DOT/FAA/TC-17/1

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

Integrated Domain Assessment Preliminary Methodology

October 2017

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

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

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

Technical Report Documentation Page

1. Report No. DOT/FAA/TC-17/1	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle INTEGRATED DOMAIN ASSESSMENT PRELIMINARY METHODOLOGY		5. Report Date October 2017 6. Performing Organization Code ANG-E272	
7. Author(s) Nathan Girdner and Jennifer Lamont		8. Performing Organization Report No.	
9. Performing Organization Name and Address Systems Enginuity, Inc. 8665 Sudley Rd #349 Manassas, VA 20110		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFACT-11-D-00010	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration National Headquarters 800 Independence Ave SW Orville Wright Bldg (FOB10A) Washington, DC 20591		13. Type of Report and Period Covered Technical Report 14. Sponsoring Agency Code AOV-100	

15. Supplementary Notes

The FAA William J. Hughes Technical Center Aviation Research Division COR was 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 (ATO's) provision of air traffic services. To support its mission, AOV initiated a research effort to develop a decision support tool, the Integrated Domain Assessment (IDA). The IDA prototype provides decision support to AOV for Safety Risk Management Document (SRMD) evaluation, NAS Change Impact (NCI) 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 (CE) against risk levels assessed in SRMDs to help AOV understand the relative importance of controls when evaluating control approval or acceptance decisions. To support NCI 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 CE and overall risk likelihood. This report builds on the IDA data model to describe the concepts and technical approach for providing system and safety indicator scores, namely System Impact, System Safety Influence, System Instability, NCI, CE, System Unavailability, and System Anomaly Rate. Indicator scores and algorithms are described in detail along with several examples using NAS and SRMD data in the IDA model.

17. Key Words NAS, NAS systems, NAS architecture, SRMD, Change Impact, Control effectiveness		18. Distribution Statement This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 52	22. Price

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AAC	Approval, Acceptance, and Concurrence
AHP	Analytical Hierarchy Process
AOV	Air Traffic Safety Oversight Service
ASR	Airport Surveillance Radar
ASRS	Aviation Safety Reporting System
ATC	Air traffic control
ATO	Air Traffic Organization
CE	Control effectiveness
CI	Control importance
CONOPS	Concept of Operations
ERAM	En Route Automation Modernization
FDIO	Flight Data Input/Output
FSEP	Facility, Service, and Equipment Profile
IDA	Integrated Domain Assessment
LCM	Log of Corrective Maintenance
LIR	Log Interrupt Report
NAS	National Airspace System
NCI	NAS Change Impact
NCP	NAS Change Proposal
NextGen	Next Generation Air Transportation System
RAV	Resource Allocation Valuation
REW	Request Evaluation Worksheet
RMLS	Remote Maintenance Logging System
SDP	Service Delivery Point
SI	System Impact
SMART	Safety Management Action Review Team
SME	Subject matter expert
SMS	Safety Management System
SOI	System of Interest
SOP	Safety Order of Precedence
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
UTM	Unsuccessful Transmission Message

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 are 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 with potential safety implications, a Safety Risk Management Document (SRMD) must be developed. In accordance with the ATO Safety Management System (SMS) Manual, NAS changes must be examined for system safety risks. 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 Air Traffic Safety Oversight Service (AOV) is responsible for independent safety oversight of air traffic services provided by ATO. As part of AOV's responsibilities, described in FAA Order 1100.161 Change 1, AOV reviews ATO SRMDs and approves or rejects controls that are proposed to mitigate high-risk safety hazards. The AOV's Approval, Acceptance, and Concurrence (AAC) Work Instructions define a step-by-step process for AOV's review of SRMDs along with approval and rejection criteria based on ATO SMS Manual compliance.

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

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

AAC activities in which AOV accepts (versus approves) controls spanning multiple FAA lines of business.

This report documents the development of analysis methodologies that will be used by the IDA tool to realize its functions as defined in the IDA Concept of Operations. Several IDA indicator scores are introduced:

- System Impact—Indicates the relative influence that a system has on current NAS operations and safety.
- System Safety Influence—Indicates the degree to which a system may impact safety risks across the NAS.
- NCI—Indicates the relative effect that a particular change to a NAS system could potentially have on NAS operations and safety.
- Control effectiveness (CE)—The theoretical capability a set of controls has in achieving the risk level associated with a given hazard.
- Control importance—Compares the initial risk of the hazard to its CE score.
- Instability—Indicates the number and kind of changes that a system is expected to undergo and the timeframe in which the changes occur.
- Unavailability—Indicates outage hours for a given system across all Service Delivery Points (SDPs) by month.
- Anomaly Rate—Indicates the number of corrective actions for a given system across all SDPs by month.

Each of these indicator scores supports one or more of the key IDA system functions, particularly “Evaluate SRMD Content,” “Evaluate Effectiveness of Controls,” and “Analyze System Impacts.” These indicator scores are derived from NAS system and SRMD data captured in the IDA database and provide tools to help AOV users in evaluating NAS systems, changes, SRMDs, and safety dependencies.

This analysis report describes each of the indicator scores and presents the input parameters and preliminary methods used to calculate each score. Additional potential research areas are described in the conclusions to this paper, including possible approaches to refine the scoring methods. The methods and algorithms described in this report provide the basis for IDA Specification. The prototype IDA tool presents these scores to AOV users to support their safety oversight processes, including evaluation of SRMDs and proposed safety risk controls.

1. INTRODUCTION

1.1 BACKGROUND

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

One of the major challenges that AOV faces is that the current ATO Safety Risk Management (SRM) process focuses on individual changes to the National Airspace System (NAS), which means that a 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 are needed to evaluate potential risks of both individual and multiple, overlapping changes in the context of the dynamic and complex NAS environment.

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

The IDA 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 key functions:

- 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 AOV with determining whether proposed controls can be expected to reduce the risk as indicated in the SRMD.
- Analyze System Impacts (SIs)—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 AOV to manage remarks and notifications regarding SRMD issues, system/NCIs, and other safety oversight concerns.

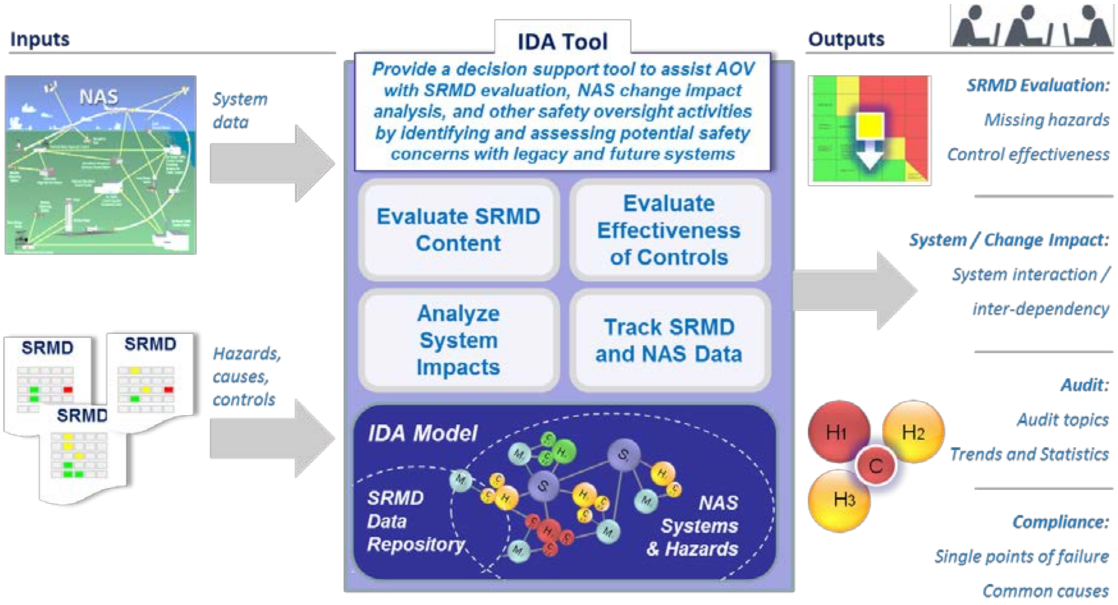


Figure 1. The IDA concept overview

As shown in figure 1, the IDA model constitutes the foundation of the tool, enabling functions to evaluate NAS SIs, 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 integrates 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 model.

1.2 PURPOSE

The purpose of this report is to describe methods IDA will use to implement function capabilities to “Evaluate SRMD Content,” “Evaluate Effectiveness of Controls,” and “Analyze System Impacts,” as identified in the IDA Concept of Operations (CONOPS) [1]. More specifically, this report describes how the IDA data model is used to support SRMD content evaluation and how NCI and control effectiveness (CE) are determined to support AOV safety oversight processes.

The essential functions of the IDA tool are described in the IDA CONOPS report. The IDA CONOPS drives the development of the initial IDA data model and the preliminary IDA methodology. The IDA model report describes the system and safety data that are collected by IDA and the relationships defined to enable analysis of the data. This preliminary IDA methodology report describes the development of analysis techniques that make use of the IDA data model to fulfill the IDA functional capabilities defined in IDA CONOPS. The IDA model report and this IDA methodology report help drive the development of IDA prototype system requirements in the IDA initial specification document.

This report focuses on the development of analysis methodologies that will be used by the IDA tool to achieve IDA functional capabilities for NCI analysis and CE evaluation. This report builds on and supersedes the IDA Initial Technical Approach report [2] submitted in 2013, which discussed potential research topics and approaches to investigate to develop the IDA analysis methodologies. Eight IDA indicator scores are introduced: SI, NCI, System Safety Influence, CE, control importance (CI), Instability, Unavailability, and Anomaly Rate. The prototype IDA tool presents these scores to AOV users to support their safety oversight processes including evaluation of SRMDs and proposed safety risk controls and risk-based prioritization of oversight activities, such as audits.

1.3 DEFINITIONS

The following terms are used throughout the document. Definitions are drawn from various FAA documents and standards, including FAA Order 1100.161 Change 1, Air Traffic Safety Oversight [3] and the ATO SMS Manual Version 2.1 [4]:

- 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. 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 that uniquely identify each entity. The physical view provides implementation details on database tables.
- 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.
- NAS Change—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.

1.4 DOCUMENT STRUCTURE

Section 2 of this analysis report presents an overview of the IDA functions defined in the IDA CONOPS and shows which functions are dependent on the development of an analysis methodology and those that can be drawn from more basic queries of the data model. Section 3 lists basic assumptions about the systems and underlying data used to develop the analysis methodologies. Section 4 addresses the SI concept and score, including the input parameters and data, and the algorithm developed to calculate SI. Section 5 describes the NCI concept and score, which includes the System Safety Influence indicator. An example drawn from a historical NAS change documented in SRMD is used to demonstrate how the NCI score would be derived. Section 6 describes the CE concept and score, including the input parameters and data and the algorithm developed to calculate the CE score. Examples drawn from two historical SRMDs are shown to demonstrate how the CE is scored and can be used by AOV users. Section 7 provides details on system indicators for Instability, Unavailability, and Anomaly Rate. Section 8 provides conclusions drawn from the research and discusses the additional research that could be done to further refine the preliminary IDA methodologies described in this report.

2. FUNCTIONAL ALLOCATIONS

The functional view of the IDA model encompasses tool functions, data outputs, and data inputs. The IDA functions are outlined and mapped to data outputs in section 2.l. A detailed description of each function and traceability to AOV stakeholder needs was previously provided as part of the 2013 IDA Needs Analysis and CONOPS Reports [1].

2.1 FUNCTIONAL HIERARCHY

The IDA CONOPS decomposed the preliminary functional needs for 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 since the CONOPS publication has resulted in refinement and reorganization of the functional hierarchy, but the overall system capabilities defined in the IDA CONOPS are retained. The IDA concept 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 AOV with determining whether proposed controls can be expected to reduce the risk as indicated in the SRMD.
- Analyze SIs—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 AOV to manage remarks and notifications regarding SRMD issues, system/NCIs, and other safety oversight concerns.

These functional objectives form the first four high-level system functions defined for the IDA tool. Two additional IDA functions were defined that support the primary tool objectives. These functions are:

- Manage & Process Remarks & Notifications—Maintain user remarks and configure, process, and generate notifications regarding SRMD issues, system/NCIs, and other safety oversight concerns requiring AOV attention.
- Generate Reports & Data Sets—Assemble and output user-requested reports, reports triggered by notifications, and user-requested data sets.

