DOT/FAA/TC-17/2

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

Integrated Domain Assessment Model

October 2017

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/TC-17/2		

4. Title and Subtitle	5. Report Date
INTEGRATED DOMAIN ASSESSMENT MODEL	October 2017
	6. Performing Organization Code: ANG-E272

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

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

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
FAA National Headquarters 800 Independence Ave SW Orville Wright Bldg (FOB10A) Washington, DC 20591	Final Report
	14. Sponsoring Agency Code: AOV-100

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 the Air Traffic Organization's provision of air traffic services. To support its mission, the AOV initiated a research effort to develop a decision support tool, the Integrated Domain Assessment (IDA). The IDA prototype provides decision support to the AOV for Safety Risk Management Document (SRMD) evaluation, National Airspace System (NAS) change impact analysis, and other safety oversight activities by identifying and assessing potential safety concerns with legacy and future systems. To support SRMD evaluation, the IDA prototype identifies potentially missing hazard, cause, and control types; potential single-cause hazards; and hazard-monitoring plan issues, among other potential SRMD issues. The prototype also evaluates and compares control effectiveness against risk levels assessed in SRMDs to help the AOV understand the relative importance of controls when evaluating control approval or acceptance decisions. To support NAS change impact analysis, the IDA prototype provides a set of system and safety indicator scores that characterize system-safety interdependencies and system performance that may affect risk control effectiveness and overall risk likelihood. The IDA data model integrates NAS architecture data and system safety data, such as hazards, causes, and controls, to form the foundation of the IDA prototype. This report describes the IDA data model according to functional, conceptual, logical, and physical views. Details about data entities, attributes, and entity relationships are provided for the IDA data model and resultant IDA database. The IDA outputs that map to the AOV's SRMD request evaluation worksheet and a detailed IDA data dictionary are provided as appendices.

17. Key Words	18. Distribution Statement
Air Traffic Safety Oversight Service, Integrated domain assessment, Risk control, Safety risk, National Airspace System systems, National Airspace System architecture, Safety management system, Safety risk management document, hazard, hazard cause, control, data model	This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	75	

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AAC	Approval, acceptance, and concurrence
AJW	Technical Operations
AOV	Air Traffic Safety Oversight Service
ASDE-X	Airport Surface Detection Equipment, Model X
ATC	Air traffic control
ATO	Air Traffic Organization
CIP	Capital investment plan
ConOps	Concept of operations
ERD	Entity-relationship diagram
ETVS	Enhanced Terminal Voice Switch
FK	Foreign key
FSEP	Facility, Service, and Equipment Profile
HRH	High-risk hazard
ICD	Interface Control Document
IDA	Integrated Domain Assessment
IRD	Interface Requirement Document
NAS EA	National Airspace System Enterprise Architecture
NCP	National Airspace System Change Proposal
NextGen	Next Generation Air Transportation System
OV	Operational View
PHA	Preliminary Hazard Analysis
PK	Primary key
REW	Request Evaluation Worksheet
RWSL	Runway Status Lights
SDP	Service delivery point
SME	Subject matter expert
SMS	Safety Management System
SMTS	Safety Management Tracking System
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
SRMDM	Safety Risk Management Decision Memo
STARS	Standard Terminal Automation Replacement System
SV	System view
TIB	Technical Interchange Bulletin
WebCM	Web Configuration Management

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 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 that has 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 existing high risks.

The FAA's Air Traffic Safety Oversight Service (AOV) is responsible for independent safety oversight of air traffic services provided by the ATO. As part of the AOV's responsibilities described in FAA Order 1100.161 Change 1, the 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 work instructions define a step-by-step process for the AOV's review of SRMDs—along with approval and rejection criteria based on ATO SMS manual compliance.

One of the major challenges that the 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 resulting from unanticipated consequences of multiple system and NAS change interactions may not be identified before deployment.

To address this shortfall, the AOV launched an Integrated Domain Assessment (IDA) research effort. The primary goal of this effort is to develop a decision-making support tool to assist the AOV with approving controls in ATO SRMDs, given the context of multiple NAS changes. The IDA tool will identify interactions and interdependencies among NAS systems and system safety hazards and provide a basis for the AOV's evaluation of SRMDs and high-risk hazard (HRH) controls. Unlike other SRM approaches, the IDA is a model-based safety 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 tool will notify the AOV of potential SRMD discrepancies and NAS change impacts (NCIs) as areas of safety concern for further AOV review and oversight action. In addition to supporting the AOV's decision-making

on the approval of proposed controls to mitigate HRHs, the IDA tool will also support other AOV safety oversight processes, including the Safety Management Action Review Team's activities, audits, and safety-compliance monitoring. The IDA may additionally be extended to support other AOV AAC activities in which the AOV accepts (versus approves) controls spanning multiple FAA lines of business.

This report documents the development of the IDA data model. The IDA data model provides the foundation of the tool and includes a repository of SRMD and NAS system architecture data. To establish this repository, the IDA data model defines the data entities, attributes, and relational structure needed to analyze SRMD and NAS system information. This report describes the IDA data model implemented for the IDA prototype demonstration in August 2015. The decision support, or business logic, that uses the IDA data model is addressed in a separate report, which addresses the tool methodology and criteria for evaluating SRMD content, assessing risk control effectiveness, and analyzing NCIs.

The IDA data model is comprised of views that are intended to capture both high-level and detailed representations of NAS system and safety-related data. The model defines, organizes, and structures the relationships among data entities to provide stakeholders and database developers a common understanding of IDA's information architecture. These entities include NAS systems, system interfaces, air traffic facilities, SRMDs, hazards, hazard causes, risk controls, and monitoring plans. The IDA data model also defines the links among systems, hazards, hazard causes, and risk controls. This relational structure, along with decision-support logic, enables the IDA to identify interactions among NAS systems and potential safety concerns as a result of system changes that affect safety hazards, causes, and risk controls.

The IDA data model has been implemented as a relational database and populated with 57 SRMDs for eight NAS systems selected for initial research. A data dictionary and physical schema for the IDA prototype database are provided in appendices B and C, respectively.

1. INTRODUCTION

1.1 BACKGROUND

The FAA's 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, the 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 (AAC) work instructions define a step-by-step process for the 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 the AOV faces is the current ATO Safety Risk Management (SRM) process that 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, the AOV launched an Integrated Domain Assessment (IDA) research effort to develop a safety-review tool to assist the 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 tool helps to identify interactions and interdependencies among NAS systems and system safety hazards, providing a basis for the AOV's evaluation of SRMDs and high-risk hazard (HRH) controls and other safety oversight activities.

The IDA will enable AOV users to more effectively and efficiently evaluate SRMDs and NAS change impacts (NCIs) by integrating multiple sources of system and safety data into a single platform. Figure 1 provides an overview of the IDA concept, which includes the following functional objectives:

- Evaluate SRMD content—Identify SRMD issues, such as potentially missing hazards and hazard causes, control vulnerabilities, and hazard-monitoring plan deficiencies.
- Evaluate effectiveness of controls—Assist the AOV with determining whether proposed controls can be expected to reduce the risk, as indicated in the SRMD.
- Analyze system impacts—Analyze the interdependencies among the NAS systems and hazards to identify other systems, hazard causes, and risk controls that may be affected by changes to the NAS.
- Track SRMD and NAS data—Maintain a model of NAS system and SRMD data, and provide utilities for the AOV to manage remarks and notifications concerning SRMD issues, system/NCIs, and other safety-oversight concerns.

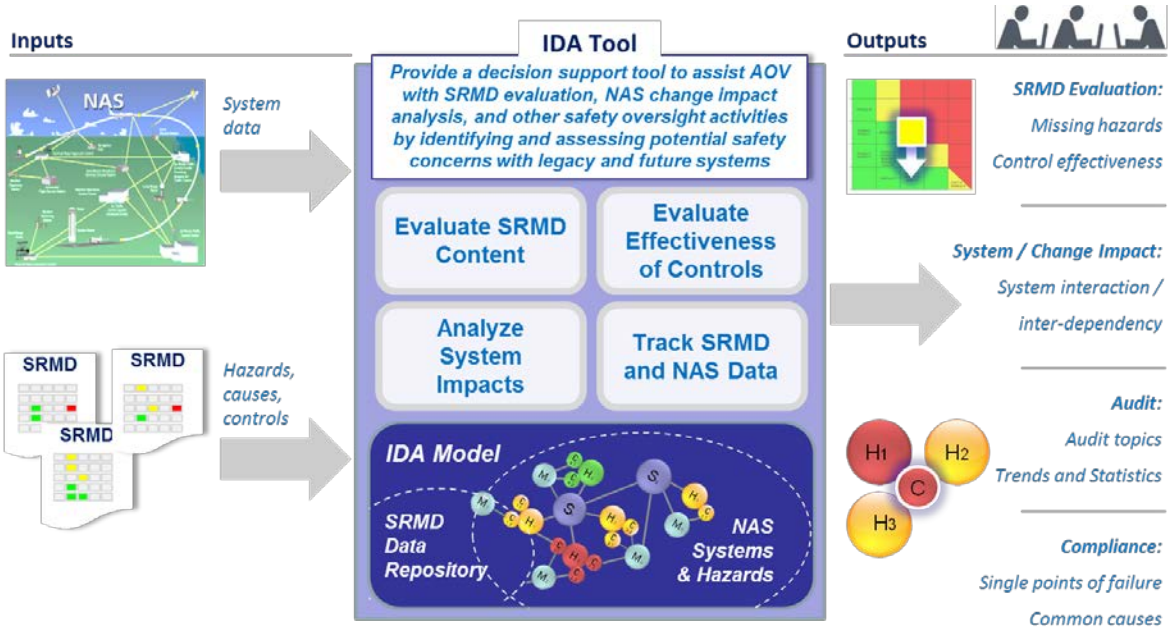

Figure 1. IDA concept overview

As shown in figure 1, the IDA data model constitutes the foundation of the tool, enabling functions to evaluate NCIs, 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 assembles NAS architecture information, system safety hazard data, and information about planned NAS changes. As the NAS evolves, system architecture changes and supporting SRMDs are used to update the IDA data model.

1.2 PURPOSE

The purpose of this report is to describe the organization and development of the data model used by the IDA to enable the analyses and functions identified in the IDA concept of operations (ConOps) [1]. The purpose of the IDA modeling effort is to organize, describe, and group data about NAS systems and identified safety hazards that have been captured by the IDA. The IDA data model is reflected in the implementation of the preliminary IDA database that underlies the IDA application. This report builds upon and supersedes the Preliminary Model Dataset Development report [2] submitted in 2013, which documented the initial work done to decompose system and safety data into elements that could be incorporated into the IDA data model.

1.3 DEFINITIONS

The following terms are used throughout this report. Definitions are drawn from various FAA documents and standards, including FAA Order 1100.161 Change 1, Air Traffic Safety Oversight [3].

- 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.
- Data model—A data model describes the static structure of information in terms of data entities and their relationships [4]. The IDA data model includes functional, conceptual, logical, and physical views. The functional view identifies tool functions and input and output data. The conceptual view shows abstracted or high-level data elements and relationships. The logical view shows entity attributes, including those attributes that uniquely identify each entity. The physical view provides implementation details on database tables.
- NAS change—Per the ATO SMS manual, any change to or modification of airspace; airports; aircraft; pilots; air navigation facilities, 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 purposes, NAS changes related to ATO NAS equipment are within the scope of this research effort.
- System—An integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, services, and other support services [5].

1.4 DOCUMENT STRUCTURE

Section 2 of this document describes the approach for establishing an IDA data model. Section 3 shows the allocation of IDA tool functions to the IDA data model as well as analytical methodologies required to produce certain function outputs. A conceptual view of the IDA data model, including key data entities and their relationships, is presented in section 4. Section 5 describes the IDA data model logical view, including the attributes of primary entities defined in the model. Section 5.3 discusses the initial implementation of a database based on the IDA data model to support future development of analytical methodologies needed for more complex IDA functions. Section 7 summarizes the IDA data model findings and outlines the next steps in the development of the data model and supporting analytical methodologies.

Three appendices are included in this report: appendix A provides a mapping of IDA functions to the AOV's request evaluation worksheet criteria, appendix B includes a data dictionary that

defines the attributes and parameters used in the IDA data model, and appendix C provides the detailed schema for the preliminary IDA database implementation.

2. MODELING APPROACH

To develop software based on real-world data, it is necessary to define a data model that describes the data. According to Ponniah:

> "Data modeling provides a method and means for describing the real-world information requirements in a manner understandable to the stakeholders in an organization. In addition, data modeling enables the database practitioners to take these information requirements and implement these as a computer database system to support the business of the organization [6]."

Therefore, a data model includes a high-level description or representation of the key data elements and their relationships and a detailed definition and logical organization of the data.

Development of a data model entails several steps. First, the need and purpose of the data model are defined by assessing the stakeholder functional needs, data outputs, and data inputs, which are captured in a functional view. Next, a conceptual view (also referred to as a semantic view) is defined. The conceptual view defines the basic ideas and entities to be captured in the model, the high-level relationships between entities, and the constraints on the entities. The conceptual view is intended to show the basic organization of data so that stakeholders and developers can understand and agree on the overall data model. The conceptual view is then further refined into a logical view. The logical view defines the attributes or constituent pieces of data that describe each entity and further defines the relationships between entities and attributes. The logical view provides a comprehensive definition of elements, attributes, constraints, and data interactions. The logical view also serves as a framework for developers to write requirements and implement a database that matches the structure of the data model at the conceptual and logical levels. Finally, a physical view identifies the database structure in terms of data tables, attribute data types, and other implementation details. [7]

Figure 2 shows the breakdown of the IDA data model into functional, conceptual, logical, and physical views with references to the report section in which each view is addressed.

