In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System (2018)

DETAILS

84 pages | 8.5 x 11 | PAPERBACK

ISBN 978-0-309-46880-0 | DOI 10.17226/24962

CONTRIBUTORS

Aviation Safety Assurance Committee; Aeronautics and Space Engineering Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine. 2018. *In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System*. Washington, DC: The National Academies Press. https://doi.org/10.17226/24962.

IN-TIME AVIATION SAFETY MANAGEMENT

Challenges and Research for an Evolving Aviation System

Aviation Safety Assurance Committee

Aeronautics and Space Engineering Board

Division on Engineering and Physical Sciences

A Consensus Study Report of

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

THE NATIONAL ACADEMIES PRESS **500 Fifth Street, NW** **Washington, DC 20001**

This study is based on work supported by Contract NNH11CD57B with the National Aeronautics and Space Administration. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any agency or organization that provided support for the project.

International Standard Book Number-13: 978-0-309-46880-0
International Standard Book Number-10: 0-309-46880-9
Digital Object Identifier: https://doi.org/10.17226/24962

Cover design by Tim Warchocki.

Copies of this publication are available free of charge from

Aeronautics and Space Engineering Board
National Academies of Sciences, Engineering, and Medicine
Keck Center of the National Academies
500 Fifth Street, NW
Washington, DC 20001

Additional copies of this publication are available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; http://www.nap.edu.

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2018. *In-time Aviation Safety Management: Challenges and Research for an Evolving Aviation System*. Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/24962.

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at **www.nationalacademies.org**.

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Consensus Study Reports published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

Proceedings published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

For information about other products and activities of the National Academies, please visit www.nationalacademies.org/about/whatwedo.

AVIATION SAFETY ASSURANCE COMMITTEE

KENNETH J. HYLANDER, Flight Safety Foundation, *Chair*
BRIAN M. ARGROW, University of Colorado, Boulder
MEYER J. BENZAKEIN, NAE,[1] Ohio State University
GAUTAM BISWAS, Vanderbilt University
JOHN W. BORGHESE, Rockwell Collins
STEVEN J. BROWN, National Business Aviation Association
DANIEL K. ELWELL,[2] Federal Aviation Administration
ANTHONY F. FAZIO, Fazio Group International
MICHAEL GARCIA, Aireon, LLC
R. JOHN HANSMAN, JR., NAE, Massachusetts Institute of Technology
GERARDO D.M. HUETO, International Air Transport Association
LAUREN J. KESSLER, Charles Stark Draper Laboratory
JOHN C. KNIGHT,[3] University of Virginia
MICHAEL J. McCORMICK, Embry-Riddle Aeronautical University
BONNIE SCHWARTZ, Air Force Research Laboratory
CRAIG WANKE, The MITRE Corporation

Staff

ALAN C. ANGLEMAN, Senior Program Officer, *Study Director*
MICHAEL H. MOLONEY, Director, Aeronautics and Space Engineering Board and Space Studies Board
ANESIA WILKS, Senior Program Assistant

[1] Member, National Academy of Engineering.
[2] Resigned on April 18, 2017.
[3] Passed away on February 23, 2017.

AERONAUTICS AND SPACE ENGINEERING BOARD

Staff

MICHAEL H. MOLONEY, Director
CARMELA J. CHAMBERLAIN, Administrative Coordinator
TANJA PILZAK, Manager, Program Operations
CELESTE A. NAYLOR, Information Management Associate
MEG A. KNEMEYER, Financial Officer
SU LIU, Financial Assistant (through July 2017)
ANTHONY BRYANT, Financial Assistant (from November 2017)

[1] Member, National Academy of Engineering.
[2] Member, National Academy of Sciences.

Preface

Commercial aviation in the United States and most other regions of the world is the safest mode of transportation. This high-level safety is the result of many factors, including decades of investments by industry and government and the dedication of researchers, engineers, pilots, air traffic controllers, and a great many other members of the aviation community.

The U.S. national airspace system (NAS) is constantly evolving to take advantage of new technologies, to accommodate growth in the volume of air traffic, to integrate new types of aircraft, to increase efficiency, and to maintain or increase safety. NASA's Aeronautics Research Mission Directorate (ARMD) conducts research related to several of these topics, including aviation safety. For example, ARMD is conducting research to support development of a real-time safety assurance system for the NAS. Such a system would operate in real time or near real time to monitor the state of the NAS, identify unsafe risks as they arise, and then assist in mitigating those risks. Research by many organizations other than NASA is relevant to the development of a real-time safety assurance system. Accordingly, ARMD requested that the National Academies of Sciences, Engineering, and Medicine convene a committee to develop a national research agenda that would (1) identify key challenges to the development of a real-time safety assurance system for the NAS and (2) identify high-priority research projects that would overcome those challenges.