Figure 2 shows the current IDA functional hierarchy.

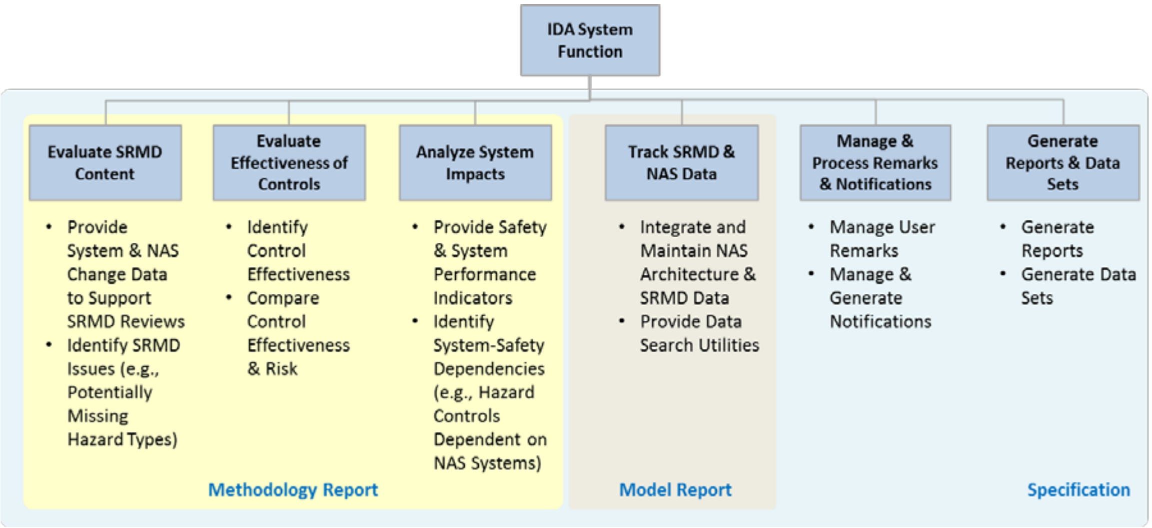

IDA System Function
Evaluate SRMD Content
Provide System & NAS Change Data to Support SRMD Reviews
Identify SRMD Issues (e.g., Potentially Missing Hazard Types)
Evaluate Effectiveness of Controls
Identify Control Effectiveness
Compare Control Effectiveness & Risk
Analyze System Impacts
Provide Safety & System Performance Indicators
Identify System-Safety Dependencies (e.g., Hazard Controls Dependent on NAS Systems)
Methodology Report
Track SRMD & NAS Data
Integrate and Maintain NAS Architecture & SRMD Data
Provide Data Search Utilities
Model Report
Manage & Process Remarks & Notifications
Manage User Remarks
Manage & Generate Notifications
Generate Reports & Data Sets
Generate Reports
Generate Data Sets
Specification

Figure 2. The IDA functional hierarchy

This IDA methodology report provides details on calculating indicator scores related to the high-level system functions “Evaluate SRMD Content,” “Evaluate Control Effectiveness,” and “Analyze System Impacts.” Details about the IDA data model are documented in the IDA Model Analysis Report. All of the IDA functions, including “Manage & Process Remarks & Notifications” and “Generate Reports & Data Sets,” are addressed in the IDA Specification Report.

2.2 FUNCTIONAL OUTPUTS

To establish the methodology, 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 complex or detailed analysis of the IDA model. Table 1 shows a list of the high-level IDA functions, sub-functions, and corresponding outputs allocated to the data model/analytical methods. The primary IDA functions, namely “Evaluate SRMD Content,” “Evaluate Control Effectiveness,” and “Analyze System Change Impacts,” are the focus of the functional allocation in table 1. Supporting functions to assemble and manage NAS and SRMD data and generate reports and user-configured notifications are addressed in other reports because they entail database administration. The outputs allocated to “Analytical Methods” are focused and described in detail in the remainder of this report. Additional details regarding the data model that supports these functions is provided in the previous IDA Model Report.

Table 1. The 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	
	Interfacing systems not identified in hazard cause list	X	
	Hazards with a single cause identified	X	
	Hazards with significant risk reduction	X	
Evaluate Effectiveness of Controls			
Identify CE	View controls from selected SRMDs	X	
	CE score		X
Compare CE and Risk	CI score		X

Table 1. The IDA functions and outputs (continued)

IDA Function	IDA Outputs	Data Model	Analytical Methods
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/hazard likelihood	X	X
	List of SDPs in which system provides services	X	
	Pending NAS changes to interfacing systems	X	

Functional outputs that are allocated to the "Data Model" are outputs that can be generated via direct query of the database that serves as the foundation of the IDA data model. This may include a combination of database filters, sorting selections, and user comparison of search results. Detailed instructions on using the IDA prototype to evaluate SRMDs (including searching for data) and using the Request Evaluation Worksheet (REW) support features in IDA are provided in the IDA User Guide, and the requirements for these queries are documented in the IDA Specification Report.

Functional outputs that are allocated to "Analytical Methods" are generated by coupling queries of the IDA database with other analytical techniques and algorithms. These analytical techniques and methods are detailed in sections 4–7.

3. ASSUMPTIONS

The preliminary methodologies presented in this report make the following assumptions:

- The AOV has access to a reasonable percentage of all SRMDs from ATO, not just SRMDs that are formally submitted for AAC.
- The ATO SRMDs have been entered into the IDA tool, and the data have been classified correctly.
- The ATO SRMD under review is related to equipment, not procedure. SRMDs that deal with procedures are not in-scope for this version of IDA.
- Hazard causes that are linked to systems in IDA specifically refer to faults; failures; errors; testing or installation issues; or other problems under the purview of that system. Hazard causes that are due to human activity/errors, procedures, or training are not linked to specific systems unless the cause will occur only if the system has malfunctioned.
- Hazard controls that are linked to systems in IDA specifically refer to system performance, design, features, and operations that help mitigate a hazard. Controls that assume the presence of a system but do not call it out explicitly (e.g., procedures or training that may assume a particular system or function) are not linked to specific systems unless the text of the control explicitly names the system as a fundamental element of the control.
- A set of controls is defined as one or more controls that mitigate a hazard.

4. THE SI

The SI is a safety indicator defined for the IDA prototype. The SI indicates the relative influence that a system has on current NAS operations and safety. Changes to highly impactful systems could potentially impact overall NAS safety. The SI accounts for direct and indirect relationships with other NAS systems and identified hazards.

There are four parameters that contribute to the SI score:

1. Dependency—Systems that have more external interfaces (particularly bidirectional and sending interfaces) are more complex and may be more impactful to other elements of the NAS.
2. Cause Influence—Systems that are cited as causes to a large number of hazards (especially external hazards) are more impactful to NAS safety than those that cause few or no hazards.
3. Control Influence—Systems that provide controls to a large number of hazards (especially external hazards) are more impactful to NAS safety than those that do not control hazards.
4. Exposure—Systems that are installed in a large number of places or provide services to large numbers of traffic are more impactful to the NAS.

The SI score fluctuates over time. Tracking these variations will give AOV personnel an indication of whether a given system is increasing or decreasing in influence, which may guide AOV decisions on whether it should receive more or less scrutiny and resources. If a system with a large SI score is identified as undergoing a change, AOV personnel may wish to:

- Look at the system architecture to identify particular interfaces.

- Investigate the system’s safety dependencies to identify the hazards caused and controlled by the system.
- Look at the locations where the system is operational to see the potential extent of the change.

4.1 THE SI PARAMETERS

Four parameters have been identified that contribute to SI. These are attributes of system and hazard dependencies that can be objectively defined and determined from data in the IDA model. Figure 3 shows an overview of the parameters that contribute to scoring SI. Sections 4.1.1–4.1.4 define these parameters in greater detail.

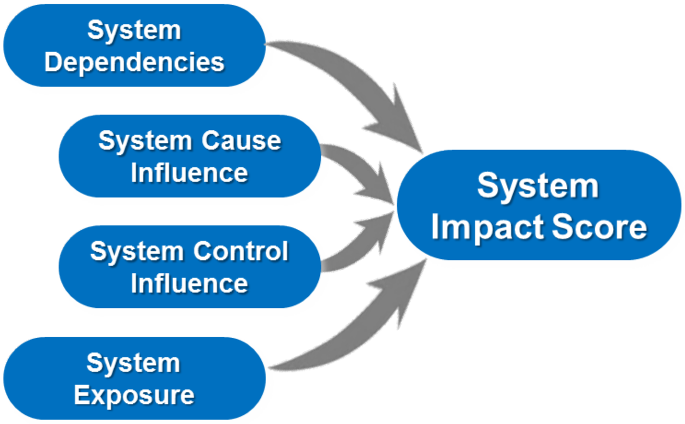


Figure 3. The SI score factors

4.1.1 System Dependency

The System Dependency (*D*) score rates the number and the strength of the connections or interfaces that a given system has with other systems in the NAS. A high System Dependency score is indicative of a system that interacts with multiple systems, receiving inputs from and delivering outputs to external systems and users. Systems with low System Dependency scores are essentially standalone systems that do not depend on external systems for their operation or do not provide safety-related functionality to other NAS systems.

System Dependency values are based on system architecture data in the IDA model. Flowe et al. have developed a method of calculating an equivalent node score for a system or system-of-systems [5]. This equivalent node score is a weighted combination of send-only, receive-only, and send-receive nodes and a complexity factor represented by the normalized number of links per node. This model captures the following assumptions about networks of NAS systems:

1. Send-receive nodes are more complex than send-only or receive-only nodes.
2. Receiving (or “downstream”) nodes increase complexity more than sending (or “upstream”) nodes.

3. Nodes that have more links are more complex than nodes with fewer links.

Figure 4 shows an example network of five NAS systems. System 1 is the System of Interest (SOI) for this analysis, and it interacts with Systems 2–5. Systems 2 and 3 are send-receive nodes, System 4 is a send-only node, and System 5 is a receive-only node. Note that this notional network only takes into account the systems that directly interact with System 1. System 5 may have other interacting systems and may be modeled as something other than a receive-only node in that context, but only the first-level interactions are examined when evaluating System Dependency for System 1.

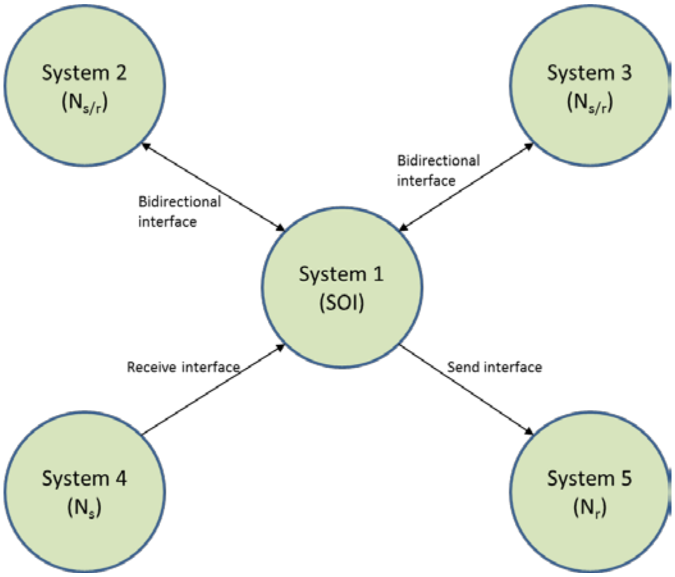


Figure 4. Notional system network diagram

The resultant equation for the equivalent node value for a NAS system and its direct interactions is given as:

$$N_e = (N_{s/r} + 0.5N_r + 0.25N_s) \tag{1}$$

where N_e is the equivalent nodes value, $N_{s/r}$ is the number of send-receive nodes, N_s is the number of send-only nodes, and N_r is the number of receive-only nodes.

The coefficients used to weight the complexity (or importance) of each node type were selected based on assumptions about the network of NAS systems. Send-receive nodes are weighted at 1, as the most complex type of network node. The model assumes that receive-only nodes add more complexity to the system than send-only nodes. This is because changes to an SOI will have less impact on an upstream data source (*Ns*) than on a downstream consumer (*Nr*) of data. Receive-only nodes are initially weighted at 0.5 (half the complexity of a send-receive node), and send-only nodes are weighted at 0.25. These weights are subject to review, and sensitivity analysis will be completed as part of future research and development.