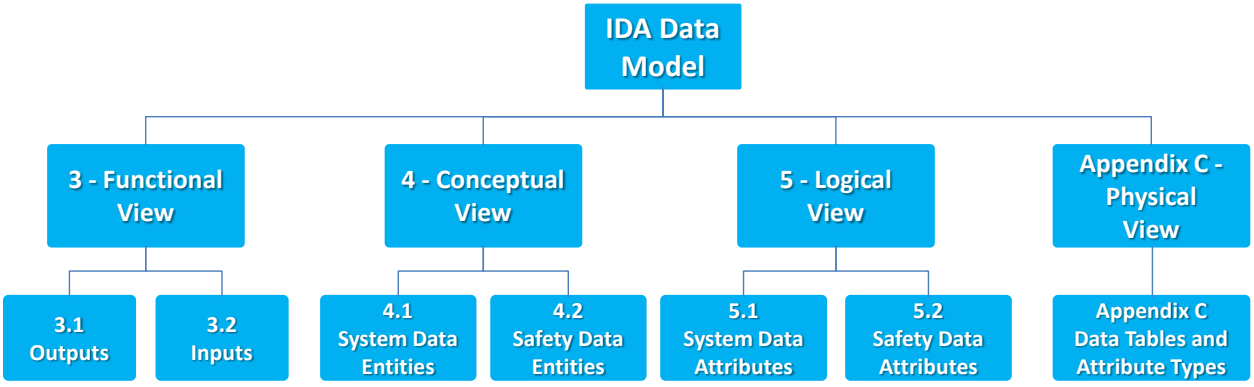

Figure 2. Data model organization

3. FUNCTIONAL VIEW

The functional view of the IDA data model encompasses tool functions, data outputs, and data inputs. The IDA ConOps decomposed the preliminary functional needs for the IDA, that were identified during the AOV needs analysis, into tool functional capabilities. The high-level IDA system functions were defined and organized into a hierarchy. Each system function provides one or more outputs that will support AOV processes. Further IDA research and development conducted since the publication of the ConOps has resulted in refinement and reorganization of the functional hierarchy, but the overall system capabilities defined in the IDA ConOps are retained. Figure 3 shows the current IDA functional hierarchy.

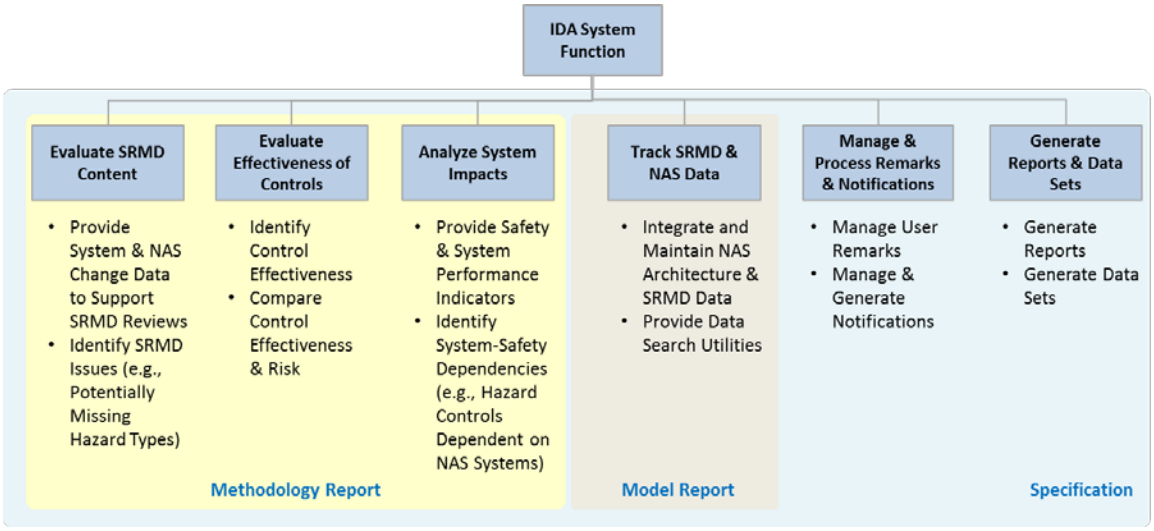

Figure 3. IDA functional hierarchy

This IDA model report provides details on developing the data model to support the identified functions. IDA functions are outlined and mapped to data outputs in section 3.l. Section 3.2 summarizes data inputs in terms of data sources accessible to the AOV and used to assemble the NAS system and safety data for the IDA.

3.1 DATA OUTPUTS

High-level IDA system functions were defined and organized into a hierarchy in the IDA ConOps. Each system function provides one or more outputs that will support the AOV processes. To refine the model development approach, the set of functional outputs was analyzed to determine which could be enabled by basic analysis of the data model (e.g., searching and filtering of modeled data) and which required more complicated or detailed analysis of the data model.

Table 1 shows a list of the high-level IDA functions, sub-functions, and corresponding outputs allocated to the data model and analytical methods. Details of the analytical methods are addressed in the IDA methodology technical report 8]. The primary IDA functions, namely "Evaluate SRMD Content," "Evaluate Effectiveness of Controls," and "Analyze System Impacts," are the focus of the functional allocation in table 1. Supporting functions to assemble and manage NAS and SRMD data and to generate reports and user-configured notifications are omitted because they entail database administration instead of user functionality. Additional details regarding the methods used to generate IDA outputs are provided in the IDA methodology technical report [8].

Table 1. IDA functions and outputs

IDA Function	IDA Outputs	Data Model	Analytical Methods
Evaluate SRMD Content			
Provide System and NAS Change Data to Support SRMD Reviews	High-level description of selected system/subsystem	X	
	Similar SRMDs based on system, system type, or NAS change type	X	
	List of subsystems of selected system	X	
	List or diagram of systems interfacing with selected system	X	
	View hazards from selected similar SRMDs	X	
	View hazard risk ratings from selected SRMDs	X	
	View monitoring tasks from selected SRMDs	X	
Identify SRMD Issues	Interfacing systems not identified in hazard cause list	X	

Table 1. IDA functions and outputs (continued)

IDA Function	IDA Outputs	Data Model	Analytical Methods
	Hazards with a single cause identified	X	
	Hazards with significant risk reduction	X	
Evaluate Effectiveness of Controls			
Identify Control Effectiveness	View controls from selected SRMDs	X	
	Control-effectiveness score		X
Compare Control Effectiveness and Risk	Control importance score		X
Analyze System Impacts			
Provide Safety and System Performance Indicators	NAS impact score for systems		X
	System safety influence score for systems		X
	NCI score for NAS changes		X
	Instability score		X
	Unavailability		X
	Anomaly rate		X
Identify System-Safety Dependencies	List of systems/subsystems interfacing with selected NAS system	X	X
	List of existing hazards potentially influenced by the system		X
	List of existing controls potentially impacted by the system		X
	Dependent NAS systems that may impact availability or hazard likelihood	X	X
	List of service delivery points where system provides services	X	
	Pending NAS changes to interfacing systems	X	

3.2 DATA INPUTS

The IDA data model is based on the collection and assembly of NAS system and SRMD data from a variety of sources. The following sections briefly describe the primary sources of NAS system and safety data that were used for IDA data model inputs.

3.2.1 System Data Inputs

Data sources used to compile information on NAS systems and architecture for the IDA data model include the:

- National Airspace System Enterprise Architecture (NAS EA) system views (SVs) and Operational Views (OVs)—The NAS EA exists to assist in NAS enterprise-level decision making. The NAS EA reports describe the composition of the NAS and high-level interconnections among lower level elements that make up the NAS. The SV and OV reports provide an organized hierarchical representation and partitioned relationship of entities within the NAS. They also provide a series of detailed diagrams showing interconnections between NAS systems and examples of data flows between NAS elements. The NAS EA's SVs and OVs provided an initial understanding of the overall NAS.
- NAS Systems Engineering Portal (SEP)—The Systems Engineering Information Management Division manages the SEP website on the FAA Intranet (https://sep.faa.gov/). This site replaces and updates the NAS EA portal that was used to develop the original IDA dataset. The SEP includes the NAS EA SV and OV reports for the as-is, mid-term, and far-term NAS. It also provides an interface for downloading reports of data from the NAS EA effort, including a system inventory, NAS hierarchy elements, and a list of NAS facilities. Data from these reports provided much of the high-level data on NAS systems in the IDA data model. The SEP also provides information on planned changes to NAS systems, which provide supplemental information to model NAS changes in the IDA.
- System Maintenance Handbooks—Maintenance handbooks for many NAS systems are available in libraries linked from the FAA's TechNet Intranet site. System maintenance handbooks proved to be good sources of data for descriptions of subsystems. The major subsystems or functional blocks of each system are usually described, along with an overview of the interactions between them. Engineering judgment is required to consolidate the narrative information and diagrams into the data points required for the IDA data model.
- NAS MD-0001 Query Tools—The FAA's Configuration Control Board (NAS MD-0001) maintains a set of query tools at repcon.faa.gov. The site enables searching for the latest versions of technical and reference documents related to a NAS system. Although the site itself only has links to Interface Requirement Documents (IRDs) and Interface Control Documents (ICDs), the list of documents and owning organizations can be used to expand searches on other sites or request additional supplemental documentation. The IRDs and ICDs provide details on system interfaces that are captured in the IDA datasets. The repcon.faa.gov website also enables queries on National Airspace System Change Proposals (NCPs). Although the site does not link to the NCPs themselves, the search tools

can be used in conjunction with the FAA's Web Configuration Management (WebCM) site to find particular NAS changes and related documentation.

- WebCM—The FAA's Enterprise Configuration Management group maintains the WebCM site (webcm.faa.gov) on the FAA's Intranet. WebCM is used to manage NCPs from initial submission by the change proponent to final decision. NCPs include details on proposed changes to the NAS, and approved NCPs often have supplemental details attached to the record in WebCM. This can be a useful source of information on changes that have been made to the NAS since the baseline NAS configuration was characterized in the dataset. SRMDs are also attached to those NCPs that require them, making WebCM a source of additional SRMD data as well.
- Facility, Service, and Equipment Profile (FSEP)—The FSEP is an inventory of the physical equipment that makes up the NAS infrastructure. Each system in the IDA is represented by one or more FSEP codes that describe the system variant or type. The FSEP data are maintained by ATO Technical Operations (TechOps) and made available via the FAA's TechNet Intranet (https:\\technet.faa.gov). Data from the FSEP database can be used to link each IDA system to the service delivery points (SDPs) that use the system or are responsible for the equipment.

The IDA data model also stores certain system performance metrics and data about the SDPs where NAS systems are operational. The data used to identify this information are obtained from the following source:

- Remote Maintenance Logging System (RMLS)—The RMLS is used to record and track logs from TechOps at facilities across the NAS. The RMLS Logs of Corrective Maintenance provide a source of data for calculating anomaly rates for systems. The RMLS Log of Interrupt Requests is used to calculate system unavailability on a monthly basis. RMLS logs are available on the FAA's TechNet Intranet (https:\\technet.faa.gov).

Two additional resources have been identified that provide information on planned changes to the NAS and NAS systems.

- NAS Capital Investment Plan (CIP)—The CIP is an FAA plan, submitted to Congress annually, which describes the planned FAA investments in the NAS over the next 5 years. It contains a comprehensive CIP for the FAA, which includes funding for each budget line item for the upcoming 5 fiscal years, with total funding for each year of the plan constrained to the funding targets for those years as estimated and approved by the Office of Management and Budget. Along with other components, it describes and outlines the implementation timelines for NextGen Operational Improvements.
- NAS EA Infrastructure Roadmap—The NAS EA Roadmap is a document, updated annually, that captures the plan for the evolution strategy of the NAS. It is a joint effort of the EA office, Joint Planning and Development Office, ATO service units, and all other FAA stakeholders who plan for initiatives required to sustain the NAS through the year 2025 and beyond. It provides the integrated decisions and synchronized investments needed to deliver NextGen and evolve the NAS (technology, policy, strategy, training, procedures, research, etc.). The NAS EA Roadmap is available on the NAS SEP website (https://sep.faa.gov/).

3.2.2 Safety Data Inputs

Identified hazard and related safety data on NAS systems and NAS changes are contained in SRMDs. The IDA data model captures SRMDs from several sources, including the:

- WebCM—The FAA's Enterprise Configuration Management group maintains the WebCM site (webcm.faa.gov) on the FAA Intranet. WebCM is used to manage NCPs from initial submission by the change proponent to final decision. In addition to details about the changes to NAS systems in the NCPs, WebCM also includes SRMDs, or Safety Risk Management Decision Memos (SRMDMs), for the changes. These SRMDs or SRMDMs are attached to those NCPs that require them, making WebCM a source of additional SRMD/SRMDM data.
- Technical Operations (AJW) NAS Digital and NAS Document Libraries—AJW maintains libraries of technical documents related to maintenance of systems under their purview. These libraries are accessible via the TechNet website on the FAA Intranet. Although the document libraries are primarily a source of Technical Interchange Bulletins (TIBs) and system architecture data, many of the system support directives include SRMDs for the changes detailed in the bulletins.
- Safety Management Tracking System (SMTS)—The ATO is required to maintain a repository of hazard-tracking data. To fulfill this requirement, the ATO set up the SMTS. The SMTS is an online tool for entering safety analyses and tracking hazards and for monitoring plans throughout their lifetime. It replaced the earlier ATO tool known as the SRM Tracking System. The SMTS is a relatively new system and data from older SRMDs do not appear to be entered at this time. As ATO expands its use of the SMTS, it may be possible to obtain more safety data from this system going forward.

4. CONCEPTUAL MODEL

The IDA ConOps is based on modeling NAS equipment architecture elements, NAS safety data elements, and the interactions between these elements. The IDA is envisioned as more than simply a repository of SRMD data: by developing a model-driven approach, it is possible to identify interactions between systems and safety hazards that might not be immediately apparent to an individual AOV analyst.

The conceptual model describes the basic entities and their relationships modeled by the IDA. The conceptual model is the first step toward defining the complete data model, which includes entity attributes that will be used by the IDA. The IDA conceptual model is assembled by identifying, organizing, and linking the various entities that describe the NAS system and safety information.

Figure 4 shows the overall IDA conceptual model. This conceptual model identifies the one-to-one, one-to-many, and many-to-many relationships among NAS systems, interfaces, NAS changes, SRMDs, hazards, causes, and controls. Omitted from this view are metric reports, remarks, and notifications, which are described in the following sections. As system and safety data are modeled by the IDA, it is possible to identify indirect system interactions and dependencies, common hazard causes, hazard mitigations that are commonly used, and other outputs described in section 2.1. This view is a composite of all of the individual views shown in

figures 2–5 and provides an overview of all the key entities and relationships in the IDA conceptual model.

