, NAS changes, and hazards to analyze and compare SRMD content. As additional SRMDs are compiled and classified as part of the IDA-FS dataset, the classification scheme will also continue to be refined.

Two possible extensions to the IDA-FS classification scheme have been identified. First, some of the data classes may benefit from additional subdivision. If a single class contains a comparatively large number of data items compared to other classes, then it may prove useful to further break down that class to provide additional granularity for cross-referencing historical SRMD information. For example, the hazard cause class "HW/SW/function fault" might be further broken down into hardware fault, software fault, and combination fault (both hardware and software elements). Because of the limited scope of the IDA-FS dataset at this time, this subdivision was not deemed practical. As additional data are collected and other systems are incorporated into the IDA-FS dataset, there may be enough supporting data to logically subdivide some classes.

Another possible extension to the classification work for IDA-FS may be to capture and classify hazard effects identified in SRMDs. The initial IDA-FS dataset captures the initial/current risk (likelihood and severity) and the predicted residual risk of each hazard but does not separately itemize hazard effects. It may be useful to capture hazard effects for comparison to safety incident and event reports to cross-check predicted risk likelihoods against observed occurrences. ICAO and AJI efforts to define occurrence-based hazard taxonomies may be applied for characterizing hazard effects.

6. REFERENCES

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

2. Standardization Workgroup of the Safety Management International Group. (April 20, 2010). Development of a common taxonomy for hazards. Retrieved from http://www.atcvantage.com/docs/SM_ICG_development_of_common_hazard_taxonomy.pdf.

3. Standardization Workgroup of the Safety Management International Collaboration Group. (April 25, 2013,). Hazard taxonomy examples. Retrieved from http://www.skybrary.aero/bookshelf/books/2301.pdf.

4. National Transportation Safety Board. (n.d.). *Aviation accident database*. Retrieved from http://www.ntsb.gov/_layouts/ntsb.aviation/index.aspx.

5. National Transportation Safety Board. (1998) Aviation coding manual. Washington, D.C. Retrieved from http://app.ntsb.gov/avdata/codman.pdf.

6. Nazeri, Z. (2007). *Cross-database analysis to identify relationships between aircraft accidents and incidents* (Doctoral dissertation). Retrieved from http://catsr.ite.gmu.edu/pubs/ZohrehDissertation[1].pdf.

7. Krokos, Kelley J. and Baker, David P. (2005). *Development of a taxonomy of causal contributors for use with ASAP reporting systems.* Washington, D.C.: American Institutes for Research. Retrieved from http://homepages.wmich.edu/~rantz/www/5100/accers_tech_report.pdf.

8. Commercial Aviation Safety Team. (2014). *The CAST/ICAO common taxonomy team*. Retrieved from http://www.intlaviationstandards.org.

9. FAA Report. (2002). Development of an FAA-EUROCONTROL Technique for the Analysis of Human Error in ATM (DOTC/FAA/AM-02/12).

10. Air Traffic Organization. (2008). Safety Management System Manual, Version 2.1.

11. Air Traffic Organization. (2013). Safety Management System Manual, Version 4.0.

12. National Airspace System. (2012). As-Is Enterprise-Level Architecture Systems Interface Description (SV-1), Version 3.0.

13. National Airspace System. (2011). Operational Node Connectivity Diagram (OV-2) As-Is, Version 1.0.

14. FAA Order 6000.5D. Facility, Service, and Equipment Profile (FSEP). (2005).

15. FAA (n.d.). FAST—FAA Acquisition System Toolset. Retrieved from http://fast.faa.gov.

16. FAA SRMD. (2012). ERAM Change Request (CR) 484/Segment Issue Group (SIG) 609 Pre-departure Traffic Flow Management (TFM) Reroute Amendments with Preferential Route Override.

APPENDIX A—CASE STUDY ON SAFETY RISK MANAGEMENT DOCUMENT CLASSIFICATION

This appendix shows how the classification scheme was applied to an example Safety Risk Management Document (SRMD) in the Integrated Domain Assessment of Future Systems (IDA-FS) dataset. This case study examined the SRMD "ERAM Change Request (CR) 484/Segment Issue Group (SIG) 609 Pre-departure Traffic Flow Management (TFM) Reroute Amendments with Preferential Route Override." [16] This SRMD deals with a new software function added to En Route Automation Modernization (ERAM) that allows traffic flow management (TFM) to send re-route information to ERAM. The Executive Summary and Section 2 of the SRMD explain the nature and scope of the change. Section 6 of that document identifies the hazards, and Section 7 provides a summary of the hazard analysis and risk assessment.