The IDA uses the NAS architecture data in its model to identify the number and type of interfaces and other inter-relationships between NAS systems. The direct data interfaces between each NAS system are captured in the IDA database. For each NAS system in the IDA model, a network of interactions can be built, in which each NAS system that interfaces with the SOI is either a send node, a receive node, or a send-receive node, and each data interface is a link, which may be unidirectional or bidirectional. The SOI is not considered a directional node for this calculation, but it does count toward the total number of nodes ($N_{t,}$).

The System Dependency score, *D*, is calculated by dividing the equivalent node value by the actual number of nodes in the network (N_t):

$$D = \frac{N_e}{N_t} \tag{2}$$

The process for calculating *D* for a system is as follows:

1. Identify the SOI.
2. Query the IDA database to identify all systems that interface with the SOI.
3. Determine the directionality of each interface:

    a. If a system sends to and receives from the SOI → Bidirectional.
    b. If a system receives from the SOI → Receive.
    c. If a system sends to the SOI → Send.

4. Count the number of nodes of each type:

    a. $N_{s/r}$: Sending and receiving data from SOI.
    b. N_r: Receiving data from the SOI.
    c. N_s: Sending data to the SOI.

5. Calculate $N_e = N_{s/r} + .5N_r + .25N_s$
6. Calculate $N_t = N_{s/r} + N_r + N_s + 1$
7. Calculate $D = N_e / N_t$

The *D* is a unitless number that represents the relative degree of interdependency for a given NAS system. The score ranges from 0.125 (for an SOI that receives from a single system) to 0.999 for a complex system with a very large number of bidirectional interfaces. Table 2 summarizes the meaning of relatively higher or lower values of *D*.

Table 2. System Dependency score meanings

D	Dependencies
0.999	Large number of bidirectional system interfaces
0.125	Receive-only SOI system (all external systems send only to the system), or very few interfacing systems

The original equation for N_e developed by Flowe included a nonlinear complexity scaling factor that related the number of links and nodes in the equivalent network to an average link/node ratio. However, the specific values derived for this scaling factor were derived from data on Department of Defense systems and budgets and are not necessarily applicable to the NAS environment. Initial analysis of the eight IDA focus systems indicates that the scaling factor may be negligible because all of the link/node relationships follow a simple convention and do not scale differently by size. As additional systems in the NAS are modeled in IDA, this assumption may be revisited to derive a more accurate scaling factor.

4.1.2 System Cause Influence

The System Cause Influence (I_{cause}) is the degree to which a system causes hazards across the NAS. This score reflects the number of and the risk represented by hazards that cite the system as a cause. A system with a high I_{cause} value is identified as causing a large number of hazards, each with significant risk.

The I_{cause} value is calculated using data maintained in IDA. The IDA data model identifies the number of hazard causes that are related to a system's operation. The I_{cause}, then, is a function of the number and type of hazards that may occur because of the loss of or malfunction in that system's function. The score is weighted so that hazards in external systems (e.g., Airport Surveillance Radar [ASR]-11 identified as a hazard in a Standard Terminal Automation Replacement System SRMD) produce a higher I_{cause} value than those that influence only hazards in that system (e.g., an ASR-11 malfunction producing an ASR-11 hazard).

A system may be identified as an external cause for one or more hazards in the NAS. Each hazard that is potentially caused by that system also has an associated risk (severity and likelihood), in which higher-risk hazards are of greater importance or interest than lower-risk hazards. The number of times that the system is cited as a cause for each hazard is also factored into the score. A system that is cited only once will have a lower cause criticality score, and a system that is listed more than once as a cause of a single hazard (e.g., multiple failure modes) will have a relatively higher score for that hazard.

To calculate system safety influence (I) for a system, the number of unique hazards in the IDA database that cites that system as an external cause must be identified. Next, the relative hazard weight is calculated for each hazard to assess whether the hazard represents a larger or smaller overall NAS risk. The hazard weight for each hazard is multiplied by the ratio of hazard causes attributed to the system to the total number of all causes identified for the hazard. Figure 5 shows the inputs used to calculate I_{cause} for a system.

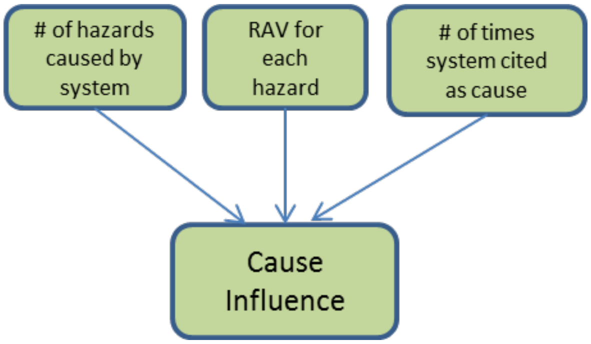
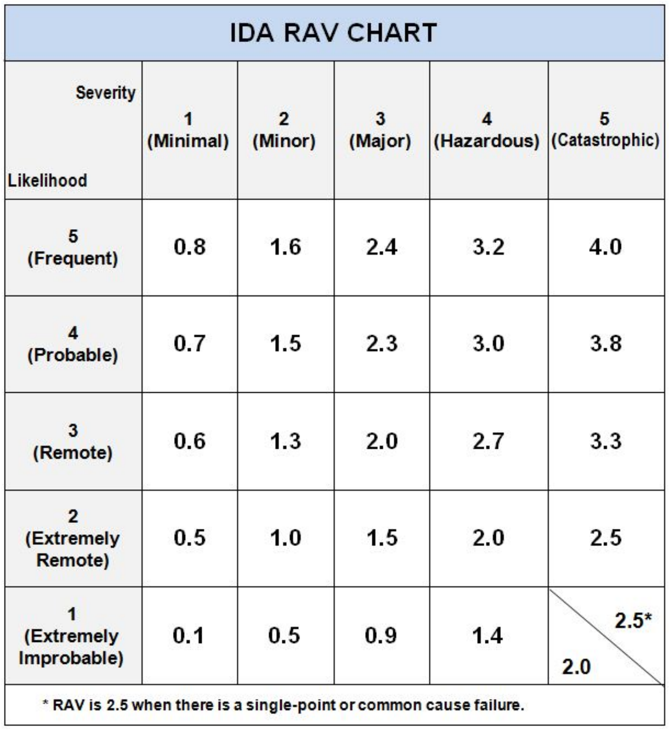

# of hazards caused by system
RAV for each hazard
# of times system cited as cause
Cause Influence

Figure 5. System control influence inputs

The AOV has developed a scoring methodology called Resource Allocation Valuation (RAV) that allows users to prioritize resources in investigating and analyzing hazards [6, 7]. The RAV converts the alphanumeric form of hazard risk to a numeric score representing the risk level. The IDA uses a modified version of the AOV RAV scoring chart to calculate the relative weight of each hazard. The RAV score for each hazard is obtained by mapping the initial risk of each hazard to the appropriate RAV value. as shown in figure 6.



IDA RAV CHART

Severity Likelihood	1 (Minimal)	2 (Minor)	3 (Major)	4 (Hazardous)	5 (Catastrophic)
5 (Frequent)	0.8	1.6	2.4	3.2	4.0
4 (Probable)	0.7	1.5	2.3	3.0	3.8
3 (Remote)	0.6	1.3	2.0	2.7	3.3
2 (Extremely Remote)	0.5	1.0	1.5	2.0	2.5
1 (Extremely Improbable)	0.1	0.5	0.9	1.4	2.5* 2.0

* RAV is 2.5 when there is a single-point or common cause failure.

Figure 6. Modified RAV for system safety influence

The process for calculating I_{cause} for a system is:

1. Identify the SOI.
2. Identify all hazard causes linked to SOI in the IDA model.
3. Identify the hazard that contains the cause for each cause identified in step 2:

   a. Count the total number of unique hazards.

4. Identify the SRMD that identifies the hazard for each hazard identified in step 3.
5. If SRMD Status = "Draft" OR "Inactive," then mark the hazards and causes identified by it as "Inactive" and disregard for subsequent calculations.
6. For each SRMD identified in step 4, identify the system associated with the NAS Change that is linked to the SRMD.
7. For each hazard identified in step 3:

   a. If <SRMD system> = SOI, then mark the hazard as "Internal."
   b. Otherwise, mark the hazard as "External."

8. For each active hazard identified in step 7, report:

   a. The Initial Severity and Likelihood:

      i. Assign the RAV score based on the IDA RAV chart.

   b. The total number of causes for the hazard = $Cause_t$.
   c. The number of causes linked to SOI = $Cause_s$.

9. For each active hazard identified in step 8:

   a. Calculate the hazard fractional contribution $Ca_h = RAV * (Cause_s / Cause_t)$.

10. Calculate Ca_{int} = sum of Ca_h for all internal hazards identified in step 7a.
11. Calculate Ca_{ext} = sum of Ca_h for all external hazards identified in step 7b.
12. For all active hazards in the IDA database:

    a. Assign the RAV score based on the IDA RAV chart.

13. Calculate the total RAV score for all active hazards = R_{total}.
14. $I_{cause} = (1.5*Ca_{ext} + 0.5*Ca_{\text{int}}) / (R_{total})$

The Cause Influence score could range from 0 (SOI is not identified as a cause of any hazards) to 1 (SOI is wholly responsible for causing all known hazards in the IDA database). Most systems are expected to have I_{cause} scores of 10% or less.

4.1.3 System Control Influence

A system may also be identified as a control for one or more hazards in the NAS. Each hazard that is mitigated by that system has an associated risk (severity and likelihood) in which higher-risk hazards are of greater importance or interest than lower-risk hazards. A system that is only listed once as a control will have a lower control influence score, and a system that is listed more than once as a control for a single hazard (e.g., an external system that provides fault detection, error correction, and backup) will have a relatively higher $I_{control}$ score for that hazard. Figure 7 shows the inputs used to calculate $I_{control}$ for a system.

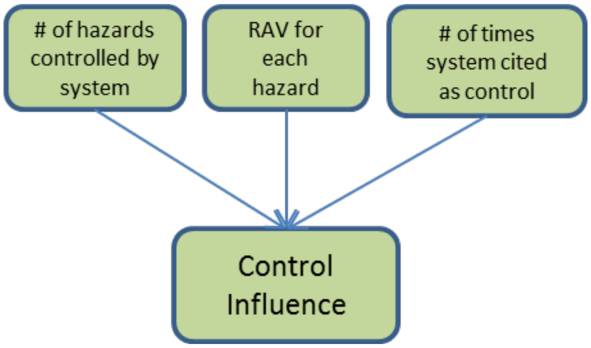

# of hazards controlled by system
RAV for each hazard
# of times system cited as control
Control Influence

Figure 7. System control influence inputs

The process for calculating $I_{control}$ is the same as the process used to calculate I_{cause}, as detailed in section 4.1.2. Instead of identifying all causes linked to the SOI, IDA identifies all controls linked to the SOI. The Control Influence score can range from 0 (SOI is not identified as a control for any hazards) to 1 (SOI is wholly responsible for controlling all known hazards in the IDA database). Most systems are expected to have $I_{control}$ scores of 10% or less.

4.1.4 System Exposure

System Exposure (*E*) is an indication of the degree to which a system is used in facilities across the NAS to support air traffic operations. Systems with high exposure are used in a large number of locations that support many ATC operations. The more places that have a system installed and the more operations that are supported or affected by a system, the greater the impact to the NAS is expected to be if that system is changed.

Because systems are installed at facilities, a change to a particular NAS system will necessarily have an effect on the facilities where that change is implemented. This extent should be identified and analyzed in the applicable SRMD, but IDA can provide a cross-check for this impact by identifying the facilities where the changed system is installed. A change to a NAS system may also have an effect on systems that interact with the changed system, whether they provide input or are downstream consumers of data or functionality that the NAS system provides. The IDA will query its architecture data to identify the systems that directly interface with the changed system or subsystem.

The *E* score is calculated from data available on the FAA’s Technet website (technet.faa.gov) and on the FAA’s OpsNet website (aspm.faa.gov). The key inputs are the number of SDPs that use (or receive data from) the SOI and the number of flight operations that are handled by each SDP. The *E* will be recalculated periodically to account for changes in ATC facility SDPs and traffic levels in the NAS.