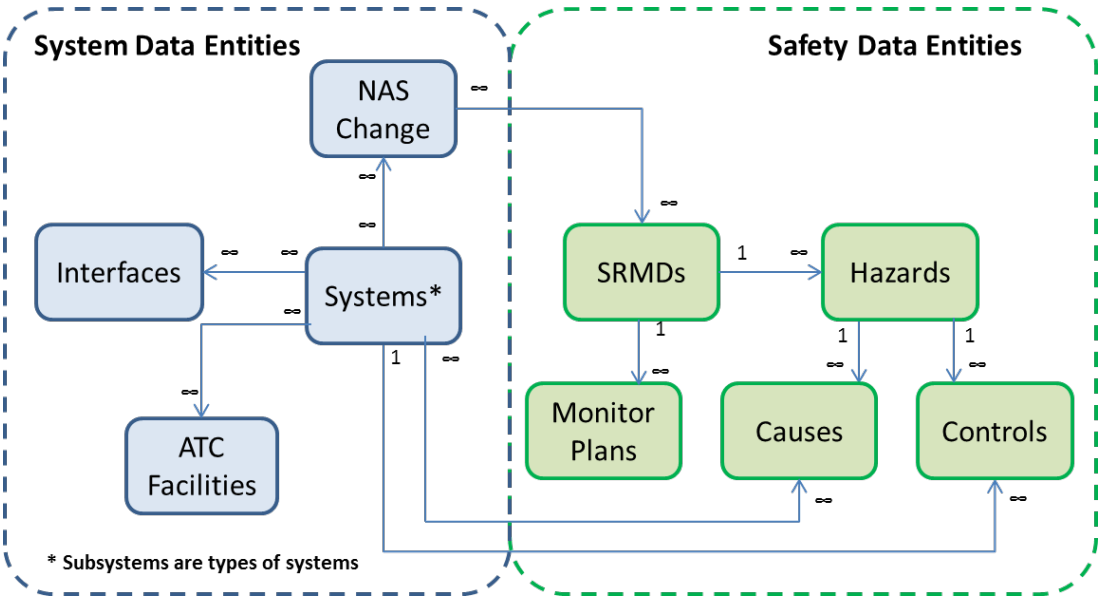

Figure 4. IDA conceptual view

4.1 SYSTEM DATA ENTITIES

The first set of entities that are modeled deal with NAS system architecture. NAS systems are defined as an integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These systems may be thought of as functional units that interact with other systems and users to provide data and functionality that support operations in the NAS. Systems may contain subsystems that provide specific functions or enable interactions with other systems. Data about systems are captured in system-specification documents, maintenance manuals, and TIBs. Systems are installed at or provide service to SDPs, which may include (but are not limited to) radar sites, airports, or ATC facilities. A particular SDP may have multiple systems installed and operational at a given point in time.

Once particular NAS systems are identified, and the facilities at which they are located are described, the interfaces between systems must be identified and modeled. Each NAS system receives input from other systems/users and provides outputs to other systems/users. The data and command inputs and outputs are modeled as interface entities in the IDA data model.

Changes to systems are captured as NAS change reports. A NAS change may be a minor system modification or a large, multi-phased technical refresh or system acquisition effort. NAS changes provide the link between systems and SRMDs and also allow the IDA to track and report on pending and planned NAS changes, which may not yet have completed SRMDs.

The IDA also maintains various indicators that further describe the performance and safety impact of each modeled system. These metric reports are stored as records that describe the systems. This modeling method allows the IDA to capture and track each system's metrics over time, which may

indicate safety issues related to a system. Specifics about the metrics recorded for each system are provided in section 5 and appendix B.

Figure 5 shows a conceptual model view of the system and interface entities, which are colored blue. Two safety-related entities (Cause, and Control) are also shown and colored green.

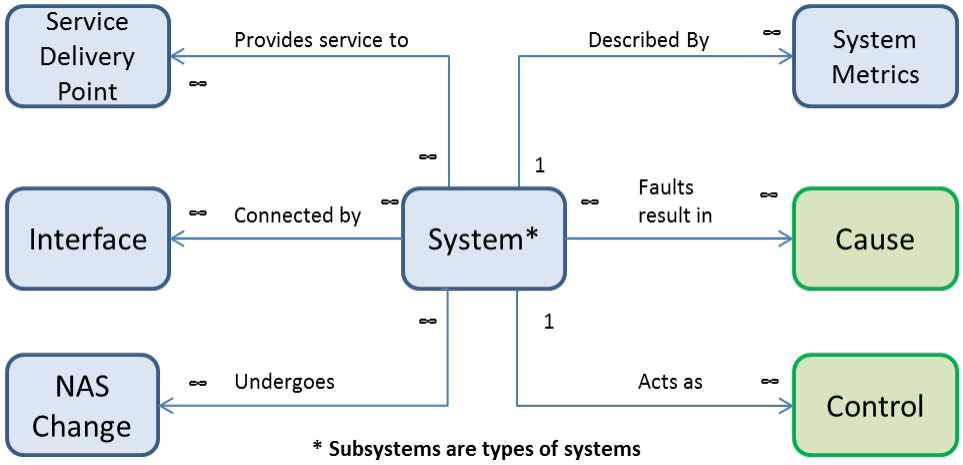

Figure 5. System entity relationships

4.2 SAFETY DATA ENTITIES

The second set of entity relationships modeled in the IDA is related to NAS safety-hazard data. These model entities capture and characterize information from SRMDs that have been written to analyze changes to the systems in the NAS system model. An SRMD describes and analyzes changes in one or more NAS systems. The SRMD identifies hazards that may result from the proposed NAS change, as well as a hazard-monitoring plan. These entities are shown in figure 6.

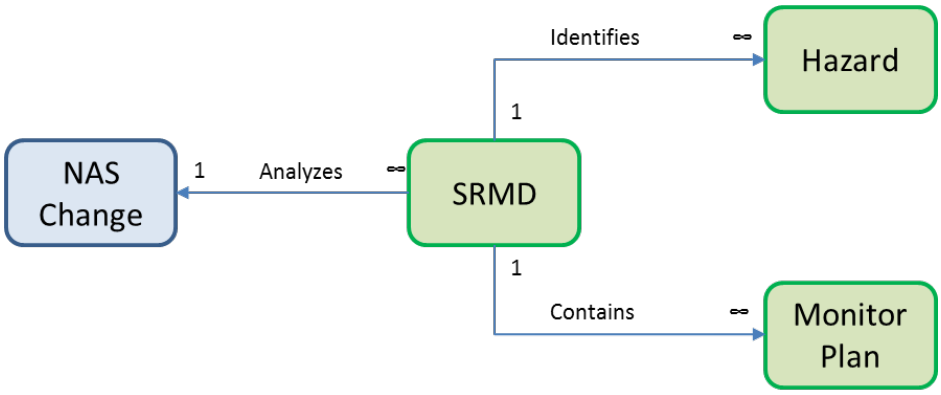

Figure 6. SRMD entity relationships

Each hazard identified in an SRMD is analyzed to identify the hazard causes that trigger the hazard and controls that mitigate the identified safety hazards. Hazard causes identified in an SRMD are linked in the IDA data model to the hazard that they cause. Similarly, the existing controls and

recommended safety controls are modeled as entities and associated with the hazard they mitigate. Figure 7 illustrates the relationships between entities related to the hazard entity in the IDA conceptual model.

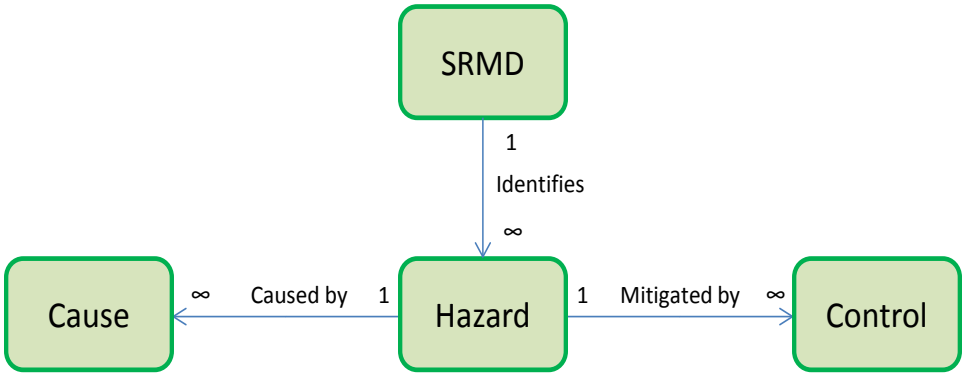

Figure 7. Hazard entity relationships

Hazard causes may be linked to NAS systems. If a hazard cause is a fault, error, or failure in the system being analyzed, it is classified as an "internal cause." If the cause is a fault, error, or failure in a different system than the primary one analyzed in the SRMD, it is classified as an "external cause." Similarly, hazard controls may be internal controls linked to the primary system addressed in the SRMD, or they may be external controls linked to other NAS systems. In addition, controls may also be related to procedures or training, in which case they will not be linked to a system at all but only to the hazard. The relationships that affect the Cause And Control entities are shown in figure 8.

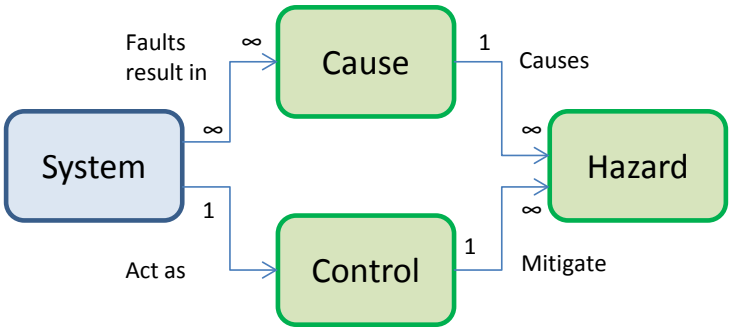

Figure 8. Cause and Control entity relationships

A final entity in the IDA data model is the Remark. Remarks are not strictly related to systems or safety data but rather can be attached to various other entities in the data model. Remarks will enable IDA users to add supplemental information and action items to entities in the IDA data model. These remarks will then be visible to other users and provide additional information and lessons learned from prior analyses that may be of use to AOV users in their safety oversight roles. Figure 9 illustrates the relationships that the Remark entity shares with other elements of the data model.

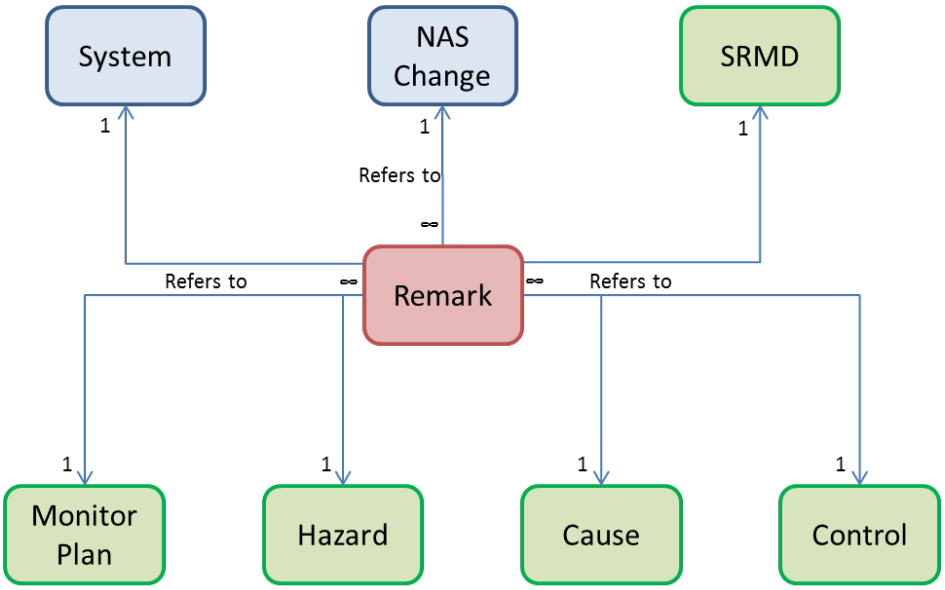

Figure 9. Remark entity relationships

5. LOGICAL VIEW

After the conceptual model has been described, the next step in development is to define the data model. The data model extends the conceptual model of entities and relationships to describe the logical and physical organization of the data [9].

Entities in a data model are represented by tables in a relational database. Entities are described by attributes that can be stored as columns in a table. A primary key (PK) is an attribute that uniquely defines a record in a table. A foreign key (FK) identifies a PK in a different table and is used to indicate a relationship between entities in the data model. The distinction between a PK and an FK is that an FK in one record points to a PK in another record as a source. For example, an SRMD will have one or more hazards. A PK identifies the SRMD record. An FK from one or more records in the hazard table would point back to the SRMD as the source. Also, in some situations, there may be a composite key, which is made up of more than one field in a table to uniquely identify a record.

Developing a logical data model from a conceptual model requires that each entity be defined with a PK attribute for identification. Additional attributes of each entity are defined so the data collected on that entity can be fully described. Next, the relationships between the entities are defined with FK attributes. Finally, a logical schema may be produced that describes the architecture of the entity tables, attributes, and relationships in the data model.

The logical data model can then be translated into a physical model that describes and defines the implementation of a relational database. The resultant database may include additional tables, properties, and operations to support or better describe the key entities in the conceptual model, but will implement the entities and relationships defined in the logical data model. The database that is implemented based on the IDA data model can be queried, searched, filtered, and analyzed to generate the outputs described in section 2.1.

Figure 10 shows a simplified logical view of the IDA data model. The attributes used as keys for each entity are shown for each entity, along with a sample of other attributes that describe the entities. Sections 5.1–5.2 provide complete descriptions of each entity's defined attributes. System and interface entities are colored blue, whereas safety-related entities are colored green. Remarks are omitted from this view for clarity, as are supplemental tables of properties and metrics that describe the primary entities.