This appendix shows the application of the classification schemes discussed in section 3 of the main report to the ERAM SRMD. Classifications are shown for SRMD attributes, hazards, causes, and controls.

A-1 SRMD DATA CLASSIFICATION

Tables A-1–A-5 show the key attributes captured for each piece of SRMD data and the IDA-FS classification categories assigned for each data item.

Table A-1. Classification of SRMD attributes

SRMD Title	Date	Number of Hazards	Primary System	System Classification	FSEP Code	NAS Change Class
En Route Automation Modernization (ERAM) CR 484 / SIG 609 Pre-departure TFM reroute amendments with preferential route override	3/7/2012	2	ERAM	ATC Automation; Flight & surveillance processing	AK00A	System modification

TFM = traffic flow management, FSEP= Facility, Service, and Equipment Profile; NAS = National Airspace System; ATC = air traffic control

Table A-2. Classification of hazards

Hazard ID	Hazard Title	System State	Hazard Effect	Initial Risk	Residual Risk	Hazard Class
SIG-609-1	Aircraft not receiving correct routing (flight plan)	Operational ERAM with ability to process automated preferential departure re-routes from TFMS	Aircraft departs on non-coordinated route. Aircraft placed in a hazardous environment (i.e., High traffic volume, weather)	3E Low	3E Low	Inaccurate or misleading data or function
SIG-609-2	Aircraft not receiving correct routing (flight plan)	Operational ERAM with ability to process automated re-routes from TFMS	Aircraft departs on non-coordinated route. Aircraft placed in a hazardous environment (i.e., High traffic volume, weather)	3E Low	3E Low	Inaccurate or misleading data or function

TFMS = Traffic Flow Management Systems

Table A-3. Classification of hazard causes

Hazard ID	Hazard	Hazard Cause	Cause Class
SIG-609-1	Aircraft not Receiving Correct Routing (Flight Plan)	Implementation of a new operating procedure, which may not be followed.	Training issues
		Changes in how an Air Traffic Control System Command Center (ATCSCC) Traffic Management Initiative (TMI) Route is coordinated.	Training issues
		New capabilities are not fully understood (i.e., new reroute tool could produce multiple routes when controller is used to seeing one).	Training issues
SIG-609-2	Aircraft not Receiving Correct Routing (Flight Plan)	Suppression of preferential routes because of protected area.	System design/development flaw
		Protected area overriding automation.	System design/development flaw
		Preferential route reapplied without notification to the controller.	System design/development flaw

Table A-4. Classification of existing controls

Hazard ID	Control	Control Class
SIG-609-1	Existing Letters of Agreement and Standard Operating Procedures directing manual coordination.	ATC procedures
	Local interfaces to ERAM System Wide Information Management (SWIM) Application Service (ESAS) are disabled at the local Monitor & Control (M&C) position.	System operating procedures
SIG-609-2	Existing Letters of Agreement and Standard Operating Procedures directing manual coordination.	ATC procedures
	Local interfaces to ESAS are disabled at the local M&C position.	System operating procedures

Table A-5. Classification of recommended controls

Hazard ID	Control	Control Class
SIG-609-1	Training (Tech Ops, local Traffic Management, and controllers).	ATC training
	MOU	ATC procedures
	Modify existing LOAs/SOPs as needed.	ATC procedures
	ZMP network routers are not configured to talk to TFMS. Functional interface from ZMP to TFMS disabled at ZMP M&C positions.	System development and test
SIG-609-2	Training (Tech Ops, local Traffic Management, and controllers).	ATC training
	MOU	ATC procedures
	Modify existing Letters of Agreement/Standard Operating Procedures as needed.	ATC procedures
	ZMP network routers are not configured to talk to TFMS. Functional interface from ZMP to TFMS disabled at ZMP M&C positions.	System development and test

MOU = Memo of Understanding , ZMP = Minneapolis Center, M&C = monitor and control