The process for calculating *E* for a particular system is as follows:

1. Identify the SOI.
2. Identify the Facility, Service, and Equipment Profile (FSEP) codes linked to the SOI.
3. Identify the SDPs that have the FSEP codes in step 2:

    a. Remove duplicates from the results (this indicates multiple instances of the same system at an SDP).

4. Go to OpsNet (aspm.faa.gov) and run a Total Terminal Detail Report:

    a. Output: detail report, MS Excel (CSV) format.
    b. Dates: by month; (Current month -2), to (Current month -1).
    c. Facilities: the facility (SDP) codes identified in step 3.

5. Identify the count of Total Operations for:

    a. Each SDP.
    b. All SDPs of that type.

6. Run a Total Terminal Detail Report for all NAS Facilities:

    a. Output: detail report, MS Excel (CSV) format.
    b. Dates: by month; (Current month -2), to (Current month -1).
    c. Facilities: all NAS facilities (leave filter blank).

7. Identify the count of:

    a. Total Operations for all SDPs of that type.
    b. Number of SDPs of that type (Tower, TRACON, Domestic Enroute, or Oceanic Enroute).

8. Calculate the percentage of SDPs supported by the system per the FAA’s FSEP:

    a. *S* = (installed SDPs)/(total SDPs of type)

9. Calculate the percentage of total operations (*O*) potentially impacted by the SOI:

    a. *O* = (total operations for SOI SDPs)/(total operations for all facilities)

10. Calculate *E* as a weighted average of SDPs and operations:

    a. *E* = (0.5 * S) + (0.5 * O)

The *E* is a unitless number that represents the relative degree to which a system contributes to the provision of ATC services in the NAS. Table 3 summarizes the meaning of relatively higher or lower values of *E*.

Table 3. System exposure score meanings

E	Meaning
1.0	System provides service to all SDPs of its type (Tower, TRACON, Domestic Enroute, or Oceanic Enroute), and those SDPs handle a significant number of flight operations in the NAS.
0.001	System provides service to very few SDPs, and those SDPs handle low traffic volume.

4.2 THE SI SCORE CALCULATION

The IDA uses a linear-weighted product method to calculate and score the SI of an NAS system. The basic equation used to score SI is:

$$SI = \omega_1 D + \omega_2 I_{cause} + \omega_3 I_{control} + \omega_4 E \tag{3}$$

where ω_1, ω_2, ω_3, and ω_4 are weighting factors that sum to 1.

These factors are initially set to 0.25 (equivalent weight for all parameters), but these weights may be adjusted based on additional study and input from subject matter experts (SMEs).

The weighting factors ω_1, ω_2, ω_3, and ω_4 may be calculated using an Analytical Hierarchy Process (AHP). The AHP uses weighted criteria to score and rank alternatives involved in a decision analysis with multiple objectives [8]. Weights are assigned to decision criteria according to the relative importance of each criterion. One or more SMEs will be interviewed to determine how important each weighting factor is relative to the next (e.g., equally important, twice as important, half as important, etc.) until a pairwise comparison matrix for all criteria is complete. Objective weights are established by dividing each column's entry in the pairwise comparison matrix by the sum of the weights in that column, such that each column sums to 1. If multiple SMEs provide input to assign weights, indices such as inter-rater reliability or intra-class correlation coefficients may be used to determine the degree to which SMEs agree or disagree.

5. THE NCI

Current SMS policy and guidance requires ATO to analyze NAS changes for safety effects. This involves describing the system; identifying the hazards that may occur; determining the causes of those hazards and the existing controls that mitigate them; and recommending additional controls to reduce the hazard risk. These analyses are documented in SRMDs developed by the change proponent. The NAS changes may also impact existing hazards/controls in the NAS. This impact may or may not be identified by an SRMD, as change proponents may not be aware of all the downstream systems that directly or indirectly rely on the system undergoing the NAS change.

The NCI is defined as an indication of the relative effect that a given change to a NAS system could potentially have on NAS operations and safety. The NCI score will allow IDA users to compare NAS changes in terms of the degree of change expected and the number and type of system and safety interactions that may be impacted. The NCI score has some similarities to the SI score, but it adds an SME evaluation of the complexity and maturity of a given NAS change. The NCI values range from 0 (no measurable impact to NAS operations or safety) to 1 (sweeping change to the NAS).

The NCI is scored for each NAS change identified in the IDA. This includes planned NAS changes (identified from the FAA Capital Investment Plan, the NAS Enterprise Architecture Roadmap, and other planning documents) and changes described in a NAS Change Proposal (NCP) or SRMD. The NCI score is a function of the characteristics of the NAS change (which may vary from change to change) and the context of the changed system in the NAS safety environment (which may only change slowly over time). The IDA presents a list of NAS changes and their NCI scores grouped by system. However, NCI is scored by system change, not by system.

5.1 THE NCI PARAMETERS

There are four parameters that contribute to the NCI score for a change: Change Complexity (*C*), Change Maturity (*M*), System Dependency (*D*), and System Safety Influence (*I*). Figure 8 shows an overview of the parameters that contribute to scoring NCI.

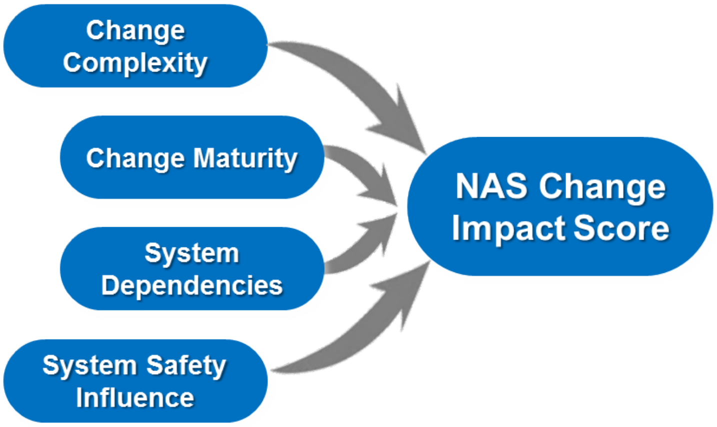


Figure 8. The NCI score factors

The selection and use of these parameters was adapted from a process for evaluating project risk in “Systems Engineering and Analysis” by Blanchard and Fabrycky [9]. Two of the NCI parameters (*D* and *I*) are attributes of the system being changed that can be objectively defined. The other two parameters (*C* and *M*) are dependent on SME evaluation of the details of the change. Together, these four parameters provide an indication of the relative impact that a particular change may be projected to have on NAS systems and safety.

The System Dependency score is defined and described in section 4.1.1.

5.1.1 Change Complexity

A NAS change may range in complexity from a very simple part redesign or software bug fix to a complete redesign of a system that involves many subsystems/modules/interacting elements. Change Complexity (*C*) is a rating of the amount of complexity represented by the proposed NAS change. A low complexity score represents a system change that is readily recognized as a simple design that requires little or no change in adjacent parts or modules. A high complexity score describes a system change that requires many new/redesigned parts, or a very significant increase in the number of (or extensive revision to a large number of existing) software modules and code used by the system.

Unforeseen interactions, emergent behaviors, and undetected bugs or fault paths may potentially increase with NAS change and design complexity. Simple changes can be more readily analyzed and understood and are generally less likely to pose significant hazards and impacts to other systems, so the contribution to overall NCI should be lower.

The change complexity value will be established by AOV users after review of the NAS change description. Details on the NAS change will be found in the relevant SRMD and supplemental documents such as NCPs. Preliminary guidelines for ranking the change complexity are found in table 4.

Table 4. Change complexity scoring criteria

Score	Change Complexity Description	Example SRMD/Rationale
0.9	Extremely complex algorithms/operations	Application of 3-NM Terminal Area Separation Standards for Air Surveillance Radar-11: This SRMD is for the initial deployment of ADS-B, which is a new technology to use GPS to determine aircraft location. The ADS-B provides more precise location information than traditional radars and can provide surveillance coverage in geographic areas not seen by ground-based radars. It is a highly complex system incorporating avionic equipment and ground stations and the ATC CARTS radar display automation.
0.7	Significant complexity or major increase in number of software modules	The SRMD Addendum for Critical Services: ATC Surveillance Services in the Gulf of Mexico With ADS-B and ERAM R2: Significant complexity or major increase in number of software modules. Changes include verification of ERAM R2 interface with subsystems; provision of ADS-B reporting; ADS-B health and status to HCS/ERAM system monitor for ADS-B service certification; and revision of ERAM maintenance handbook similar to HCS for certification and procedures for Virtual Radar application.
0.5	Moderate increase in complexity	SRMD-ATO-T-CARTS-R37A-PHA CARTS Software Release Revision 37a: This revision includes large-scale software modifications to CARTS to include the implementation of a new fused-display presentation mode to accommodate the use of ADS-B inputs. Though the technology to perform this function is proven, the inclusion of this type of software change without corrupting other software is moderately complex.
0.3	Minor increase in complexity or number of software modules	ERAM Flight Plan Updates Not Output to Flight Data Input/Output When Strip Printing Fails (PR57238): Minor rewrites/changes to established ERAM software to update how flight data strip printing and related errors are handled.
0.1	Simple design or existing adaptation/configuration change	Application of 3-NM Terminal Area Separation Standards for Air Surveillance Radar-11: Simple design or existing adaptation/configuration change. No changes were made to the system form or fit. The use of the system was expanded to allow aircraft to fly closer together between 40 and 60 miles from the antenna.

Note**:** Intermediate values 0.2, 0.4, 0.6, and 0.8 may also be used to score *C* at the user's discretion.
ADS-B = Automatic Dependent Surveillance-Broadcast; CARTS = Common Automated Radar Terminal System; ERAM = En Route Automation Modernization; HCS = Host Computer System

5.1.2 System Change Maturity

The system or technology used to implement a NAS change may be well established, generally accepted, and understood by all relevant parties, such as the selection of an existing commercial off-the-shelf product. On the other extreme, the change may involve a state-of-the-art technique and/or the development of equipment, software, and systems that have little or no precedent in the NAS. Most NAS changes will fall somewhere between those two extremes. System Change Maturity (*M*) is an indicator of the precedent for a proposed change, in which a low value is an existing solution and a high value represents increasing levels of redesign and prototyping. A higher *M* score indicates greater potential for unforeseen issues or consequences to the system's operation/failure.

The system change maturity value will be established by AOV users after review of the system and documentation. Details on the system should be found in the system-description section of the SRMD or NCP and maintenance manuals and other supplemental documents recorded in the IDA database. Preliminary guidelines for ranking the system change maturity are found in table 5.

Table 5. System change maturity scoring criteria

Score	Change Maturity Description	Example SRMD/Rationale
0.9	State of the art design, few or no operational examples	Terminal ATC with ADS-B and CARTS: This SRMD addresses ATC use of ADS-B and CARTS with fusion capability to provide terminal air traffic separation services as part of the SBS Program’s Critical Will Verification Services. This is the initial use of ADS-B by the FAA in the Continental U.S. for separation.
0.7	Technology available, complex design	The SRMD for ERAM Release 3 introduced a new function that provides Traffic Flow Management with the capability to send a pre-departure re-route to ERAM (via System Wide Information Management). This change uses state of the art cloud technology, which is in use by other entities but untested in FAA applications.
0.5	Major change or extension of existing technology	SRMD-ATO-T-CARTS-R37A-PHA CARTS Software Release Revision 37a: This is a major software revision to a very mature system. Though the CARTS system has been proven over many years of deployment, this is a life-cycle maintenance update to the CARTS program. It contains Program Technical Reports resolutions to software problems and new and changed functionality.
0.3	Minor redesign of existing product	ERAM Flight Plan Updates Not Output to Flight Data Input/Output When Strip Printing Fails (PR57238): Minor revision of existing software to change how flight data strip printing and related errors are handled.
0.1	Deployment of existing hardware or software	Application of 3-NM Terminal Area Separation Standards for Air Surveillance Radar-11: This SRMD allows the time-tested ASR-11 radar system to be used for 3-mile separation for aircraft between 40 and 60 miles from the radar antenna rather than the 5-mile separation previously used. This had already been allowed with the mode S ASR-9 system with no negative consequences.