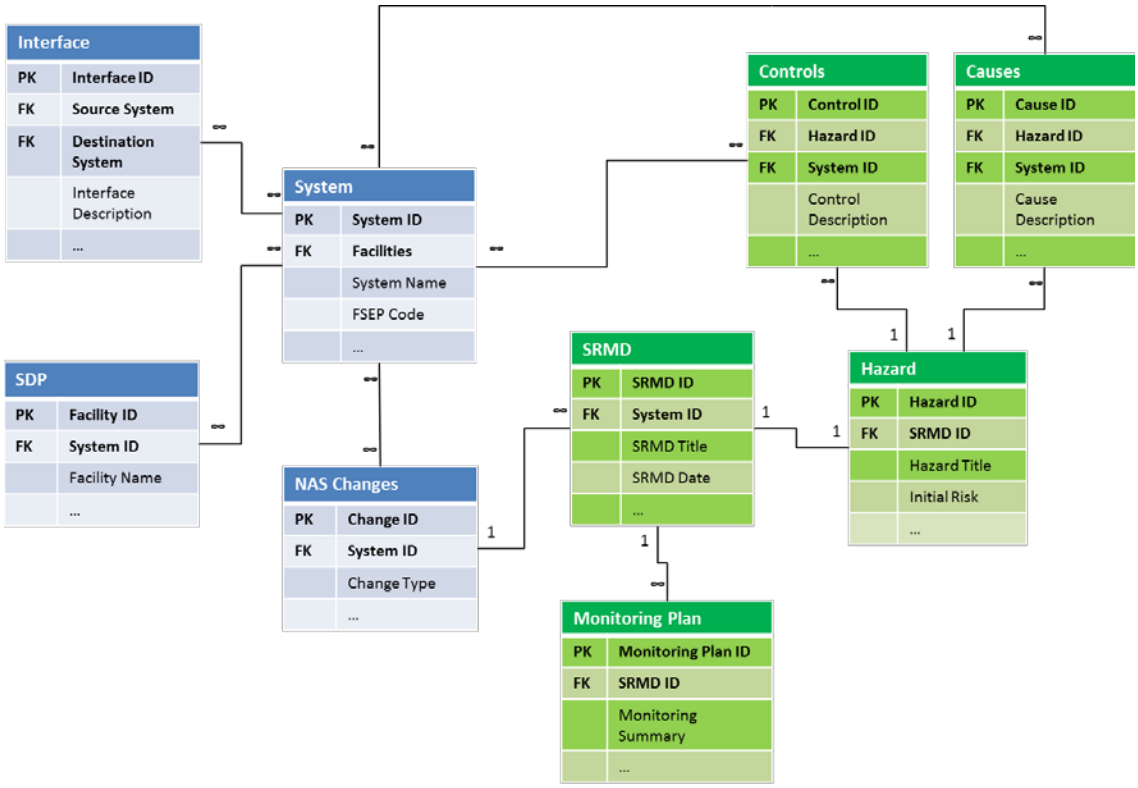

Figure 10. IDA logical view

5.1 SYSTEM DATA ATTRIBUTES

NAS architecture data are captured by two main entities in the IDA data model: Systems and Interfaces. Two additional entities, SDPs and NAS changes, are used to capture additional properties and interactions of NAS systems.

5.1.1 Systems

Systems are modeled as functional units that provide data and functionality that support operations in the NAS. Systems may contain subsystems that provide specific functions or enable interactions with other systems. The IDA tool is intended to address NAS system equipment that is under the FAA ATO line of business, so the system entities represent the ground-based systems and equipment that make up the NAS. Aircraft and airborne systems are not modeled in detail.

Eight NAS systems were chosen for initial study and modeling by the IDA. These systems were chosen because they provide a representative cross section of system types, they represent varying levels of life-cycle maturity, and SRMDs have been written to identify hazards in each one. The eight chosen systems follow:

- Airport Surveillance Radar model 11 (ASR-11)
- Standard Terminal Automation Replacement System (STARS)
- Common Automated Radar Terminal System (CARTS)
- En Route Automation Modernization (ERAM)
- Advanced Technologies and Oceanic Procedures (ATOP)
- Airport Surface Detection Equipment, Model X (ASDE-X)
- Enhanced Terminal Voice Switch (ETVS)
- Runway Status Lights (RWSL)

Key properties of systems that are captured in the IDA data model are described in table 2. It should be noted that subsystems are modeled as a type of system in the IDA. NAS systems contain subsystems that provide specific data, functional processing, and interactions with other systems. These subsystems are captured as system entities in the data model that are contained in (or owned by) a parent system entity. By modeling systems and subsystems with the same type of model entity, it is possible to examine NAS architecture at varying levels of detail, either at a system or subsystem level. Subsystem entities possess many, but not all, of the same attributes as their parent systems; attributes applicable to subsystems are indicated by an asterisk.

Table 2. System entity attributes

Attribute	Description	Keys
System ID*	Unique identification number for the system	PK
System Name*	The full name of the system	
System Acronym*	The commonly used acronym for the system	
System Description*	A brief overview of the system, purpose, major functions, inputs/outputs, users, and other general information	
NAS Element/Sub-element Classification	The element and sub-element in the NAS hierarchy that the system is classified under (e.g., automation, surveillance, weather)	
NAS EA Portal Number	The ID number assigned to the system in the NAS enterprise architecture reports	
FSEP Codes	The FSEP codes for the system and its variants	
Primary Users	The classes of users who primarily interact with the system	
System Reference Documents*	Documents that provide details or supplemental information about the system and architecture	
Facilities	Facilities where the system is currently installed	
Parent System ID*	Applies to subsystem only: The system ID for the system that contains the subsystem	FK

External systems, such as aircraft and airborne systems, will not be explicitly modeled by the IDA and will be captured only to the extent required to indicate an interface with ATO NAS system equipment. NAS users (ATC, TechOps, pilots, etc.) will be identified as interacting with ATO NAS system equipment, but user procedures and tasks are not modeled in the IDA.

5.1.2 Interfaces

The other key entity defined in the IDA data model of NAS architecture is Interfaces. Interfaces describe the data flows between NAS systems. Each NAS system receives inputs from other systems/users and provides outputs to other systems/users. The IDA captures data flows between systems by modeling them as Interface entities. The data that characterize the system interactions in the IDA data model may be captured from IRDs, ICDs, system specifications, and system maintenance manuals, and from EA modeling that has been done by other FAA programs.

The key properties of interface entities that are captured in the data model are described in table 3.

Table 3. Interface entity attributes

Attribute	Description	Keys
Interface ID	Unique identification number for the interface	PK
Source System ID	The system (or subsystem) that sends data via the interface	FK
Destination System ID	The system (or subsystem) that receives data from the interface	FK
Interface Type	The type of interface being modeled (Note: only data interfaces are modeled in the IDA at this time)	
Interface Description	High-level description of the interface between the source system and its destination system	
Data Description	A description of the data exchanged via the interface	
Data Format	The format or protocol used to exchange data on the interface	
Interface Reference Document	Documents that provide details or supplemental information about the interface	

5.1.3 SDPs

SDP entities represent the locations where systems are installed and operated. A facility may consist of a single piece of equipment, such as a standalone VHF Omnidirectional Range, or it may have many systems collocated or co-managed, such as an ATC tower/TRACON facility with local radar, voice switches, and other systems. The IDA models the SDPs that receive and manage the facility equipment. SDP data, including facility equipage, is obtained via the FSEP search tools on the FAA's TechNet website.

The key properties of SDPs that are captured in the data model are described in table 4.

Table 4. SDP entity attributes

Attribute	Description	Keys
Record_ID	Unique identification number for the records downloaded from TechNet	PK
FacilityCode	Three- (or four-) letter facility identification code, as defined in FAA Order JO 7350.9	
EquipIdent	An identifier for the equipment type or class	
FacilityLoc	The city where the equipment is located	
FacilityState	The state where the equipment is located	
RestorationCode	Code indicating the number of hours allowed for TechOps to restore service	
FSEP_Code	The FSEP Fac_Code used to identify the specific system variant installed at a location. It consists of a system ID field (1 character), facility field (4 characters), and class field (1 character)	FK
EquipStatus	Code to indicate if the equipment is operational at the installed site	
ResponsibilityCode	A 1-character code assigned by TechOps that identifies the owner of the equipment and who is responsible for maintenance, certification, and inspection	
FSEPSysID	The system ID field of the FSEP code is a 1-character identifier that indicates how the system is used in the NAS	
FSEPFacility	The facility field of the FSEP code is a four-character identifier consisting of a one-digit capability code, two-digit type code, and one-digit model code	
FSEPClass	The class field of the FSEP code is a one-character alphanumeric code further identifying equipment, as defined in the FSEP Desk Guide.	
SDP_Ident	The three-letter acronym for the SDP that is primarily responsible for/the recipient of data from the equipment	
SDPType	The type of SDP represented by the facility	

5.1.4 NAS Changes

The eight systems addressed in the initial IDA data model are at various stages in the FAA Lifecycle Management Process. Some systems (e.g., RWSL) are relatively new and still going through system acquisition, whereas others are already in service or in the process of going through Tech Refresh to replace obsolete components (e.g., ASDE-X). Still others are approaching end-of-life and will be replaced by other new systems and then decommissioned (e.g., ETVS). The IDA data model is intended to account for changes in NAS architecture over time; therefore, planned NAS changes and key lifecycle dates must be captured in the model.

Each change to a system modeled in the IDA is captured as a NAS change entity. Completed and in-progress NAS changes may be linked to one or more SRMDs that analyze the change, whereas planned and in-progress NAS changes may have only high-level NAS change details recorded. Schedule data for these attributes are identified in the NAS CIP and NAS EA Infrastructure Roadmap and may be added or edited by IDA users who possess the appropriate permissions.

Table 5 provides a summary of the attributes about NAS changes that will be captured in the IDA data model.

Table 5. NAS change entity attributes

Attribute	Description	Keys
NASChange ID	Unique identification number for the change	PK
System ID	The system to be changed	FK
Change Type	The NAS change type classification that describes the planned change	
Change Title	Brief title to identify the NAS change	
Change Description	High-level description or overview of the planned change	
Start Date	The date when the change implementation began (or is planned to begin)	
End Date	The date when the change implementation ended (or is scheduled to end)	
Change Status	The current state of the change (e.g., planned, in-process, complete)	
NAS EA Change ID	The ID number for the change used in the NAS EA Roadmap	
CIP Reference ID	The ID number for the project in the FAA CIP document	

5.2 SAFETY DATA ENTITIES

The other group of elements in the IDA data model represents NAS safety data. The attributes of entities in this group are derived from SRMDs prepared by the ATO. Each SRMD identifies hazards, hazard causes, and controls that mitigate the identified safety hazards associated with NAS changes.

The ATO SMS manual describes the methods and activities that must be used to identify and treat safety risks in the NAS. When a change to the NAS is proposed, an SRM panel is convened to identify hazards related to the change. Risks associated with the hazards are analyzed in terms of severity and likelihood. The hazards are then treated by developing controls to mitigate the effects or reduce the likelihood of each hazard. According to the ATO SMS manual, hazards that are classified as having high risk must be treated to reduce the risk to medium or low. The results of the formal safety assessment are documented in an SRMD, which must be approved by the appropriate stakeholders and authorities. The ATO SMS manual defines who must approve SRMDs and accept the risks identified for the NAS change. SRMDs that contain HRHs must be submitted to the AOV for review and approval of the proposed hazard controls. The IDA will model safety data from all available SRMDs, not just those that contain HRHs.

There are five entities that represent the key safety data modeled by the IDA: SRMDs, hazards, causes, controls, and monitoring plans.

5.2.1 SRMDs

SRMDs that are captured in the IDA data model are those that address NAS changes, including hardware changes, software upgrades, and the introduction and integration of new systems at one or more NAS facilities. Each SRMD is linked to a NAS change in the data model. To be included in the IDA data model, SRMDs must meet the following criteria:

- The document must be an SRMD and not an SRMDM.
- The change to the NAS addressed in the SRMD must be focused on NAS equipment; this excludes air traffic procedural waivers.
    - Note: Future IDA research may address ATC procedures; non-equipment SRMDs may be incorporated into the model at that time.
- The SRMD must be approved by all required parties.
    - Note: SRMDs may exist in a “draft” state. These SRMDs may be added to the database but will not be used to calculate safety indicator scores.
- The SRMD must be available via the FAA’s WebCM, ATO NAS digital library, or AOV Connect because these sources are accessible for the IDA research effort and do not require special permission for the AOV to obtain an ATO SRMD.
- The SRMD must be dated after May 2008 (the date on which the ATO SMS manual version 2.1 went into effect).

- (Note 1: Some SRMDs dated after May 2008 may be developed in accordance with ATO SMS manual version 1.1).
- (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 2007).

In the IDA data model, an SRMD entity is linked to one NAS change. By querying the NAS change entity, IDA can determine the system or systems that are analyzed by the SRMD. Each SRMD is linked to one or more hazards and one or more monitoring parameters identified in the SRMD. Table 6 provides a list of attributes that describe SRMD entities.

Table 6. SRMD entity attributes

Attribute	Description	Keys
SRMD ID	Unique identification number for the SRMD.	PK
NASChange ID	Unique IDA identification number for the NAS change associated with the SRMD.	FK
SRMD Title	The complete title of the SRMD.	
Document number	The document tracking number for the SRMD, if any.	
SRMD Version	The version number associated with the SRMD, if any.	
SRMD Date	The effective date on the cover page of the SRMD.	
SRMD Summary	A high-level description and overview of the NAS change analyzed by the SRMD. May be drawn from the executive summary.	
SMS Version	The version of the ATO SMS manual under which the SRMD was prepared.	
NAS Change Type	The NAS change type classification that best describes the change analyzed in the SRMD.	
SRMDStatus	Flag to indicate the current status of the SRMD (Draft = 2, Active = 1, Inactive = 0).	
ShortTitle	An abbreviated SRMD title that can be used in the IDA User Interface displays.	

5.2.2 Hazards

In the IDA data model, a hazard entity is linked to the SRMD which identifies the hazard. A hazard also links to one or more causes identified in the SRMD as potentially triggering the hazard. One

or more controls (existing and recommended) that mitigate the risk associated with a hazard is also linked to the applicable hazard.

The IDA data model captures hazards from equipment-related SRMDs so all the hazards modeled will be related to NAS equipment under the jurisdiction of the ATO. Hazards arising from changes to procedures, facility waivers, security concerns, or occupational safety are not in-scope for this version of the IDA. These hazards are analyzed and treated through other processes and organizations and should not be identified in any of the SRMDs that meet the criteria outlined in section 5.2.1.

Table 7 provides a list of attributes that describe hazard entities.

Table 7. Hazard entity attributes

Attribute	Description	Keys
Hazard ID	Unique identification number for the hazard.	PK
Hazard Title	The title and description of the hazard as identified in the SRMD.	
SRMD ID	The SRMD in which the hazard is identified.	FK
Hazard Number	The number assigned to the hazard in the SRMD.	
System State	A description of the worst-case system state as identified in the SRMD.	
Hazard Effect	The potential effect(s) listed for the hazard in the PHA or hazard analysis worksheet included in the SRMD.	
Initial Severity	The initial (or current) severity rating for the hazard.	
Severity Rationale	Brief description of the reason for the initial severity rating from the PHA/HAW.	
Initial Likelihood	The initial (or current) likelihood rating for the hazard.	
Likelihood Rationale	Brief description of the reason for the initial likelihood rating from the PHA/HAW.	

Table 7. Hazard entity attributes (continued)

Attribute	Description	Keys
Initial Risk	The initial (or current) risk rating for the hazard from the PHA/HAW.	
Residual Severity	The predicted residual severity rating for the hazard after implementing all recommended controls.	
Residual Likelihood	The predicted residual likelihood rating for the hazard after implementing all recommended controls.	
Predicted Residual Risk	The predicted residual risk rating for the hazard after implementing all recommended controls.	
Hazard Classification/ Sub-class	The hazard type class and sub-classification that best describe the type of hazard identified. Used to identify similar hazards.	
Comment	Supplemental details about the hazard from the PHA/HAW or SME who entered the hazard.	

PHA = preliminary hazard analysis; SME = subject matter expert

5.2.3 Causes

Hazard causes are the events, faults, failures, flaws, and issues that result in the occurrence of a hazard. Causes are stored as entities in the IDA data model. Each cause record is linked to the hazard that identifies it. Causes may also be linked to a system entity that is the source of, or implicated in, the identified cause. Causes that are due to human errors or environmental conditions will not be linked to a NAS system. Table 8 provides a list of attributes that describe cause entities.

Table 8. Cause entity attributes

Attribute	Description	Keys
Cause ID	Unique identification number for the cause.	PK
Hazard ID	The hazard that identifies the cause.	FK
Cause Description	The description of the cause in the PHA/HAW.	
Cause Class/ Sub-class	The cause type class and sub-classification that best describe the type of cause identified. Used to identify similar causes.	
System ID	The system whose function, fault, or failure is involved in the hazard cause.	FK

5.2.4 Controls

Controls are the systems; safety devices; warnings and cautions; procedures; training requirements; and directives that are used to prevent the occurrence of, or mitigate the effects of, hazards. Controls are stored as entities in the IDA data model. Each control record is linked to the hazard that identifies it. Controls may also be linked to a NAS system entity that provides the control or required functionality. Non-system controls (e.g., procedures, training) are not linked to a NAS system entity.

According to the ATO SMS manual, a control is anything that prevents or reduces a hazard's occurrence or mitigates its effects. There are two states that a control may be in: existing or recommended. A control is considered existing if it has been validated and verified with objective evidence. If it is not validated and verified with objective evidence, it is considered a recommended requirement.

Existing controls contribute to the initial or current risk of a hazard, whereas recommended controls contribute to the evaluation of the predicted residual risk of a hazard. When a recommended control is validated and verified as implemented, its status will change to existing and it will become part of the baseline for the system and future hazard analyses. The IDA data model accounts for these states by flagging a control as "existing" or "recommended" and changing this flag as appropriate.

Table 9 provides a list of attributes that describe control entities.

Table 9. Control entity attributes

Attribute	Description	Keys
Control ID	Unique identification number for the control.	PK
Hazard ID	The hazard that identifies the cause.	FK
Control Description	The description of the control (or recommended safety requirement) in the PHA/HAW.	
Existing/ Recommended	A flag indicating whether the control is an existing control or a recommended safety requirement.	
Control Class/ Sub-class	The control type class and sub-classification that best describe the type of cause identified. Used to identify similar controls.	
Internal/ External	A flag indicating if the control is internal or external to the system analyzed by the SRMD.	
System ID	The system whose function, presence, or operation is involved in providing or enabling the control.	FK

5.2.5 Monitoring Plans

According to the ATO SMS manual, hazards that are identified as having an initial or residual risk of medium or high must be formally monitored for the lifecycle of the system or change, or until the risk is mitigated to low. Monitoring must also be done to verify the effectiveness of the controls mitigating the risk. SRMDs must provide a plan for ongoing monitoring of the hazard and the proposed controls.

The details of the monitoring plan and the specific monitoring tasks are captured as entities in the IDA data model. Each monitoring task (or the monitoring summary) is linked to the SRMD that identifies it. Table 10 provides a list of attributes that describe monitoring plan entities.

Table 10. Monitoring plan entity attributes

Attribute	Description	Keys
Monitoring Plan ID	Unique identification number for the monitoring plan task	PK
SRMD ID	The SRMD that identifies the monitoring plan task	FK
Monitoring Summary	Brief description of the overall monitoring plan as identified in the SRMD	
Monitoring Activity/Task	Brief description of the specific task or activity to monitor the parameter as specified in the SRMD	
Responsible Monitoring Organization	The organization or office identified in the SRMD as responsible for performing the specified monitoring and reporting	
Monitoring Due Date/ Frequency	Schedule of monitoring requirements as specified in the SRMD	
Monitoring Comment	Additional details or comments on the plan entered by the SME entering the SRMD	

5.3 INDICATORS AND METRICS

In addition to the primary model elements described in sections 5.1 and 5.2, the IDA data model also stores indicator scores related to systems, NAS changes, and controls. These scores are stored in the database and are attached to the applicable elements, as described below.

5.3.1 System Metrics

IDA incorporates certain system performance and safety metrics in its model. These metrics use equipment performance data (such as unavailability and anomaly rates) and other indicator scores (such as instability and hazard influence). Because metric scores are expected to change over time, the IDA data model stores historical scores for each system in the IDA data model.

Refer to the IDA Methodology Report 8] for details pertaining to calculating system performance metrics. Table 11 provides a list of attributes that describe system metric report entities.

Table 11. System metric report attributes

Attribute	Description	Keys
Metric Report ID	Unique IDA identification number for the system metric report	PK
Metric Report Date	The date associated with the system metric report	
System ID	The IDA system ID number for the NAS system	FK
Dependency	The system dependency score on the report date	
Cause Influence	The cause influence score on the report date	
Control Influence	The control influence score on the report date	
Hazard Influence	The hazard influence score on the report date	
Unavailability	The system unavailability rate for the previous month calculated by the IDA on the report date	
Anomaly	The anomaly rate on the report date	
Stability	The system stability score on the report date	

5.3.2 NAS Change Metrics

The IDA incorporates certain metrics about the NAS changes tracked in its model. These metrics include the complexity and maturity of the change and the overall NCI score. Each NCI score is associated with a single NAS change in the IDA data model. Refer to the IDA Methodology Report for NCI calculation details. Table 12 provides a list of attributes that describe NAS change metric report entities.

Table 121. NAS change metric report attributes

Attribute	Description	Keys
Change Metric Report ID	Unique IDA identification number for the NAS change metric report	PK
Change Metric Report Date	The date associated with the metric report	
NAS Change ID	Unique IDA identification number for the NAS change being scored	FK
Complexity	The change complexity parameter score for the NAS change as of the report date	
Maturity	The change complexity parameter score for the NAS change as of the report date	
NCI	The NCI score for the NAS change as of the report date	

5.3.3 Control Effectiveness

One of the primary functions of the IDA is to help evaluate control effectiveness. A control-effectiveness score is determined for the set of controls that mitigate each hazard. The overall control-effectiveness score and parameter values used to determine each score are tracked in the IDA data model. Refer to the IDA Methodology Report for control-effectiveness scoring details. Table 13 provides a list of attributes that describe control-effectiveness data entities.

Table 13. Control-effectiveness attributes

Attribute	Description	Keys
Hazard ID	Unique IDA identification number for the hazard	FK
Suitability	Flag indicating whether the controls satisfy the suitability check	
Detectability	Flag indicating whether the controls satisfy the detectability check	
Breadth	Flag indicating whether the controls satisfy the breadth check	
Depth	Flag indicating whether the controls satisfy the depth check	
Autonomy	Flag indicating whether the controls satisfy the autonomy	
CE Score	Control-effectiveness score for the hazard	
CI Score	Control-importance score for the hazard	

6. DATABASE IMPLEMENTATION

As part of the IDA data-modeling effort, a preliminary database was developed in 2014 to implement and test the basic structure and organization of the IDA data model. This preliminary database was used to support the analytical methodology development and to verify the integrity of the preliminary model and data. This database was used to further refine the IDA data model and capture additional system and safety data. The preliminary IDA database model was implemented using Microsoft® Access® 2010.

In early 2015, work began on converting the preliminary IDA database to the MySQL platform. MySQL comprises an open-source set of tools designed for developing and managing structured query language databases. The new database used the preliminary Microsoft Access database as a starting data source, but standardized naming conventions expanded the number of data tables and relationships. This allowed the database to better support IDA application development. The data dictionary in appendix A and the physical database view in appendix C reflect the IDA database as currently implemented.

7. CONCLUSIONS

The Integrated Domain Assessment (IDA) data model expands upon the initial IDA dataset by defining and structuring the relationships between National Airspace System (NAS) system and safety data entities. These entities include NAS system equipment, system interfaces, air traffic service delivery points, NAS system changes, Safety Risk Management Documents (SRMDs), hazards, causes, controls, and monitoring parameters.

The data model is comprised of views intended to capture high-level and detailed representations of NAS system and safety-related data. The model defines, organizes, and structures the relationships among data entities to provide stakeholders and database developers with a common understanding of IDA's information architecture.

The IDA data model has been implemented as a relational database in MySQL and populated with 57 SRMDs for the eight NAS systems selected for initial research. To date, the SRMDs captured encompass a range of system lifecycle phases from initial investment analysis through in-service management and decommissioning or removal. The database will continue to be populated with additional SRMDs obtained through FAA online resources accessible to the Air Traffic Safety Oversight Service.

The IDA's relational database structure, along with custom-developed query and business logic, enables the tool to identify dependencies among NAS systems and potential safety concerns as a result of NAS changes that may affect safety hazards, causes, and risk controls. Development of decision-support logic requires analytical methodologies to build on and extend the IDA data model. These methodologies are provided in the IDA Preliminary Methodology Analysis Report [8], which addresses use of the IDA data model to produce IDA outputs and techniques to determine system and safety indicator scores for SRMD evaluation and NCI analysis.

8. REFERENCES

1. FAA Report. (2017). Integrated Domain Assessment of Future Systems Concept of Operations (DOT/FAA/TC-16/53). Report Not Yet Published.

2. FAA Internal Report. (2013). IDA-FS Preliminary Model Dataset Development.

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

4. Software Engineering Institute. (2009). *Data model as an architectural view* (CMU/SEI-2009-TN-024). Retrieved from http://www.sei.cmu.edu/reports/09tn024.pdf.

5. FAA Air Traffic Organization. (2008). *Safety management system manual. Version 2.1*.

6. Ponniah, P. (2007). *Data modeling fundamentals: A practical guide for IT professionals*. Hoboken, NJ: Wiley-Interscience.

7. Data modeling—conceptual, logical, and physical data models. Retrieved from http://www.1keydata.com/datawarehousing/data-modeling-levels.html

8. FAA Report. (2017). Integrated Domain Assessment Preliminary Methodology. (DOT/FAA/(TC-17/1). Report Not Yet Published.

9. Hull, R. & King, R. (1987). Semantic database modeling: survey, applications, and research issues. *ACM Computing Surveys*, *19*(3), 201–260.

.

APPENDIX A—IDA MAPPING TO AOV REQUEST EVALUATION WORKSHEET

Two key objectives of the Integrated Domain Assessment (IDA), as defined in the concept of operations, are to:

- Support the evaluation of Safety Risk Management Documents' (SRMDs') content and compliance with approved SMS processes.
- Support the Air Traffic Safety Oversight Service's (AOV's) assessment of controls proposed to mitigate high-risk hazards.

The primary process by which the AOV performs these activities today is by reviewing SRMDs for acceptance, approval, and concurrence (AAC). The AAC process is guided by the AOV's AAC work instructions, which include a Request Evaluation Worksheet (REW). The REW, along with its associated job aid [A-1], provides guidance to AOV reviewers pertaining to the criteria used for evaluating SRMDs.

Because the IDA is intended in part to support AOV analysts in reviewing SRMDs, the IDA's functional outputs were mapped to specific REW questions. This mapping was done to ensure that the IDA functions provide data of use to AOV analysts. Table A-1 shows the mapping of the IDA functional outputs to REW criteria.