Note**:** Intermediate values 0.2, 0.4, 0.6, and 0.8 may also be used to score *M* at the user’s discretion.
ADS-B = Automatic Dependent Surveillance-Broadcast; CARTS = Common Automated Radar Terminal System; ERAM = En Route Automation Modernization

There appears to be a correlation or relationship between change maturity and change complexity in the examples shown in table 5. The SRMD examples used to illustrate each level have similar values for both scores. However, this is not necessarily the case for all possible NAS changes. It should be emphasized that these two scores should be assessed independently for each NAS change because it is possible for a mature, established system to undergo a technically complex revision or to implement a simple change in a new, immature NAS system.

5.1.3 System Dependency

The System Dependency (*D*) score rates the number and the strength of the connections or interfaces that a given system has with other systems in the NAS. Details for calculating *D* are given in section 4.1.1.

5.1.4 System Safety Influence

System Safety Influence (*I*) is an indication of the degree to which a system is expected to influence safety risks/provide safety functionality. This score is particularly concerned with the number of hazards that rely on the system as a hazard control or that may be caused by the system, not just the number of systems that have direct interfaces. A system with a high *I* value is a "mission-critical" system in which loss or failure could result in a hazardous or catastrophic safety effect. By way of comparison, a system with a low *I* value does not directly cause or mitigate any identified hazards, and, therefore, a loss of functionality is expected to have little or no immediate safety effect.

System Safety Influence is a composite of the System Cause Influence (I_{cause}) and System Control Influence ($I_{control}$) scores. Figure 9 shows the relationship between these two scores and their input parameters.

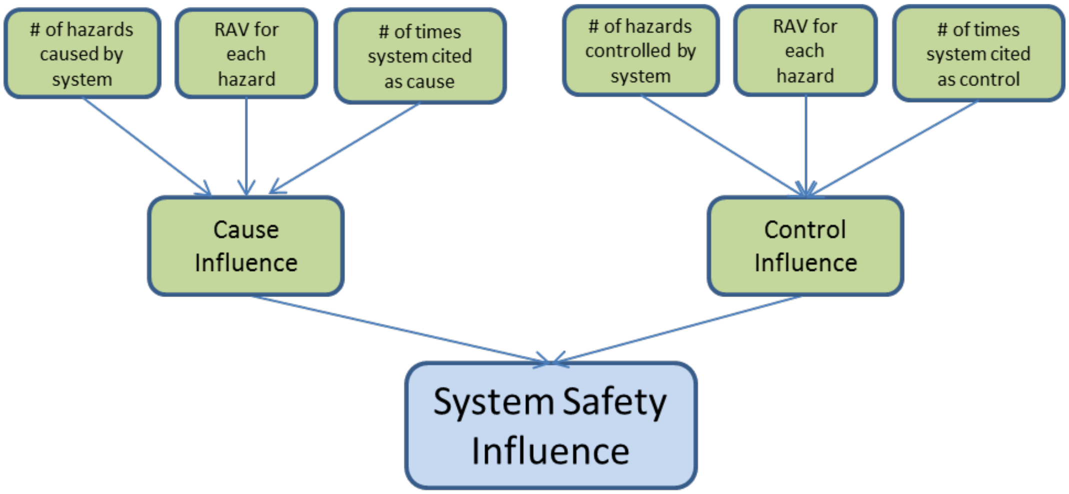

# of hazards caused by system
RAV for each hazard
# of times system cited as cause
# of hazards controlled by system
RAV for each hazard
# of times system cited as control
Cause Influence
Control Influence
System Safety Influence

Figure 9. System safety influence factors

The methodology for calculating (I_{cause}) is discussed in section 4.1.2. The methodology for calculating ($I_{control}$) is discussed in section 4.1.3. The *I* is calculated by:

$$I = \omega_5 I_{cause} + \omega_6 I_{control} \tag{4}$$

where ω_5 and ω_6 are weighting factors that sum to 1. These factors are initially set to 0.5 (equivalent weight), but these weights may be adjusted based on additional study and input from SMEs. This results in a score of relative safety influence for the system in which the higher the *I* value, the greater the chance that a loss of function or error in the system could have a large safety effect. Table 6 summarizes the meaning of relatively higher or lower values of *I*.

Table 6. System safety influence score meanings

I	Level of Influence
1	Functional loss/error in the system will produce catastrophic safety effects in multiple external systems (unrealistic score)
0.5	Functional loss/error in the system could produce a significant safety effect in the NAS (maximum expected score)
0	Functional loss/error in the system will have minimal safety effects

5.2 THE NCI SCORE CALCULATION

The IDA uses a linear-weighted product method to calculate and score the NCI of a system change. The basic equation used to score NCI is:

$$NCI = \omega_7 C + \omega_8 M + \omega_9 D + \omega_{10} I \tag{5}$$

where ω_7, ω_8, ω_9, and ω_{10} are weighting factors that sum to 1.

These factors are initially set to 0.25 (equivalent weight for all parameters), but these weights will be adjusted based on additional study and input from SMEs.

Note that *C* and *M* are scored for each proposed NAS change, and there may be significant variation in these values from NCP to NCP or from SRMD to SRMD. The *D* and *I* are calculated for the system that is being changed and will see relatively little variation when calculated for two changes occurring around the same time. The *D* and *I* may increase or decrease over time based on the evolution of the NAS and as additional SRMDs are modeled in IDA, but will be comparable between systems and NAS changes examined in the same timeframe.

5.3 THE NCI APPLIED EXAMPLE

This case study examines the computation of the NCI score for the change described in an SRMD. The SRMD chosen as an example is entitled “ERAM Flight Plan (FP) Updates Not Output to Flight Data Input/Output (FDIO) When Strip Printing Fails (PR57238).” The proposed change description in the SRMD states:

> "ERAM will be modified to send FDIO flight updates after previously failing to send a flight strip to the FDIO primary or backup devices for the flight. If the flight update strip fails, a new Unsuccessful Transmission Message (UTM) with the time and flight update information will be sent to the adapted Air Traffic Specialist position. Also, the UTM indicator to the applicable EnRoute sector will re-highlight if the previous UTM has been acknowledged" [10].

Based on the change description, the AOV user first scores the change complexity and system change maturity values. Using the criteria in table 4, the user rates $C = 0.3$ because there will be a minor increase in the complexity of En Route Automation Modernization (ERAM) software modules as a result of the FDIO and UTM handling logic in ERAM. Using the criteria in table 5, the user rates $M = 0.3$ because the proposed change is a minor redesign of existing software and logic.

Next, the System Dependency value is calculated for ERAM. System architecture data are used to identify the NAS systems (nodes) that are linked to ERAM. The resultant ERAM system network consists of 14 send-receive nodes, 14 send-only nodes, and 5 receive-only nodes. Plugging these values into the equation in section 5.1.3 produces $N_e = 20$. The equivalent node value is divided by the number of actual nodes to produce $D = 0.588$.

System Safety Influence is calculated based on the hazard data stored in the IDA database. First, the number of hazards that cite ERAM as a cause are identified, and the RAV score for each hazard is computed. The ERAM is not cited as an external cause for any hazards, but it is an internal cause for 22 hazards. Multiplying the RAV score for each hazard by the number of times ERAM is cited as a cause, and dividing by the maximum possible RAV score (323.8) results in a cause influence score of $I_{cause} = .0322$. Similarly, the control criticality score is obtained by querying IDA for the hazards that cite ERAM as a control. The ERAM is an internal control for 15 hazards. The resultant control influence score is $I_{control} = .0067$. The IDA combines I_{cause} and $I_{control}$, as described in section 5.1.4. The final value for $I= 0.0195$.

Taking these values for *C, M, D,* and *S,* IDA multiplies each score by the relevant weighting factor. For this example, the weighting factors are assumed to be equivalent, so they are all set to 0.25. These values may be updated once additional feedback is obtained from SMEs:

$$NCI = \omega_1(0.3) + \omega_2(0.3) + \omega_3(0.588) + \omega_4(0.195) \tag{6}$$

The NCI score for this SRMD = 0.302.

As more system and SRMD data are added to IDA, NCI scores will be produced for additional NAS changes. The distribution of NCI scores will be analyzed in conjunction with AOV user feedback to determine threshold values for low, medium, and high change impact scores. Developing these ranges will improve the utility of NCI scores for AOV safety oversight activities.

5.4 FUTURE ENHANCEMENTS

Some possible adjustments to the scoring methodologies may be considered for further research and development. This section outlines potential refinements that may be evaluated as IDA development progresses.

The NCI entails two parameters that require AOV SME inputs to determine: NAS change maturity (*M*) and change complexity (*C*). Because users may differ regarding how mature or complex a NAS change is, a study may need to be conducted to determine inter-rater reliability and to adjust rating guidelines to improve rating consistency. In addition, use of a numeric versus qualitative rating scale for maturity and complexity may need to be evaluated after IDA is extended to additional systems and SRMDs.

Because NCI relies on subjective user inputs, SI was identified as an alternative indicator to characterize potential safety impacts of a system in the NAS. Both indicators will initially be maintained in the IDA prototype to allow AOV to evaluate how useful each indicator is in prioritizing systems (and associated SRMDs) for oversight action. After AOV has sufficient run time to experiment with both indicators, a decision may be made to maintain both or only one of these indicators.

Finally, System Safety Influence scoring is dependent on available SRMDs that reference the SOI. This constraint is not an issue for the eight legacy systems selected for initial IDA study because historical SRMDs were obtained for all these systems. When IDA is applied to additional systems, however, NCI results may not reflect the potential safety impact of new NAS system acquisitions because, initially, there will be no SRMDs for those new systems. For new systems or systems that lack SRMDs, an alternate parameter of system service criticality based on FAA-assigned service classifications could be used.

According to NAS SR-1000, NAS systems may be classified as Critical, Essential, or Routine service. Each of these classes has specific requirements for reliability, maintainability, and availability. These service classes are assigned to a system based on system function and the possible impact to operations and safety if it is unavailable. These service classes may be used as part of an alternate approach to determine System Safety Influence until the system has enough SRMDs so that a more representative score may be calculated.

6. THE CE

6.1 BACKGROUND

The AOV is responsible for reviewing and approving controls that are recommended to mitigate high-risk hazards and concurring with controls that cross multiple lines of business within the FAA. To do so, AOV developed criteria as part of a REW to assess the adequacy of ATO SRMDs. The REW asks AOV evaluators to examine various aspects of the ATO's hazard analysis and to determine whether there is "evidence to dispute" the effectiveness of both existing and recommended controls (among other criteria).

For IDA purposes, the effectiveness of controls is defined as the capability of achieving the initial risk (in the case of one or more existing controls) or the reduction from initial to predicted residual risk (in the case of one or more recommended controls). Risk is the composite of the severity of a hazard's effects and the likelihood that those effects occur. Risk is affected by the combination of hazard causes, the system state (or operating environment characteristics), risk-control effectiveness, and the effects of the hazard. One or more controls are put into place to mitigate or prevent the hazard causes/effects. If new controls are proposed as part of a safety analysis (and documented in an SRMD), then the predicted residual risk is assessed based on an assumption that both recommended and existing controls are effective. It should be noted that neither existing AOV guidance material on SRMD evaluation nor the ATO's SMS Manual explicitly define CE; the definition proposed in this report is intended to support IDA objectives only.

The CE may be influenced by factors such as the adequacy of the risk-mitigation approach, the performance of the implemented controls, and the stability of systems on which controls depend, among other factors. Arguably, a hypothesis that controls are effective could be tested against the observed frequency and severity of safety incident occurrences over time. However, certain real-world limitations and other constraints preclude pursuing an empirical approach to evaluating CE for AOV purposes. One key limitation of the initial evaluation of CE (for the purpose of making an AAC decision) is that controls and NAS changes do not have enough "run time," if any, in an operational setting; AAC decisions are typically made before a NAS change is implemented operationally. As a result, validation and verification of controls is accomplished within a limited testing period and test environment. Some risks entail extremely improbable frequencies of occurrence, and it is not feasible to validate the frequency of rare events with any statistical confidence during a limited testing period. Furthermore, the testing environment is not necessarily representative of the range of operating environments applicable to the NAS change.