Table A-1. REW criteria to IDA functional outputs

REW Criteria	IDA Outputs
1. How do you rate the adequacy of system description?	High-level description of selected system/subsystem
	List or diagram of subsystems of selected system
	List or diagram of systems interfacing with selected system
	List of facilities where system is installed
2. How do you rate the description and documentation of the proposed change?	List or diagram of systems interfacing with the selected system
	List of systems/subsystems potentially impacted by the change
	List of facilities potentially impacted by the change
3. The request evaluation team or request lead must review the identified panel of experts to ensure that all impacted stakeholders are included. How do you rate the composition of the Safety Risk Management Panel?	List of systems potentially impacted by the change

Table A-1. REW criteria to IDA functional output (continued)

REW Criteria	IDA Outputs
	List of facilities potentially impacted by the change
4. The RET must ensure that all supplemental documents have been included and signed by the appropriate level of authority (i.e., letter of agreement, notice to airmen, etc.)	N/A
5. For all requests that require coordination with AOV, the request lead must ensure that coordination has been achieved prior to rendering the AOV's final disposition (e.g., aviation flight standards, aircraft certification, accident investigation and prevention).	N/A
6. How do you rate the identified hazards? RET must verify and validate identified hazard(s) within the context of the proposed change. RET or RL should consider reviewing the following as applicable: similar waivers, related compliance issues, daily monitoring of safety data, and other information deemed appropriate by the RET or RL.	Identify similar SRMDs based on system, system type, and/or NAS change type
	Display/compare hazard lists from SRMDs
	Highlight interfacing systems not identified in hazard cause list
	Identify potential system interoperability issues to compare to hazard list
	Highlight impacted systems not identified in hazard cause list
	Capture remarks from reviewer
	Query/view comments from other AOV reviewers
7. How do you rate the evidence provided to support the determination of the worst credible outcome of an event (severity). *Pay particular attention to single point of failure hazard(s).*	Display hazard causes
	Display/compare hazard risk ratings from historical SRMDs
	Query number of incidents/trouble reports related to a system
	Highlight hazards with a single cause identified
	Capture remarks from reviewer
	Query/view comments from other AOV reviewers

Table A-1. REW criteria to IDA functional outputs (continued)

REW Criteria	IDA Outputs
8. How do you rate the quantitative/ qualitative evidence provided to support the determination of likelihood of an event? Pay particular attention to relevant existing control(s) and mitigation(s).	Identify dependent NAS systems that may impact availability/hazard likelihood
	Highlight hazards with a single cause identified
	Query number of incidents/trouble reports related to a system
9. How do you rate the predicted initial and residual safety risk in terms of the adverse impact of the potential hazard(s)? Pay particular attention to single point of failure hazard(s).	Display/compare hazard risk ratings from historical SRMDs
	Highlight hazards with a single cause identified
	Query number of incidents/trouble reports related to a system
10. Based on the RET's findings, how do you rate the adequacy of the proposed mitigation(s) to eliminate or control the adverse impact of the hazard(s)? RET or RL must review the following as applicable: related compliance issues, daily monitoring of safety data, and any other information deemed appropriate by the RET or RL.	Identify similar SRMDs based on system, system type, and NAS change type
	Display/compare controls from SRMDs
	Query number of incidents/trouble reports related to a system
	Evaluate control-effectiveness score
	Capture remarks from reviewer
	Query/view comments from other AOV reviewers
11. Note: If this request pertains to change to an existing SRMD, the RET must ensure that the ATO has provided objective evidence to validate the previously approved mitigation(s) were implemented and provided objective evidence to support the effectiveness of the mitigation.	N/A
12. How do you rate the adequacy of the continuous monitoring plan and the hazard-tracking method?	Identify similar SRMDs based on system, system type, and NAS change type
	Display/compare monitoring tasks from historical SRMDs

REFERENCES

A-1. AAC Evaluation Phase Job Aid (REW – Request Evaluation Worksheet for SRMD) (2014).

APPENDIX B—IDA DATA DICTIONARY

A number of parameters have been defined to describe the data captured in the Integrated Domain Assessment (IDA) data model. Table B-1 is a complete list of the IDA attributes defined in the prototype IDA database and definitions of the data described by each parameter or its use in the model.

Table B-1. IDA data dictionary

IDA Parameter Name	Definition
Acronym	The commonly used acronym for the system (or subsystem).
Anomaly	The anomaly rate calculated by IDA on the report date.
AttachedTo(Remarks)	The category object to which the remark is attached.
AttachedToDetail(Remarks)	The specific object to which the remark is attached.
Autonomy	Flag indicating whether the controls satisfy the autonomy check (0 = No, 1 = Yes).
Breadth	Flag indicating whether the controls satisfy the breadth check (0 = No, 1 = Yes).
Cause_ID	Unique IDA identification number for the cause.
CauseClass_ID	Unique IDA identification number for the top-level cause classification category.
CauseClassName	Name for the top-level cause classification category.
CauseDescription	The description of the cause in the PHA/hazard analysis worksheet.
CauseInfluence	The cause influence score calculated by the IDA on the report date.
CauseSubClass_ID	Unique IDA identification number for the second-level cause classification.
CauseSubClassName	Name for the second-level cause classification category.
CEScoreNum	Numeric value for the control-effectiveness score.
CEScoreVal	Ordinal value for the control-effectiveness score.
ChangeDesc	A brief description of the NAS change.

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
ChangeMetricReport_ID	Unique IDA identification number for the NAS change metric report.
ChangeMetricReportDate	The date associated with the metric report.
ChangeStatus	The current status of the NAS change.
CIPRef	Identifies where the FAA Capital Investment Plan references the NAS change (if applicable).
CIScore	Control importance score for the hazard.
Comment	Supplemental details about the hazard from PHA/HAW or SME who entered the hazard.
Complete	Flag to indicate that all information on this SRMD has been entered into the IDA database.
Complexity	The change complexity parameter score for the NAS change as of the report date.
Control_ID	Unique IDA identification number for the control.
ControlClass_ID	Unique IDA identification number for the top-level control classification category.
ControlClassName	Name for the top-level control classification category.
ControlInfluence	The control-influence score calculated by the IDA on the report date.
ControlSubClass_ID	Unique identification number for the second-level control classification category.
ControlSubClassName	Name for the second-level control classification category.
DataDescription	A description of the data exchanged via the interface.
DataFormat	The format or protocol used to exchange data on the interface.
Date	The effective date on the cover page of the SRMD. If it is a revised version, use the latest date indicated or date of the last signature.
Definition (cause subclassification)	Definition of the second-level cause classification as specified in the IDA taxonomy.

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
Definition (CauseClassification)	Definition of the top-level cause classification as specified in the IDA taxonomy.
Definition (control classification)	Definition of the top-level control classification as specified in the IDA taxonomy.
Definition (Control subclassification)	Definition of the second-level control classification as specified in the IDA taxonomy.
Definition (Hazard classification)	Definition of the top-level hazard classification as specified in the IDA taxonomy.
Definition (Hazard subclassification)	Definition of the second-level hazard classification as specified in the IDA taxonomy.
Definition (NAS Change type)	Definition of the NAS change classification category as specified in the IDA taxonomy.
Dependency	The system-dependency score calculated by the IDA on the report date.
Depth	Flag indicating whether the controls satisfy the depth check (0 = No, 1 = Yes).
Description (NAS Element)	Definition of the NAS element classification category as specified by the NAS enterprise architecture documentation.
Description (Remarks)	User-defined description given to the remark.
DestinationSys_ID	The system ID number for the system that receives data via the interface.
Detectability	Flag indicating whether the controls satisfy the detectability check (0 = No, 1 = Yes).
DocumentNum	The document tracking number for the SRMD, if any.
DueDateFrequency	Schedule of monitoring requirements as specified in the SRMD.
DueDateFrequency (Remarks)	Paired with the notification flag. Specified the date on which to send the notification.
Email(ida_users)	Email of the user.
Enabled(ida_users)	Flag used to specify that the user account is enabled.

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
encryptedPassword(ida_users)	The password given to the user account in an encrypted state.
EndDate	The planned or actual end (or completion) date for the NAS change.
EnteredBy(Remarks)	The username of the person adding the remark.
EquipIdent	An identifier for the equipment type or class (Note: the identifier is assigned by TechOps and may or may not match the system name in the IDA).
EquipStatus	Code to indicate whether the equipment is operational at the installed site.
ExistingRecommendedControl	A flag indicating whether the control is validated and verified as existing (Existing = 1, Recommended = 2).
FacilityCode	Three-letter facility identification code as defined in FAA Order JO 7350.9. (Note: A fourth letter may be appended to identify multiple installations at the same location and can be ignored.)
FacilityLoc	The city where the equipment is located .
FacilityState	The state where the equipment is located.
Filename	The filename for the source SRMD.
FirstName(ida_users)	First name of the user.
FlagName	The name of the SRMD flag that can be automatically identified by the IDA.
FlagType_ID	Unique identification number for the type of SRMD flag that can be identified.
FSEP_Code	The FSEPhigh- Fac_Code used to identify the specific system variant installed at a location. It consists of a system ID field (1 character), facility field (4 characters), and class field (1 character).

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
FSEP_Code	The FSEP Fac_Code that represents the system variant.
FSEPClass	The class field of the FSEP code is a 1-character alphanumeric code further identifying equipment as defined in the FED.
FSEPFacility	The facility field of the FSEP code is a 4-character identifier consisting of a 1-digit capability code, 2-digit type code, and 1-digit model code.
FSEPSysID	The system ID field of the FSEP code is a 1-character identifier that indicates how the system is used in the NAS.
Hazard_ID	Unique IDA identification number for the hazard.
HazardClass	Name for the top-level hazard classification category.
HazardClass_ID	Unique IDA identification number for the top-level hazard classification category.
HazardEffect	The potential effect(s) listed for the hazard in the PHA/HAW.
HazardInfluence	The hazard-influence score calculated by the IDA on the report date.
HazardSubClass_ID	Unique IDA identification number for the second-level hazard classification category.
HazardSubClassName	Name for the second-level hazard classification category.
Id(ida_users)	Unique IDA identification number for the user record.
Idremarks	Unique IDA identification number for the remark.
InitialLikelihood	The initial (or current) likelihood rating for the hazard.
InitialRisk	The initial (or current) risk rating for the hazard from the PHA/HAW.
InitialSeverity	The initial (or current) severity rating for the hazard.
Interface_ID	Unique IDA identification number for the interface.
InterfaceDescription	High-level description of the interface between the source system and its destination system.

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
InterfaceType	The type of interface being modeled, such as data, mechanical, network, power, or voice (Note: only data interfaces are modeled in the IDA at this time)
InternalExternalControl	A flag indicating whether the control is internal or external to the system analyzed by the SRMD (Internal = 1, External = 2)
LastName(ida_users)	Last name of the user
LastUpdated (Hazard)	The timestamp of the last edit to the hazard <not currently used>
LastUpdated (SRMD)	Timestamp of the last edit to the SRMD <not currently used>
LikelihoodRationale	Brief description of the reason for the initial likelihood rating from the PHA/HAW
LinkedElement	<not currently used>
LinkedSystem_ID	Unique IDA identification number of the NAS system linked to the cause or control
Maturity	The change complexity parameter score for the NAS change as of the report date
MetricReport_ID	Unique IDA identification number for the system metric report
MetricReportDate	The date associated with the system metric report
Monitoring_ID	Unique IDA identification number for the monitoring task or activity
MonitoringActivityTask	Brief description of the specific task or activity to monitor the parameter as specified in the SRMD
MonitoringComment	Additional details or comments on the plan entered by the SME entering the SRMD
MonitoringSummary	Brief description of the overall monitoring plan as identified in SRMD
Name	The full name of the system (or subsystem)
NAS_Change_Type	Name for the NAS change type classification category
NASChange_ID	Unique IDA identification number for the NAS change

Table B-1.IDA data dictionary (continued)

IDA Parameter Name	Definition
NASChangeSubType	Additional field to classify NAS changes with greater granularity <not currently used>
NASChangeType_ID	Unique IDA identification number for NAS change type classification category
NASEAPortalID	The ID number assigned to the system in the NAS EA reports
NASEARef	Identifies where the NAS EA Roadmap references the NAS change (if applicable)
NASElementID	Unique IDA identification number for the NAS element (or sub-element) used to classify systems
NASElementName	Name for the NAS element classification category
NCI	The NAS Change Impact score for the NAS change as of the report date
Notification(Remarks)	True/false flag assigned to the remark if the user wants a notification sent regarding the remark
NotificationProcessed(Remarks)	True/false flag to specify that the notification was processed by the system
Organization(ida_users)	Organization associated with the user account
ParentNASElementID	The NASElementID for the top-level NAS element that contains the sub-element
ParentSystem_ID	The IDA identification number for the system that contains the subsystem
Phone(ida_users)	Phone number associated with the user account
PortalID	The number used to identify the NAS element in the NAS EA portal
PrimaryUsers	The classes of users who primarily interact with the system
Record_date(ida_users)	Date that the user account was created or updated
Record_ID	Unique identification number for the records downloaded from TechNet
ReferenceDocs	Documents that provide details or supplemental information about the system

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
ReferenceDocument	Documents that provide details or supplemental information about the interface
ResidualLikelihood	The predicted residual likelihood rating for the hazard after implementing all recommended controls
ResidualRisk	The predicted residual risk rating for the hazard after implementing all recommended controls
ResidualSeverity	The predicted residual severity rating for the hazard after implementing all recommended controls
ResponsibilityCode	A 1-character code assigned by TechOps that identifies the owner of the equipment and who is responsible for maintenance, certification, and inspection
ResponsibleOrg	The organization or office identified in the SRMD as responsible for performing the specified monitoring and reporting
RestorationCode	Code indicating the number of hours allotted for TechOps to restore service
Role(ida_users)	Role associated with the user account
SafetyRequirements	The description of the control (or recommended safety requirement) in the PHA/HAW
saltPassword(ida_users)	A unique system-generated number used in the encryption process for the user password
SDP_Ident	The 3-letter acronym for the SDP that is primarily responsible for/ the recipient of data from the equipment
SDPType	The type of SDP represented by the facility
SeverityRationale	Brief description of the reason for the initial severity rating from the PHA/HAW
ShortTitle	An abbreviated SRMD title that can be used in the IDA UI displays
SMSVersion	The version of the ATO Safety Management System manual under which the SRMD was prepared
SourceSys_ID	The system ID number for the system that sends data via the interface
SRMD_ID	Unique IDA identification number for the SRMD

Table B-1. IDA data dictionary (continued)

IDA Parameter Name	Definition
SRMDHazardNum	The number assigned to the hazard in the SRMD
SRMDStatus	Flag to indicate the current status of the SRMD (Draft = 2, Active = 1, Inactive = 0)
SRMDTitle	The complete title of the SRMD
SRMDVersion	The version number associated with the SRMD, if any
Stability	The system stability score calculated by the IDA on the report date
StartDate	The planned or actual start (or implementation) date for the NAS change
StatusComment	Comment on the SRMD status entered by the SME who entered or edited the SRMD
Suitability	Flag indicating whether the controls satisfy the suitability check (0 = No, 1 = Yes)
Summary	A high-level description and overview of the NAS change analyzed by the SRMD, which may be drawn from the executive summary
System_ID	Unique IDA identification number for the NAS system/subsystem
SystemDescription	A brief overview of the system (or subsystem), purpose, major functions, inputs/outputs, users, and other general information
SystemState	A description of the worst-case system state as identified in the SRMD
SystemStatus	Indicates whether the system is “Active” (currently in use in the NAS) or “Inactive” (not currently used anywhere in the NAS)
Tag(Remarks)	User-assigned tag given to the remark
Title(Remarks)	User-defined name given to the remark
TitleDescription	The title and description of the hazard as identified in the SRMD
Unavailability	The system unavailability rate for the previous month calculated by the IDA on the report date
username(ida_users)	Name assigned to the user account
workLocation(ida_users)	Work location associated with the user account

EA = Enterprise Architecture; NAS = National Airspace System; PHA = prelimilnary hazard analysis; FSEP = Facility, Service, and Equipment Profile; SDP = service delivery point; SME = subject matter expert; SMS = Safety Management System ;

APPENDIX C—IDA DATA MODEL PHYSICAL VIEW

This appendix provides detailed information regarding the attributes of the physical view of the Integrated Domain Assessment (IDA) data model, including the schema and database tables. A total of 29 database tables are defined in the current IDA database schema. Detailed Entity Relationship Diagrams (ERDs) are presented, as are additional details about each database table and the relationships defined between data items. A data dictionary that defines the data and table attributes is found in appendix B.

Figure C-1 provides a detailed entity-relationship diagram (ERD) with the relationships identified for all tables in the initial IDA database. This ERD is based on the conceptual and logical data-model views presented in sections 4 and 5. National Airspace System (NAS) systems and their direct interfaces are captured in the systems, systems properties, and system interfaces tables. Safety Risk Management Documents (SRMDs) are mapped to NAS changes, and SRMDs contain hazards and monitoring parameters. Each hazard contains causes and controls, which are captured in the corresponding tables. Finally, hazard causes and hazard controls are mapped to NAS systems. Many other tables are used to capture supplemental information, such as classifications used to identify similar records.

Note that the final IDA database includes some additional tables to support the IDA application. These include tables of users, remarks, and notification data. These tables and attributes are described in figure C-1, but are omitted from the ERD view for clarity.

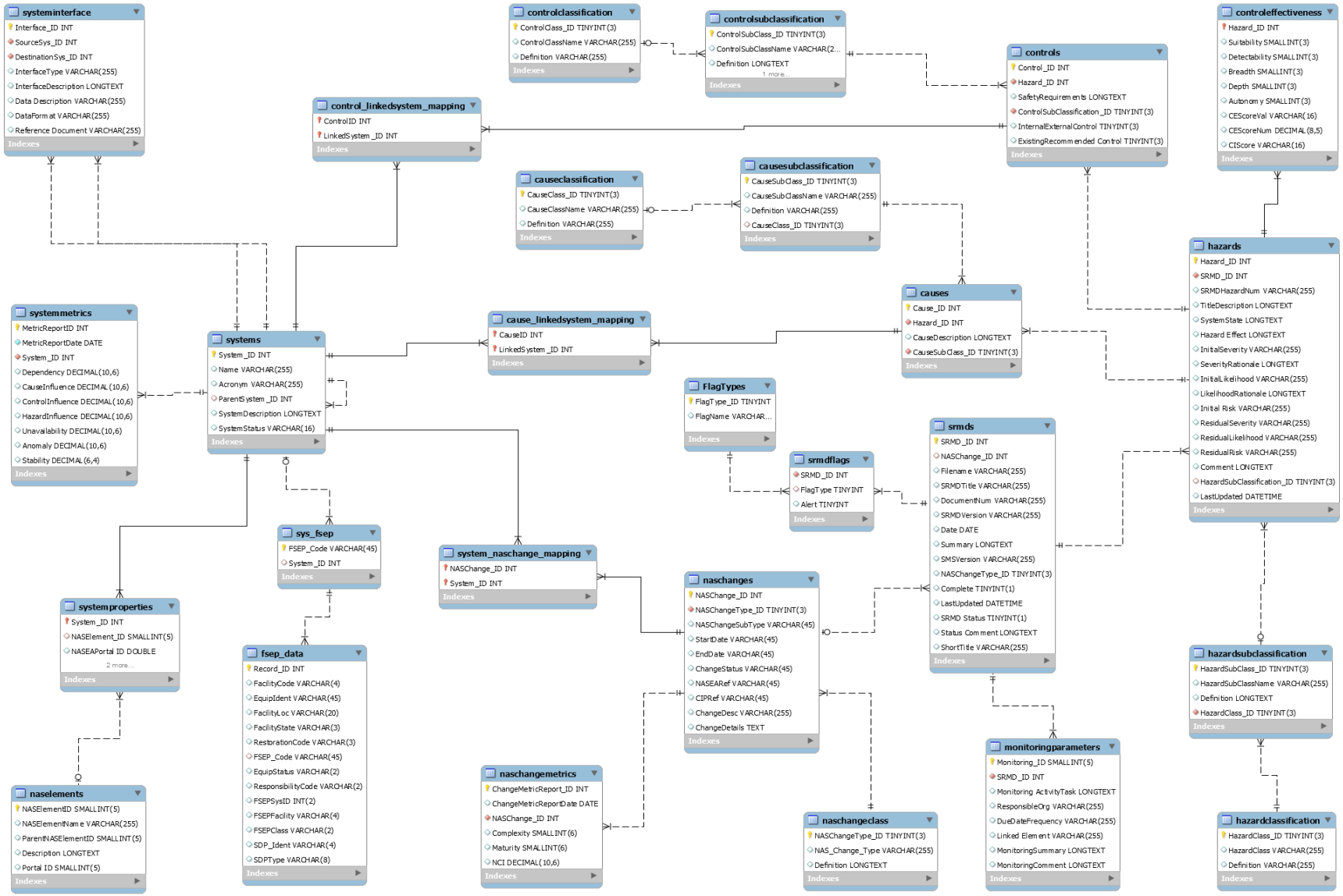

Figure C-1. IDA physical view (database entity relationship diagram)

The following tables provide details about the database tables, relationships between database entities, and data fields defined in the database. Database table names and definitions are listed in table C-1.

Table C-1. IDA database tables

No.	Table Name	Definition
1	Cause_LinkedSystem_Mapping	Links each cause to one or more NAS systems and allows each NAS system to map to one or more causes
2	CauseClassification	Defines the top-level IDA taxonomy classification for causes
3	Causes	Provides details about causes identified in SRMDs
4	CauseSubClassification	Defines the second-level IDA taxonomy classification for causes
5	Control_LinkedSystem_Mapping	Links each control to one or more NAS systems and allows each NAS system to map to one or more controls
6	ControlClassification	Defines the top level IDA taxonomy categories for classifying controls
7	ControlEffectiveness	Stores the control effectiveness and control importance scores and component parameters for each hazard
8	Controls	Provides details about controls identified in SRMDs
9	ControlSubClassification	Defines the second-level IDA taxonomy classification for controls
10	FlagTypes	Stores the names of the types of SRMD flags that the IDA can automatically identify
11	FSEP_Data	Stores data, downloaded from TechNet, about system status at each SDP in the NAS
12	HazardClassification	Defines the top-level IDA taxonomy classification for hazards

FSEP = Facility, Service, and Equipment Profile; SDP = service delivery point; NCI = NAS Change Impact

Table C-1. IDA database tables (continued)

No.	Table Name	Definition
13	Hazards	Provides details about hazards identified in SRMDs
14	HazardSubClassification	Defines the second-level IDA taxonomy classification for hazards
15	Ida_users	Stores details about the IDA system users account
16	MonitoringParameters	Provides details about hazard-monitoring tasks identified in SRMDs
17	NASChangeType	Defines the IDA taxonomy classification for NAS changes
18	NASChangeMetrics	Stores reports of the NCI score and component parameters for each NAS change
19	NASChanges	Provide details about NAS changes
20	NASElements	Defines the top-level NAS EA element for classifying NAS systems
21	Remarks	Stores details and associated attributes of user-created remarks
22	SRMDFlags	Stores the type and a count of the IDA flags thrown for each SRMD
23	SRMDs	Provide details about SRMDs modeled in the IDA
24	Sys_FSEP	Maps each NAS system to one or more FSEP codes
25	System_NAS Change_Mapping	Maps each NAS system to one or more NAS changes and allows each NAS change to map to one or more NAS systems
26	SystemInterface	Provides details about interfaces between NAS systems
27	SystemMetrics	Stores reports of system performance and system influence metrics
28	SystemProperties	Stores details about each NAS system modeled
29	Systems	Identifies NAS systems modeled in the IDA

Tables C-2–C-30 describe the columns in each table of the prototype IDA database. Column names in bold serve as primary keys for the table, whereas those in italics indicate that the column is a foreign key linked to an external table. Definitions for each attribute can be found in appendix B–IDA—data dictionary.

Table C-2. Cause_linkedsystem_mapping table details

Column Name	Data Type	Definition
Cause_ID	INT	Unique IDA identification number for the cause
LinkedSystem_ID	INT	Unique IDA identification number of the NAS system linked to the hazard cause

Table C-3. CauseClassification table details

Column Name	Data Type	Definition
CauseClass_ID	INT(3)	Unique IDA identification number for the top level cause classification category
CauseClassName	VARCHAR(255)	Name for the top-level cause classification category
Definition	VARCHAR(255)	Definition of the top-level cause classification, as specified in the IDA taxonomy

Table C-4. Causes table details

Column Name	Data Type	Definition
Cause_ID	INT	Unique IDA identification number for the cause
Hazard_ID	INT(5)	Unique IDA identification number for the hazard that owns the cause
CauseDescription	LONGTEXT	The description of the cause in the PHA/hazard analysis worksheet (HAW)
CauseSubClass_ID	INT(3)	Unique IDA identification number for the second-level cause classification

PHA = preliminary hazard analysis

Table C-5. CauseSubClassification table details

Column Name	Data Type	Definition
CauseSubClass_ID	INT(3)	Unique IDA identification number for the second-level cause classification
CauseSubClassName	Varchar(255)	Name for the second-level cause classification category
Definition	Varchar(255)	Definition of the second-level cause classification, as specified in the IDA taxonomy
CauseClass_ID	INT(3)	Unique IDA identification number for the top-level cause classification category

Table C-6. Control_LinkedSystem_Mapping table details

Column Name	Data Type	Definition
Control_ID	INT	Unique IDA identification number for the control
LinkedSystem_ID	INT	Unique IDA identification number of the NAS system linked to the control

Table C-7. ControlClassification table details

Column Name	Data Type	Definition
ControlClass_ID	INT(3)	Unique IDA identification number for the top-level control classification category
ControlClassName	VARCHAR(255)	Name for the top-level control classification category
Definition	VARCHAR(255)	Definition of the top-level control classification, as specified in the IDA taxonomy

Table C-8. ControlEffectiveness table details

Column Name	Data Type	Definition
Hazard_ID	INT	Unique IDA identification number for the hazard
Suitability	INT(3)	Flag indicating whether the controls satisfy the suitability check (0 = No, 1 = Yes)
Detectability	INT(3)	Flag indicating whether the controls satisfy the detectability check (0 = No, 1 = Yes)
Breadth	INT(3)	Flag indicating whether the controls satisfy the breadth check (0 = No, 1 = Yes)
Depth	INT(3)	Flag indicating whether the controls satisfy the depth check (0 = No, 1 = Yes)
Autonomy	INT(3)	Flag indicating whether the controls satisfy the autonomy check (0 = No, 1 = Yes)
CEScoreVal	VARCHAR(16)	Ordinal value for the control-effectiveness score
CEScoreNum	DECIMAL(8,5)	Numeric value for the control-effectiveness score
CIScore	INT(6)	Control-importance score for the hazard

Table C-9. Controls table details

Column Name	Data Type	Definition
Control_ID	INT	Unique IDA identification number for the control
Hazard_ID	INT	Unique IDA identification number for the hazard that owns the control
SafetyRequirements	LONGTEXT	The description of the control (or recommended safety requirement) in the PHA/HAW

Table C-9. Controls table details (continued)

Column Name	Data Type	Definition
ControlSubClassification_ID	INT(3)	Unique IDA identification number for the second-level control classification
InternalExternalControl	INT	A flag indicating if the control is internal or external to the system analyzed by the SRMD (Internal = 1, External = 2)
ExistingRecommendedControl	INT(3)	A flag indicating whether the control is validated and verified as existing (Existing = 1, Recommended = 2)

Table C-10. ControlSubClassification table details

Column Name	Data Type	Definition
ControlSubClass_ID	INT	Unique identification number for the second-level control classification category
ControlSubClassName	VARCHAR(255)	Name for the second-level control classification category
Definition	LONGTEXT	Definition of the second-level control classification, as specified in the IDA taxonomy
ControlClass_ID	INT(3)	Unique IDA identification number for the top-level control classification category

Table C-11. FlagTypes table details

Column Name	Data Type	Definition
FlagType_ID	TINYINT(3)	Unique identification number for the type of SRMD flag that can be identified
FlagName	VARCHAR(45)	The name of the SRMD flag that can be automatically identified by the IDA