Another limitation for determining or validating CE is based on the lack of traceability between safety incident data and the functional, system, subsystem, and operating and support hazards in ATO equipment SRMDs. Publically available safety incident and occurrence data (e.g., NASA Aviation Safety Reporting System (ASRS), NTSB, and FAA Aviation Safety Information Analysis and Sharing Accident and Incident Data System) are difficult to trace to specific ATO equipment faults and failures. These sources typically identify aircraft, avionics, environmental factors, or human factors as contributors to safety incidents. The ASRS does include ATC equipment as a contributing factor, but keyword searching ASRS records by variants of ATO equipment names and then confirming that the incident narrative actually relates to an ATO equipment hazard occurrence is not practical on a large scale.

One of the IDA's key functions is to evaluate CE to support two AOV safety oversight roles—SRMD evaluation for AAC purposes versus maintaining Safety Management Action Review Team (SMART) situational awareness of NAS system safety issues. In the case of SRMD evaluation, an AAC decision is typically made before a new system of NAS change is implemented. This means that there is limited, if any, information on the performance of that system or NAS change at the time the AAC decision is required. Therefore, an initial evaluation of CE cannot depend on performance but may instead assess the theoretical adequacy of the control strategy design. In addition, AOV has indicated that its mission is not to recreate the ATO's safety analysis but rather to identify what, if any, findings may dispute the adequacy of the ATO's safety analysis or its compliance with safety standards. In addition to AAC, AOV also has a safety oversight role that requires life-cycle monitoring and insight into CE after a NAS change is implemented, whether or not an AAC decision was ever requested for the SRMD accompanying that NAS change. This role of maintaining situational awareness of NAS safety issues is part of AOV's SMART charter. The SMART monitors safety issues associated with new NAS systems, equipment modifications, and equipment decommissioning/removal. Safety concerns identified by the SMART are elevated for AOV management action and potentially AOV audit. For example, cases in which a system is cited as or required for a risk control in multiple SRMDs may get flagged for SMART attention, particularly if that system is undergoing modifications or removal.

Based on how CE would be used for AOV's different safety oversight roles and the data available to AOV, the following objectives and constraints are identified for a methodology to evaluate CE:

1. An initial assessment of CE in achieving initial and predicted residual risk is needed at the time of the AAC decision request (e.g., typically before the NAS change is implemented).
2. The purpose of the initial assessment of CE in the AAC context is to support AOV's decision process to approve (or concur), reject, or request additional information from the ATO regarding the risk controls for the NAS change. That is, the CE assessment is not intended to serve as an independent validation and verification of the safety risk or risk-control requirements identified in an SRMD.
3. The technical approach should not attempt to redo or develop a safety risk analysis to cross-check the ATO's assessment of initial and predicted residual risk likelihood and severity. Consequently, CE is relative to "achieving" the target risk level as established by the ATO.
4. The CE should be monitored periodically to enable the SMART to identify NAS systems (or NAS system changes) for risk-based prioritization of AOV audit and or AOV management attention.
5. The technical approach should use only data that are available to AOV without the need for special access permission.

Additional objectives and constraints for evaluating CE are derived by examining the initial IDA dataset comprising 57 SRMDs for 8 NAS systems:

1. The technical approach for assessing CE must accommodate SRMDs with a mix of hazard and hazard-cause types. Though the scope of the initial IDA research focuses on NAS system equipment, the SRMDs sampled include not only equipment functional hazards but also process hazards related to the deployment, operation, and maintenance of NAS systems.
2. The technical approach must also accommodate SRMDs with a mix of controls that entail any of the following: equipment function; design and performance requirements; testing; installation; operational and maintenance procedures; human factors; and training.
3. The CE must be assessed for SRMDs with one or many existing controls and 0, 1, or many recommended controls.
4. Effectiveness relative to achieving initial risk must be assessed in addition to predicted residual risk; 200 of 290 hazards (or 69%) for 8 NAS systems entailed no risk reduction (i.e., predicted residual = initial risk).

6.2 THE CE PARAMETERS

This section presents a methodology for establishing a qualitative CE score for a set of controls identified for a given hazard. Therefore, each hazard has one CE score. For ease of reference, this report refers to a "set of controls" for cases in which an SRMD contains only one control (existing or recommended) and cases in which an SRMD contains multiple controls (existing/recommended). Sections 6.2.1–6.2.3 define the parameters used for evaluating CE.

Figure 10 shows the attributes of a risk-mitigation approach, which in turn influences CE. A set of rules is applied to determine whether a set of controls satisfies basic principles of SRM, consistent with the ATO SMS Manual and other safety-management guidance. Specifically, the risk-mitigation approach addresses criteria for control suitability, reliance on hazard detectability, defenses in breadth, defenses in depth, and autonomy of controls. These criteria are defined as follows and described in sections 6.21–6.23:

- Suitability–Consistency between control type, cause type, and risk rating.
- Defenses in Depth–Difference between the number of controls and the number of hazard causes.
- Defenses in Breadth–Variety of control types.
- Control Autonomy–Independence of controls from the system experiencing or causing the hazard.

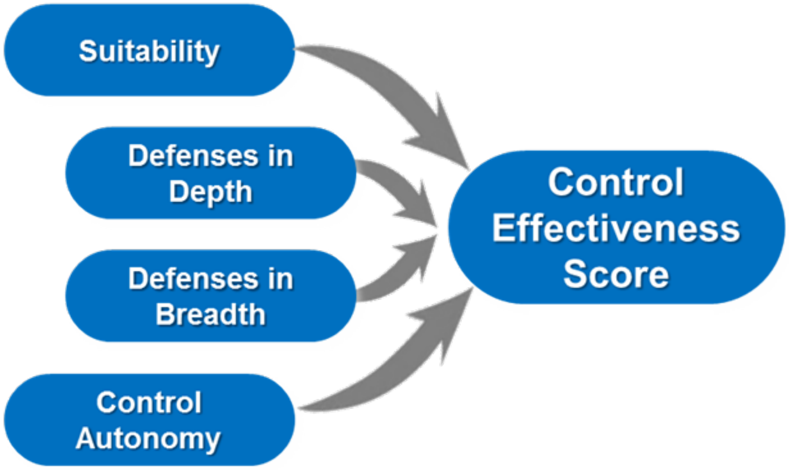


Figure 10. The CE parameters

6.2.1 Suitability

The Suitability of risk mitigation considers whether the control strategy is consistent with the type of hazard causes and risk rating. The rules for assessing suitability are adapted from a technique proposed by White and Benner [12]. In that paper, the authors proposed numerical rankings for each severity-likelihood pair in a risk matrix used in the Department of Defense's MIL-STD-882. Potential risk controls (or corrective actions) are also ranked by applying a Safety Order of Precedence (SOP), in which design for minimum risk is the preferred method to eliminate risk, and procedures and training are a last resort when risk cannot be eliminated or reduced through design, safety devices, or warnings. The suitability of potential risk controls is evaluated by comparing the consistency between risk and control rankings. Specifically, the risk rank should never be more than 1 higher than the highest control rank (e.g., controlling an unacceptable high risk through design is preferred, though use of an automated safety device is also appropriate in certain cases). Applying only a warning device or procedural controls is not suitable for the same high risk. Controlling an undesirable medium risk may be accomplished through non-automated safety devices (and automated safety devices and design); however, applying only warnings and procedures is not recommended. Acceptable low risk may be treated through the use of warnings and procedures.

For IDA, evaluation of control suitability compares the type of control with the type of hazard cause. Control types and values are based on the SOP described in the ATO SMS Manual version 2.1. The SOP ranks four types of controls by order of effectiveness and desirability, as shown in table 7. Based on SMS guidance, the preferred safety-risk mitigation approach for high-risk hazards is to design the system to eliminate risk. Cause types and values presented in table 8 are based on the Draft IDA Taxonomy Development Report, which provides a classification scheme for hazard causes. There are four high-level cause types—Equipment, Process, Human, and Environment—consistent with classifications developed by the Safety Management International Collaboration Group in the Development of a Common Taxonomy for Hazards and the ATO Office of Safety's preliminary Common Taxonomy.

Table 7. Control types and values

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

Table 8. Cause types and values

Cause Type	Description	Value
Equipment	System design or development flaws; hardware, software, or interface faults or failures; latency/timing faults; data corruption; or system interoperability flaws.	4
Process	Management, procedural, or documentation issues (e.g., improper coordination of airport test events, installation faults, adaptation/configuration errors, system maintenance errors, etc.).	3
Human	Incorrect action or inaction on the part of a human operator, user, or maintenance support. Physical or psychological limitations on human performance in the system state. Insufficient/out-of-date/incorrect training in relevant operations/procedures/ conditions.	2
Environmental	Climate, weather, or natural disasters that affect a system. Radiofrequency interference, heavy traffic, or other conditions that impact a system's operating environment. The physical conditions and infrastructure in which equipment operates.	1

For control suitability, IDA applies minimum Boolean rules to determine whether the difference between the numeric values assigned to control type and cause type is acceptable according to risk level. For a high-risk hazard, the highest-valued control type must be greater than or equal to the highest-valued cause type for the hazard. For example, a high-risk hazard with an equipment cause (cause type = 4) must have at least one design control (control type = 4). For a medium-risk hazard, the highest valued control type must be greater than or equal to the highest valued cause type minus 1. So, for example, a medium-risk hazard with a process cause as the highest value (cause type = 3) may be mitigated by design, safety device, or warning controls (control types 4, 3, and 2, respectively). For a low-risk hazard, the highest valued control type must be greater than or equal to the highest valued cause type minus 2.

The IDA approach for assessing control suitability by comparing the control SOP level to the cause type according to risk level is a simplified version of the White and Benner methodology [12] and allows a true/false decision to be quickly evaluated for any hazard in the IDA database. Rule-based logic is applied to flag hazards for AOV review when control suitability may need closer inspection. However, IDA is not a substitute for AOV subject matter expertise in evaluating whether the complete set of controls adequately addresses the mix of hazard causes, operating environment characteristics, system state variants, and range of safety effects.

6.2.2 Defenses in Breadth and Defenses in Depth

Another aspect of the risk-mitigation approach is the degree to which defenses in breadth and depth are used to mitigate hazards. According to the "Swiss-cheese model" of risk, by implementing different types of hazard controls across a system, multiple barriers to hazards can be created. The more barriers of different types that are created, the more resistant the system will be to errors and potentially unsafe conditions. It also follows that the higher the risk that is presented by a hazard, the more important defenses in depth and breadth become to adequately mitigate the hazard.

The control types summarized in table 7 are used to characterize defense in breadth. The IDA counts the number of different control types used within a set of controls to establish breadth. For example, a set of controls that uses design and warnings but no other control types would be assigned a breadth of 2. The IDA applies minimum Boolean rules to determine whether defense in breadth is acceptable according to risk level. For a high-risk hazard, defenses in breadth must be at least 3, whereas a medium-risk hazard must have at least two different control types.

In keeping with SMS guidance, the preferred risk-mitigation strategy is to design the system to eliminate risk. The higher the risk, the more emphasis is placed on "designing out" hazard causes. Accordingly, IDA assesses defenses in depth according to the difference of the number of existing and recommended controls and the number of hazard causes. For high-risk hazards, the number of existing and recommended hazard controls must be the number of hazard causes. For medium-risk hazards, the number of existing and recommended hazard controls must be at least 2/3 of the number of hazard causes (this threshold may be adjusted pending further evaluation of SRMD data and feedback from AOV SMEs). It should be noted that few SRMDs sampled actually provide an allocation of controls to specific causes, system state parameters, or risk effects. Therefore, IDA cannot determine whether certain controls are intended to mitigate system state elements or alleviate the severity of risk effects rather than addressing hazard causes. The approach for characterizing defenses in depth relies instead on a minimum rule set that flags high and medium risks that have more causes than controls over a given threshold ratio.

6.2.3 Autonomy

A risk-mitigation approach may also entail autonomy (the reliance of a control strategy on internal versus external systems and processes). An internal control is one that is a part of the system design, and an external control is a system or process that is independent of the system that may experience or cause the identified hazard. In general, controls that are internal to a system tend to mitigate the causes of a hazard, whereas external controls tend to mitigate the effects or outcome of the hazard once it has occurred.

The IDA applies a minimum rule for high-risk hazards to confirm that at least one recommended control is external (i.e., that control is not dependent on the system causing or experiencing the hazard). The external control may, for example, involve an independent backup system or contingency procedures executed by personnel.

6.3 THE CE SCORING METHOD

Parameters for evaluating the adequacy of a risk-mitigation approach are presented in section 6.2. Each parameter is associated with criteria for determining CE according to low, medium, and high initial risk as outlined in table 9. Each criterion is evaluated as true or false based on whether the conditions specified in the applicable column are met.

Table 9. Risk Mitigation Approach Criteria

	Criteria		
Parameter	High Initial Risk	Medium Initial Risk	Low Initial Risk
Suitability *Consistency between control type, cause type, and risk rating*	The highest-valued control type must be greater than or equal to the highest-valued cause type for the hazard. *Note: See 6.2.1for values assigned to cause types and control types* max control type >= max cause type	The highest-valued control type must be greater than or equal to the highest-valued cause type minus 1. max control type >= max cause type - 1	The highest-valued control type must be greater than or equal to the highest-valued cause type minus 2. max control type >= max cause type -2
Depth *Ratio of hazard causes to controls*	The number of existing and recommended hazard controls must be more than the number of hazard causes.	The number of existing and recommended hazard controls must be at least 2/3 of the number of hazard causes.	N/A
Breadth *Variety of control types*	Existing and recommended controls must include at least three different SOP types.	Existing and recommended controls must include at least two different SOP types.	N/A
Autonomy *Independence of controls from system hazard*	At least one recommended control must be external (i.e., that control is not dependent on the system causing or experiencing the hazard).	N/A	N/A

The combinations of true and false values for a control set are mapped to a qualitative CE score in table 10. The CE scores range from weak to strong based on which criteria are true or false. To obtain a "strong" CE score, all criteria (suitability; defenses in breadth and depth; and autonomy of controls) must be true. If suitability is false, then CE is considered "weak." If suitability is true, and only one other criterion is false, then CE is "somewhat strong." If suitability is true, and two out of the three other criteria are false, then CE is "moderate." Finally, if breadth, depth, and autonomy are all false, then CE is considered "weak."

Table 10. The CE scoring

Criteria	Result (T = True F= False - = True or False)									
Suitability	T	T	T	T	T	T	T	T	F	-
Depth	T	F	T	T	F	F	T	F	-	-
Breadth	T	T	F	T	F	T	F	F	-	-
Autonomy	T	T	T	F	T	F	F	F	-	-
CE	Strong	Somewhat Strong	Somewhat Strong	Somewhat Strong	Moderate	Moderate	Moderate	Weak	Weak	Weak

6.4 THE CI

Characterizing CE alone is not sufficient for AOV to make AAC decisions. For example, controls with potentially weak effectiveness may not warrant an AAC decision to disapprove a risk control if the initial risk level is low. Instead, CE needs be compared with the initial risk of the hazard to determine how important the control set is at mitigating risks. Assessing the importance of the control set helps to support AOV's AAC decision.

To support AOV's AAC decision process, CE is compared against initial hazard risk to rate the importance of each control set within an individual SRMD. SRMDs with hazards with high CI scores may be unacceptable for control approval or concurrence. Conversely, SRMDs with weak CE but low hazard risk may be acceptable with or without contingencies. A matrix of CI is presented in figure 11 along with the suggested AAC approval consideration.

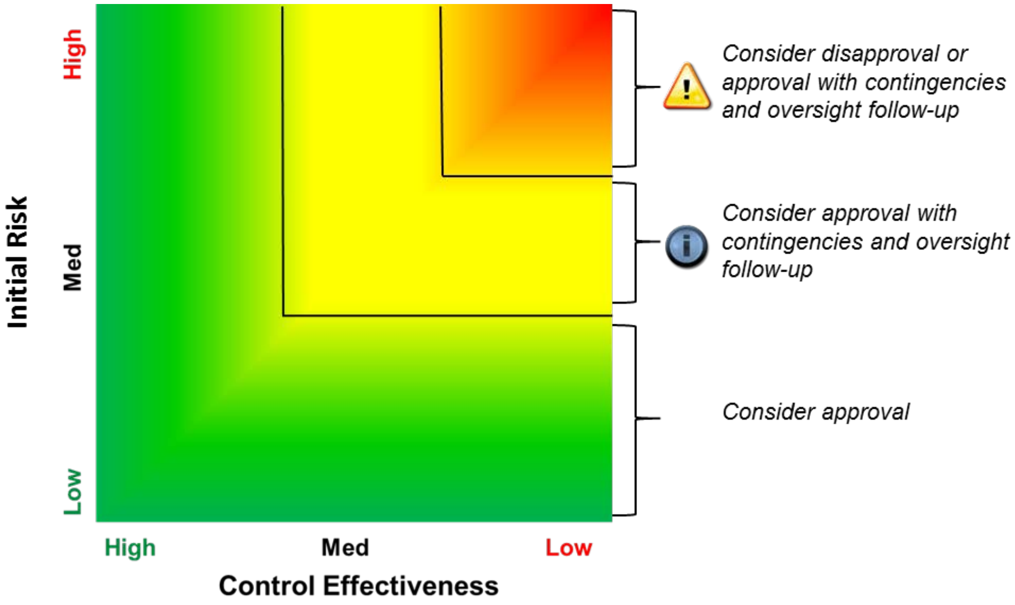
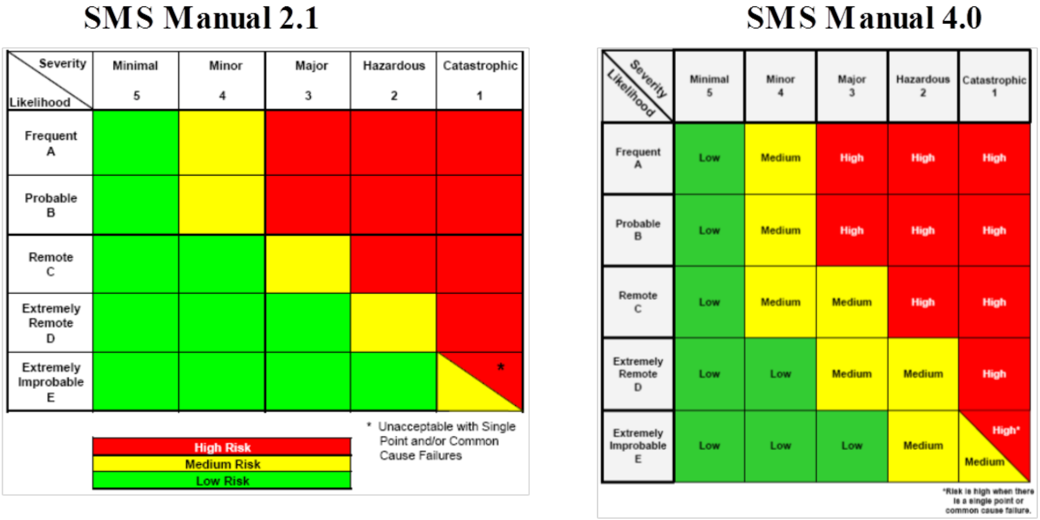


Figure 11. The CI for AAC decision

It should be noted that ATO SMS Manual version 4.0 changes the level of risk from low to medium for three severity-likelihood pairs in the SMS Manual 2.1 risk matrix [10]. Figure 12 provides a side-by-side comparison of the risk matrices for SMS Manual 2.1 versus 4.0. The CI rules should be consistently applied, regardless of what SMS Manual version was used during preparation of the SRMD. Accordingly, it is recommended that the more conservative risk levels in SMS Manual 4.0 be used as indicated in figure 12.



SMS Manual 2.1

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	🟩	🟨	🟥	🟥	🟥
Probable B	🟩	🟨	🟥	🟥	🟥
Remote C	🟩	🟩	🟨	🟥	🟥
Extremely Remote D	🟩	🟩	🟩	🟨	🟥
Extremely Improbable E	🟩	🟩	🟩	🟩	🟨 🟥 *

🟥 High Risk
🟨 Medium Risk
🟩 Low Risk

* Unacceptable with Single Point and/or Common Cause Failures

SMS Manual 4.0

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	Low	Medium	High	High	High
Probable B	Low	Medium	High	High	High
Remote C	Low	Medium	Medium	High	High
Extremely Remote D	Low	Low	Medium	Medium	High
Extremely Improbable E	Low	Low	Low	Medium	High* Medium

*Risk is high when there is a single point or common cause failure.

Figure 12. The ATO SMS risk matrices

6.5 A CE APPLIED EXAMPLE

One SRMD was selected to show the application of the CE scoring method:

- En Route Automation Modernization (ERAM) Flight Plan (FP) Updates Not Output to Flight Data Input/Output (FDIO) when Strip Printing Fails (PR57238) SRMD, May 16, 2012

In the case of the ERAM SRMD, one high-risk hazard was identified and provided to AOV for an AAC decision; this hazard (PR 57238- 01) as shown in table 11 is the focus of this example. The type values assigned to each cause and control are highlighted and denoted by brackets.

Table 11. The ERAM hazard PR 57238-01

Hazard Description: PR 57238- 01 AT Controller at Terminal Facility is unaware of a Flight Plan notification and there is also no indication of the failure to update the Flight Plan provided to the Center Controller.		
Current/Initial Risk: High 2C		Predicted Residual Risk: Low 2E
Causes ERAM failed to provide notification of a failed amendment/update message [Equipment].	Existing Controls The FDIO (tower inbound) facility should get an amendment strip with accurate information or EnRoute should get a UTM if information is not passed [Design]. Non-radar coordination is required per 7110.65, paragraph 2-1-14. This coordination could be automated (sending of the strip to the FDIO facility) or manual. If the EnRoute controller is aware that the tower is not getting a strip, manual coordination is needed. A nonradar tower requires verbal coordination to perform handoff. The altitude information provided is just the cleared for approach (not an actual altitude). If the EnRoute controller changes anything of significance, verbal coordination is needed again [Procedure]. Controller training is to coordinate verbally when there is an amendment to a flight going to a non-radar tower facility. However, some Air Route Traffic Control Centers (ARTCCs) just apply this to situations without flight data, and flight data are available in this case. FAA Order 7110.65 Paragraph 2-1-16 says you do not need to manually coordinate, and a Letter of Agreement may allow the coordination to occur via automated means [Training].	Recommended Controls When EnRoute receives a UTM for an arrival into an FDIO-only equipped facility, coordinate the UTM and notify the OMIC Operations Manager In Charge/Tech Ops to check the interface and verify printer status. AT mitigations must begin with manual coordination for all additional changes to the flight [Procedure]. Ensure FDIO opening procedures are in facility checklist Tech Ops/Operations Manager In Charge/TMU as applicable [Procedure].

Note: When there is a failure to send flight plan for a flight to an external interface, a UTM event occurs and the state is set to manual for the flight to the external interface to indicate manual coordination is required. When the coordination state is manual, no further updates are sent. However, it was found that this rule does not apply for FDIO positions.

6.5.1 Suitability

The ERAM hazard PR 57238-01 includes one cause and four controls. The cause and control types are shown in Table 12. The highest valued cause type is a “4,” an equipment-related cause, and the highest-valued control type is also a “4” for design. Accordingly, the suitability criteria for initial high risk is TRUE given that the difference between the highest valued cause and highest valued control is zero.

6.5.2 Defenses in Depth

The ERAM hazard PR 57238-01 includes one cause and four controls per table 12. Therefore, the number of existing and recommended controls is more than the number of hazard causes, which means the initial high-risk criteria are met. Defenses in depth is TRUE.

Table 12. The ERAM PR 57238-01 cause and control types

Cause Type (Value)	No. Causes
Equipment (4)	1
Environmental (3)	0
Process (2)	0
Human (1)	0
Total No. Causes	1

Control Type (Value)	No. Controls
Design (4)	1
Safety Device (4)	0
Warning (3)	0
Procedures (2)	3
Training (1)	0
Total No. Controls	4

6.5.3 Defenses in Breath

The ERAM hazard PR 57238-01 includes two different types of controls, as per table 12. The criteria for initial high-risk defenses in breadth were not met; therefore, defense in breadth is FALSE.

6.5.4 Autonomy

As shown in table 12, ERAM hazard PR 57238-01 includes three procedural controls. However, the controls rely on ERAM first issuing a UTM for the procedure to be executed. As a result, the controls have an internal dependency on the ERAM system. In this case, autonomy is FALSE.

6.5.5 Summary

In summary, CE would be considered “Moderate” for ERAM hazard PR 57238-01 given the combination of true and false values for the criteria in table 13. To support an AAC decision evaluation, CI is compared with CE. Because ERAM hazard PR 57238-01 has an initial risk of 2C (high), the CI relative is also high.