Table C-12. FSEP_Data table details

Column Name	Data Type	Definition
Record_ID	INT	Unique identification number for the records downloaded from TechNet
FacilityCode	VARCHAR(4)	Three-letter facility identification code, as defined in FAA Order JO 7350.9. (Note: A fourth letter may be appended to identify multiple installations at the same location and can be ignored.)
EquipIdent	VARCHAR(45)	An identifier for the equipment type or class. (Note: The identifier is assigned by TechOps and may or may not match the system name in the IDA)
FacilityLoc	VARCHAR(20)	The city where the equipment is located
FacilityState	VARCHAR(3)	The state where the equipment is located
RestorationCode	VARCHAR(3)	Code indicating the number of hours allowed for TechOps to restore service
FSEP_Code	VARCHAR(45)	The FSEP Fac_Code used to identify the specific system variant installed at a location, which consists of a system ID field (1 character), facility field (4 characters), and class field (1 character)
EquipStatus	VARCHAR(2)	Code to indicate whether the equipment is operational at the installed site
ResponsibilityCode	VARCHAR(2)	A 1-character code assigned by TechOps that identifies the owner of the equipment and who is responsible for maintenance, certification, and inspection
FSEPSysID	INT(2)	The system ID field of the FSEP code, which is a 1-character identifier that indicates how the system is used in the NAS

Table C-12. FSEP_Data table details (continued)

Column Name	Data Type	Definition
FSEPFacility	VARCHAR(4)	The facility field of the FSEP code, which is a 4-character identifier consisting of a 1-digit capability code, two-digit type code, and 1-digit model code
FSEPClass	VARCHAR(2)	The class field of the FSEP code, which is a 1-character alphanumeric code further identifying equipment as defined in the FED
SDP_Ident	VARCHAR(4)	The 3-letter acronym for the SDP that is primarily responsible for, and/or the recipient of, data from the equipment
SDPType	VARCHAR(8)	The type of SDP represented by the facility

Table C-13. HazardClassification table details

Column Name	Data Type	Definition
HazardClass_ID	INT(3)	Unique IDA identification number for the top-level hazard classification category
HazardClass	VARCHAR(255)	Name for the top-level hazard classification category
Definition	LONGTEXT	Definition of the top-level hazard classification, as specified in the IDA taxonomy

Table C-14. Hazards table details

Column Name	Data Type	Definition
Hazard_ID	INT	Unique IDA identification number for the hazard
SRMD_ID	INT	Unique IDA identification number for the SRMD that owns the hazard
SRMDHazardNum	VARCHAR(255)	The number assigned to the hazard in the SRMD
TitleDescription	LONGTEXT	The title and description of the hazard, as identified in the SRMD
SystemState	LONGTEXT	A description of the worst-case system state, as identified in the SRMD
HazardEffect	LONGTEXT	The potential effect(s) listed for the hazard in the PHA/HAW
InitialSeverity	VARCHAR(255)	The initial (or current) severity rating for the hazard
SeverityRationale	LONGTEXT	Brief description of the reason for the initial severity rating from the PHA/HAW
InitialLikelihood	VARCHAR(255)	The initial (or current) likelihood rating for the hazard
LikelihoodRationale	LONGTEXT	Brief description of the reason for the initial likelihood rating from the PHA/HAW
InitialRisk	VARCHAR(255)	The initial (or current) risk rating for the hazard from the PHA/HAW
ResidualSeverity	VARCHAR(255)	The predicted residual severity rating for the hazard after implementing all recommended controls

Table C-14. Hazards table details (continued)

Column Name	Data Type	Definition
ResidualLikelihood	VARCHAR(255)	The predicted residual likelihood rating for the hazard after implementing all recommended controls
ResidualRisk	VARCHAR(255)	The predicted residual risk rating for the hazard after implementing all recommended controls
Comment	LONGTEXT	Supplemental details about the hazard from PHA/HAW or subject matter expert (SME) who entered the hazard
HazardSubClassification_ID	INT(3)	Unique IDA identification number for the second-level hazard classification category
LastUpdated	DATETIME	The timestamp of the last edit to the hazard (not currently used)

Table C-15. HazardSubClassification table details

Column Name	Data Type	Definition
HazardSubClass_ID	INT(3)	Unique IDA identification number for the second-level hazard classification category
HazardSubClassName	VARCHAR(255)	Name for the second-level hazard classification category
Definition	LONGTEXT	Definition of the second-level hazard classification, as specified in the IDA taxonomy
HazardClass_ID	INT(3)	Unique IDA identification number for the top-level hazard classification category

Table C-16. IDA_Users table details

Column Name	Data Type	Definition
id	INT	Unique IDA system ID number for the IDA user account
userName	VARCHAR(255)	The user name associated with the user account
encryptedPassword	MediumBLOB	The password used to authenticate the IDA account in a secure encrypted format
saltPassword	MediumBLOB	This is a system-generated number used in the password encryption process
FirstName	VARCHAR(50)	The first name associated with the user account
LastName	VARCHAR(50)	The last name associated with the user account
Email	VARCHAR(255)	The email associated with the user account
role	VARCHAR(255)	The role associated with the user account
organization	VARCHAR(255)	The organization associated with the user account
workLocation	VARCHAR(255)	The work location associated with the user account
phone	VARCHAR(45)	The phone number associated with the user account
enabled	CHAR(1)	A flag to indicate if the account is enabled
record_date	DATE	The date the account was created or updated

Table C-17. MonitoringParameters table details

Column Name	Data Type	Definition
Monitoring_ID	INT	Unique IDA identification number for the monitoring task or activity
SRMD_ID	INT	Unique IDA identification number for the SRMD that identifies the monitoring task
MonitoringActivityTask	LONGTEXT	Brief description of the specific task or activity to monitor the parameter, as specified in the SRMD
ResponsibleOrg	VARCHAR(255)	The organization or office identified in the SRMD as responsible for performing the specified monitoring and reporting
DueDateFrequency	VARCHAR(255)	Schedule of monitoring requirements, as specified in the SRMD
LinkedElement	VARCHAR(255)	Not currently used
MonitoringSummary	LONGTEXT	Brief description of the overall monitoring plan, as identified in the SRMD
MonitoringComment	LONGTEXT	Additional details or comments on the plan entered by the SME in the SRMD

Table C-18. NASChangeType table details

Column Name	Data Type	Definition
NASChangeType_ID	INT(3)	Unique IDA identification number for NAS change classification category
NAS_Change_Type	VARCHAR	Name for the NAS change type classification category
Definition	LONGTEXT	Definition for the NAS change classification category, as specified in the IDA taxonomy

Table C-19. NASChangeMetrics table details

Column Name	Data Type	Definition
ChangeMetricReport_ID	INT	Unique IDA identification number for the NAS change metric report
ChangeMetricReportDate	DATE	The date associated with the metric report
NASChange_ID	INT	Unique IDA identification number for the NAS change being scored
Complexity	INT(6)	The change complexity parameter score for the NAS change as of the report date
Maturity	INT(6)	The change maturity parameter score for the NAS change as of the report date
NCI	DECIMAL(10,6)	The NCI score for the NAS change as of the report date

Table C-20. NASChanges table details

Column Name	Data Type	Definition
NASChange_ID	INT	Unique IDA identification number for the NAS change
NASChangeType_ID	INT(3)	Unique IDA identification number for NAS change classification category that best describes the NAS change
NASChangeSubType	VARCHAR(45)	Additional field to classify NAS changes with greater granularity (not currently used)
StartDate	VARCHAR(45)	The planned or actual start (or implementation) date for the NAS change
EndDate	VARCHAR(45)	The planned or actual end (or completion) date for the NAS change
ChangeStatus	VARCHAR(45)	The current status of the NAS change
NASEARef	VARCHAR(45)	Identifies where the NAS Enterprise Architecture (EA) Roadmap references the NAS change (if applicable)

Column Name	Data Type	Definition
CIPRef	VARCHAR(45)	Identifies where the FAA Capital Investment Plan references the NAS change (if applicable)

Table C-20. NASChanges table details (continued)

Column Name	Data Type	Definition
ChangeDesc	VARCHAR(255)	A brief title for the NAS change
ChangeDetails	TEXT	A longer description of the NAS change, proving additional details

Table C-21. NASElements table details

Column Name	Data Type	Definition
NASElementID	INT(5)	Unique IDA identification number for the NAS element (or sub-element) used to classify systems
NASElementName	VARCHAR(255)	Name for the NAS element classification category
ParentNASElementID	INT(5)	The NASElementID for the top-level NAS element that contains the sub-element
Description	LONGTEXT	Definition of the NAS element classification category, as specified by the NAS EA documentation
PortalID	INT(5)	The number used to identify the NAS element in the NAS EA portal

Table C-22. Remarks table details

Column Name	Data Type	Definition
idremarks	INT	Unique IDA system ID number for the IDA remarks
Title	MediumText	The title given to the remark
Description	LongText	The description given to the remark
AttachedTo	VARCHAR(255)	The category entity to which the remark is attached

Table C-22. Remarks table details (continued)

Column Name	Data Type	Definition
AttachedToDetail	LongText	The detail entity to which the remark is attached
Notification	VARCHAR(45)	A true/false flag used to specify that the user will be notified of the remark on a specific date
DueDateFrequency	Date	The date on which the notification will be sent
EnteredBy	VARCHAR(255)	The user name of the person entering the remark
NotificationProcessed	VARCHAR(45)	A true/false flag to be set when the notification has been sent to the user

Table C-23. SRMDFlags table details

Column Name	Data Type	Definition
SRMD_ID	INT	Unique IDA identification number for the SRMD
FlagName	VARCHAR(64)	The name of the flag that was thrown
Alert	INT(1)	Indicates whether the flag thrown was of type Alert (1) or Info (0)

Table C-24. SRMDs table details

Column Name	Data Type	Definition
SRMD_ID	INT	Unique IDA identification number for the SRMD.
NASChange_ID	INT	Unique IDA identification number for the NAS change associated with the SRMD.
Filename	VARCHAR(255)	The filename for the source SRMD.
SRMDTitle	VARCHAR(255)	The complete title of the SRMD.

Table C-24. SRMDs table details (continued)

Column Name	Data Type	Definition
DocumentNum	VARCHAR(255)	The document tracking number for the SRMD, if any.
SRMDVersion	VARCHAR(255)	The version number associated with the SRMD, if any.
Date	DATE	The effective date on the cover page of the SRMD. If it is a revised version, use the latest date indicated or date of the last signature.
Summary	LONGTEXT	A high-level description and overview of the NAS change analyzed by the SRMD. May be drawn from the executive summary.
SMSVersion	VARCHAR(255)	The version of the ATO SMS manual under which the SRMD was prepared .
NASChangeType_ID	INT(3)	Unique IDA identification number for NAS change classification category that best describes the SRMD.
Complete	INT(1)	Flag to indicate that all information on this SRMD has been entered into the IDA database.
LastUpdated	DATETIME	Timestamp of the last edit of the SRMD (not currently used).
SRMDStatus	INT(1)	Flag to indicate the current status of the SRMD (Draft = 2, Active = 1, Inactive = 0).
StatusComment	LONGTEXT	Comment on the SRMD status entered by the SME who entered or edited the SRMD.
ShortTitle	VARCHAR(255)	An abbreviated SRMD title that can be used in the IDA UI displays.

SMS = Safety Management System

Table C-25. Sys_FSEP table details

Column Name	Data Type	Definition
FSEP_Code	VARCHAR(45)	The FSEP Fac_Code used to identify the specific system variant installed at a location. It consists of a system ID field (1 character), facility field (4 characters), and class field (1 character).
System_ID	INT	Unique IDA identification number for the system/subsystem.

Table C-26. System_NASChange_Mapping table details

Column Name	Data Type	Definition
NASChange_ID	INT	Unique IDA identification number for the NAS change
System_ID	INT	Unique IDA identification number for the NAS system

Table C-27. SystemInterface table details

Column Name	Data Type	Definition
Interface_ID	INT	Unique IDA identification number for the interface
SourceSys_ID	INT	The system ID number for the system that sends data via the interface
DestinationSys_ID	INT	The system ID number for the system that receives data via the interface
InterfaceType	VARCHAR(255)	The type of interface being modeled, such as data, mechanical, network, power, and voice (Note: Only data interfaces are modeled in the IDA at this time)

Table C-27. SystemInterface table details (continued)

Column Name	Data Type	Definition
InterfaceDescription	LONGTEXT	High-level description of the interface between the source system and its destination system
DataDescription	VARCHAR(255)	A description of the data exchanged via the interface
DataFormat	VARCHAR(255)	The format or protocol used to exchange data on the interface
ReferenceDocument	VARCHAR(255)	Documents that provide details or supplemental information about the interface

Table C-28. SystemMetrics table details

Column Name	Data Type	Definition
MetricReport_ID	INT	Unique IDA identification number for the system metric report
MetricReportDate	DATE	The date associated with the system metric report
System_ID	INT	The IDA system ID number for the NAS system
Dependency	DECIMAL(10,6)	The system dependency score calculated by the IDA on the report date
CauseInfluence	DECIMAL(10,6)	The cause influence score calculated by the IDA on the report date
ControlInfluence	DECIMAL(10,6)	The control influence score calculated by the IDA on the report date
HazardInfluence	DECIMAL(10,6)	The hazard influence score calculated by the IDA on the report date
Unavailability	DECIMAL(10,6)	The system unavailability rate for the previous month calculated by the IDA on the report date
Anomaly	DECIMAL(10,6)	The anomaly rate calculated by the IDA on the report date
Stability	DECIMAL(10,6)	The system stability score calculated by the IDA on the report date

Table C-29. SystemProperties table details

Column Name	Data Type	Definition
System_ID	INT	The IDA system ID number for the NAS system
NASElement_ID	INT(5)	The IDA identification number for the element (or sub-element) that contains the system
NASEAPortalID	DOUBLE	The ID number assigned to the system in the NAS EA reports
PrimaryUsers	VARCHAR(255)	The classes of users who primarily interact with the system
ReferenceDocs	VARCHAR(255)	Documents that provide details or supplemental information about the system

Table C-30. Systems table details

Column Name	Data Type	Definition
System_ID	INT	Unique IDA System ID number for the NAS system (or subsystem)
Name	VARCHAR(255)	The full name of the system (or subsystem)
Acronym	VARCHAR(255)	The commonly used acronym for the system (or subsystem)
ParentSystem_ID	INT	The IDA identification number for the system that contains the subsystem
SystemDescription	LONGTEXT	A brief overview of the system (or subsystem), purpose, major functions, inputs/outputs, users, and other general information
SystemStatus	VARCHAR(16)	Indicates whether the system is Active (currently in use in the NAS) or Inactive (not currently used anywhere in the NAS)