Table 13. The ERAM hazard PR 57238-01 CE score

Criteria	Result
Suitability	T
Breadth	T
Depth	F
Autonomy	F
CE	Moderate

Finally, the “Moderate” CE is charted against the High initial risk of the hazard, as shown in figure 13. Because it falls into the yellow portion of the matrix, AOV may choose to approve the hazard controls, but might request additional monitoring or follow-up on the hazard to ensure that the controls are effective.

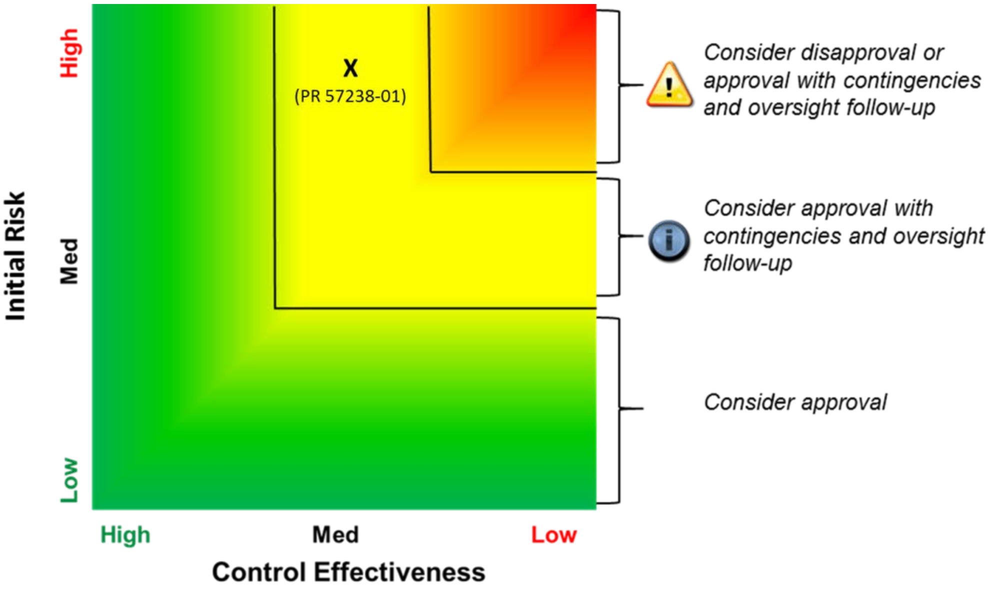


Figure 13. Initial risk versus effectiveness (ERAM hazard PR-57238-01)

7. SYSTEM MONITORING

Though CE is assessed primarily for AAC decision purposes, the AOV’s SMART may benefit from continued monitoring of system performance, particularly when a system provides hazard controls. The AOV’s SMART maintains situational awareness of NAS equipment changes and elevates safety concerns for AOV management action and, potentially, AOV audit. As NAS changes proceed from a planning stage into implementation and in-service management, CE and control performance may also change. Accordingly, several parameters have been identified for monitoring the performance of equipment-related controls over time. The selection and use of these parameters was adapted from a process for evaluating project risk in Blanchard and Fabrycky [9]. Sections 7.1–7.3 define these parameters in detail.

7.1 SYSTEM INSTABILITY

System Instability is an indicator of the number and timing of system changes and the degree to which the system may be disrupted by those changes.

A control strategy that is dependent on a system is only as stable as the underlying system. NAS changes, such as the introduction of a new system, equipment modifications (e.g., due to technology refreshes, system upgrades, etc.), and equipment replacement/decommissioning, all represent potential instabilities that could affect the performance of the control strategy.

Controls relying on systems that are undergoing significant changes may have a period of reduced performance or availability or an increase in the number of system anomalies. A highly stable control strategy relies on systems with established operational service records that have no, or only minor, planned changes for the foreseeable future. An unstable control strategy relies on new systems that have yet to be implemented (and therefore have no service record) or that are scheduled for near-term decommissioning/removal.

System Instability is calculated based on NAS change data and change type classifications stored as part of the IDA model.

Instability is given by:

$$Instability = \sum_{i=1}^{n_{near}} (d_{near})_i + 0.5\sum_{i=1}^{n_{far}} (d_{far})_i + 0.25\sum_{i=1}^{n_{complete}} (d_{complete})_i \tag{7}$$

where *i* is systems 1…n required to execute the set of controls; n_{near} is the number of changes to be completed for system *I* within the next 3 years; n_{far} is the number of changes planned for system *i;* $n_{complete}$ is the number of changes completed in the past 2 years; d_{near} is the degree of changes to be completed for system *i* within the next 3 years, where degree is assigned according to the following heuristics: 1 = system modification, 2 = new system, and 3 = removal/decommissioning; d_{far} is the degree of changes planned for system *i* after the next 3 years, where degree is assigned according to the following heuristics: 1 = system modification, 2 = new system, and 3 = removal/decommissioning.

Far-term NAS changes are weighted by a 0.5 multiplier to account for the uncertainty in the approval, final scope, and timeframe of a planned change. Similarly, recently completed NAS changes are weighted by a 0.25 multiplier to account for the minimal, but likely nonzero, disruption that they may produce in the system.

Based on the range of input values, the maximum possible Instability score is 4. This represents a “worst-case scenario” of a system that is installed as a new system, undergoes multiple system modifications, and is decommissioned and removed all within a short period of time (7 years). Therefore, the instability score for a system is divided by 4 to normalize the score to a value between 0 and 1.

The process for calculating Instability is as follows:

1. Identify the SOI.
2. Identify all NAS changes for the SOI.
3. For each change in step 2, assign a degree score based on its change type:

    a. Modification = 1
    b. New System = 2
    c. Decommissioning = 3

4. Sort each change in step 2 into one of the following categories:

a. Near-term: Status = in-progress, or start date within 36 months of today's date.
b. Far-term: Start date between 36 and 60 months from today's date.
c. Complete: Status = complete, and end date within 24 months of today's date.

5. Count the number of NAS changes in each category.
6. S_{near} = (sum of near-term change degrees)/(number of near-term changes)
7. S_{far} = (sum of far-term change degrees)/(number of far-term changes)
8. $S_{complete}$ = (sum of complete change degrees)/(number of complete changes)
9. Instability = S_{near} + (0.5*S_{far}) + (0.25*$S_{complete}$)
10. $\text{Instability}_{\text{norm}}$ = Instability/4

The date thresholds for the near-term, far-term, and recently completed change categories are adaptable parameters and may be adjusted based on further research/feedback from SMEs and AOV users of IDA.

7.2 SYSTEM UNAVAILABILITY

System availability accounts for the operational "uptime" of a system relative to the maximum number of operating hours possible in a given time period. Scheduled and unscheduled system outages affect control availability. A safety analysis will typically account for system availability (or unavailability) when calculating the likelihood of a hazard. However, the analysis assumption may vary from actual system performance.

The FAA Remote Maintenance Logging System (RMLS) Log Interrupt Reports (LIRs) are available via the FAA's TechNet website. The LIR tool provides a query capability for system outage records by facility and date range. The IDA uses the count of scheduled and unscheduled outages to determine individual system availability statistics, which are then used to establish an overall availability for a set of recommended controls. The narrative content or description of the outage is not used, only the count of outage durations for a given system across all sites.

System unavailability ($C_{unavailability}$) is given by:

$$C_{unavailability} = 1 - \left[\frac{t_{\max} - t_{outage}}{t_{\max}} \right] \qquad (8)$$

where t_{max} is the maximum number of operating hours possible in a given period for system *i* (e.g., there are 8760 possible operating hours in a year), and t_{outage} is the total number of hours the system was out of service (scheduled + unscheduled downtime) during the same period.

The maximum number of possible operating hours (t_{max}) must be adjusted to account for cases in which the system was not deployed for the full period of time. For example, if a system did not reach initial operational capability until February 1, 2013, then t_{max} is 8016 hours for that system in 2013 (i.e., 8760 hours in year – [31 days in Jan. x 24 hours per day]).

7.3 SYSTEM ANOMALY RATE

System anomaly frequency accounts for the number of reported anomalies in a given time period at all SDPs that receive services from the system. Systems that have frequent faults or errors may impact the effectiveness of a risk-control strategy that relies on correct system performance. Safety analyses may account for system faults, data errors, and other anomalies when identifying hazard causes and likelihoods. As with system availability, safety analysis assumptions on correct system performance may vary from actual performance.

The FAA RMLS Logs of Corrective Maintenance (LCMs) are available via the FAA's TechNet website. The LCM tool provides a query capability for system anomalies that required corrective maintenance actions by facility and date range. The IDA uses the count of corrective actions to determine individual system anomaly statistics, which are then used to establish an overall anomaly frequency for a set of recommended controls. The narrative content or descriptions in the LCMs are not used, only the count of LCM records for a given system across all sites.

System anomaly frequency ($C_{anomaly}$) is given by:

$$C_{anomaly} = \left(\frac{n_{anomaly\_t}}{t_{\max}} \right) \quad (9)$$

where $n_{anomaly\_t}$ is the total number of anomaly records for the system during the given time period, and t_{max} is the maximum number of operating hours possible in a given period for system i (e.g., there are 8760 possible operating hours in a year).

The maximum number of possible operating hours (t_{max}) must be adjusted to account for cases in which systems are not deployed for the full period of time.

8. CONCLUSIONS AND FUTURE RESEARCH

The analysis methods described have been run against the 8 National Airspace Systems and 57 Safety Risk Management Documents modeled in the Integrated Domain Assessment (IDA) prototype to demonstrate the methodology and draw preliminary conclusions about the utility of the indicators. The scores presented in the prototype tool show that the system and safety data in the IDA data model along with IDA's taxonomy support the proposed methodologies for scoring the system and safety indicators addressed in this report. Further research and refinement are recommended as the IDA dataset expands to additional systems and ATC procedure changes to ensure that the IDA methodology remains valid and yields meaningful differences in scores to enable the FAA Air Traffic Oversight Service (AOV) to make risk-based safety oversight decisions.

As IDA development continues, it will be necessary to assess the range of values and sensitivity of the weighting scheme for certain indicators and the rules comprising CE. This assessment will be a vital part of interpreting and validating the scores produced when applying these methodologies to real-world data. Sensitivity analysis will be performed to determine if any of the identified parameters are particularly impacted by small changes in value or if any of the parameters consistently overwhelm other factors in valuation of the final scores. Input will be solicited from AOV users and safety SMEs to adapt and optimize weights assigned to the various input parameters. Additional research and collaboration with AOV will be required to define thresholds for qualitative levels associated with each score and potential corresponding Approval, Acceptance, and Concurrence, Safety Management Action Review Team, and other oversight considerations.

9. REFERENCES

1. FAA Report. (2017). *IDA-FS Concept of Operations* (DOT/FAA/TC-16/53). Report Not Yet Published.

2. FAA Internal Report. (2013). *IDA-FS Preliminary Technical Approach for IDA-FS Modeling.*

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

4. ATO (2008), *Air Traffic Organization Safety Management System Manual*, (Version 2.1).

5. FAA Report. (2014). IDA Taxonomy Development Report (DOT/FAA/TC-17/3). Report Not Yet Published.

6. Flowe, R.M., Kasunic, M., Brown, M.M., Harding III, P.L., McCurley, J.M., Zubrow, D., & Anderson, W.B. (2010). *Programmatic and Constructive Interdependence: Emerging Insights and Predictive Indicators of Development Resource Demand*. Retrieved from http://repository.cmu.edu/sei/13

7. FAA AOV (2013). *Resource Allocation Valuation: A Framework for the Expression of Risk*.

8. Wondolowski, F. (2014). *RAV Math Review: Assumptions and Limitations.* Presentation.

9. Winston, W. L. (1994). *Operations research, applications and algorithms*. (3rd ed.). International Duxbury Press.

10. Blanchard, B. S., & Fabrycky, W. J. (1998). *Systems Engineering and Analysis.* (3rd ed.). Upper Saddle River, New Jersey: Prentice Hall.

11. ATO (2014). *Air Traffic Organization Safety Management System Manual*. (Version 4.0).

12. White, L. M., & Benner, L. Jr. (1985). *Corrective Action Evaluation*. Proceedings from the Seventh International System Safety Conference, San Jose, California.