The Aeronautics and Space Engineering Board of the National Academies Division on Engineering and Physical Sciences has assembled a committee to carry out the assigned statement of task (see Appendix A). The committee members (see Appendix B) met four times during 2017, three times at the Academies' facilities in Washington, D.C., and once at the National Academies' facility in Woods Hole, Massachusetts. As specified in the statement of task, the committee has developed a research agenda consisting of a set of high-priority research projects organized around four key elements of a real-time aviation safety assurance system: concept of operations and risk prioritization, system monitoring, system analytics, and mitigation and implementation. The report's principal finding summarizes the key challenges, and the principal recommendation summarizes the high-priority research projects (see Chapter 6).

Kenneth Hylander, *Chair*
Aviation Safety Assurance Committee

Acknowledgment of Reviewers

This Consensus Study Report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published report as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

We thank the following individuals for their review of this report:

Ella M. Atkins, University of Michigan,
R. Stephen Berry, NAS,[1] University of Chicago,
Raj M. Bharadwaj, Honeywell Aerospace Advanced Technologies,
Stephen J. Lloyd, SJL and Associates, Inc.,
James T. Luxhøj, Rutgers University,
Brad Shelton, Delta Air Lines,
Agam N. Sinha, ANS Aviation International, LLC,
Alexander J. Smits, NAE,[2] Princeton University, and
John Valasek, Texas A&M University.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations of this report nor did they see the final draft before its release. The review of this report was overseen by Chris T. Hendrickson, NAS, Carnegie Mellon University. He was responsible for making certain that an independent examination of this report was carried out in accordance with the standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the authoring committee and the National Academies.

[1] Member, National Academy of Sciences.
[2] Member, National Academy of Engineering.

In Memoriam

This report is dedicated to Dr. John C. Knight, an accomplished researcher and educator in the field of safety-critical computer systems, especially in the automotive and aerospace fields. He embraced the opportunity to serve on the Aviation Safety Assurance Committee despite a long-term battle with hypersensitivity pneumonitis, and we have missed his camaraderie and counsel in the completion of this work.

Contents

Summary

BACKGROUND

Real-time system-wide safety assurance (RSSA) is one of six focus areas for the National Aeronautics and Space Administration (NASA) aeronautics program. NASA envisions that an RSSA system would provide a continuum of information, analysis, and assessment that supports awareness and action to mitigate risks to safety. NASA's research plans state that development of an RSSA system for the national airspace system (NAS) will necessitate automating safety assurance of air transportation system components, integrating component-level systems, and reducing the safety assurance cycle time until real-time safety assurance is achieved at the system-of-systems level. The safety assurance system envisioned by NASA will combine air traffic and onboard aircraft technologies as well as automated data mining capabilities for continuous safety monitoring and threat prediction.[1] This system is expected to maintain or exceed the current level of aviation safety while accommodating global increases in air travel and rapid introduction of new technologies. The RSSA system would not be expected to directly address issues related to design, development, training, or maintenance because the detection of problems in these areas and the process of implementing corrective actions falls outside the short time horizon of an RSSA. Other systems are already in place to address these aspects of aviation safety.

NASA envisions that the process of developing a comprehensive and fully functional RSSA system would include three intermediate milestones:[2]

- *Domain-Specific*[3] *(Real-time) Safety Monitoring and Alerting Tools (2015-2025).* Expanded system awareness through increased access to safety-relevant data and initial integration of analysis capabilities; improved safety through initial real-time detection and alerting of hazards at the domain level; and decision support for limited, simple operations.[4]

[1] NASA, 2015, *NASA Technology Roadmaps TA 15: Aeronautics*, NASA, Washington, D.C., https://www.nasa.gov/sites/default/files/atoms/files/2015_nasa_technology_roadmaps_ta_15_aeronautics_final.pdf.

[2] Briefing by J. Nowinski at the first meeting of the Aviation Safety Assurance Committee, January 23, 2016, Washington, D.C., p. 6.

[3] One example of a "domain-specific tool" would be a tool that monitors the NAS and determines the system state as it applies to a specific class of aircraft operating in the airspace near a specific airport. After such a tool is demonstrated and validated at that airport, continued development could expand its applicability to other classes of aircraft and other airports.

[4] In the context of this milestone, "limited, simple operations" are intended by NASA to refer to, for example, tools with limited automated decision-making and mitigation capabilities that could be demonstrated and validated in low-risk operations, such as those involving small unmanned aircraft systems (UAS) operating in unpopulated areas.

- *Integrated Predictive Technologies with Domain-Level Application (2025-2035)*. NAS-wide availability of more fully integrated real-time detection and alerting for enhanced risk assessment and support of initial assured human and machine decision support for mitigation response selection for more complex operations.
- *Adaptive Real-time Safety Threat Management (2035-2045)*. Fully integrated threat detection and assessment that support trusted methods for dynamic, multi-agent planning, evaluation, and execution of real-time risk-mitigating response to hazardous events.[5]

Maintaining the safety of the NAS as it evolves will require integration of a wide range of safety systems and practices, some of which are already in place and many of which need to be developed. Maintaining system safety into the future will require rapid detection and timely mitigation of safety issues as they emerge and before they become hazards. This report identifies challenges to establishing an RSSA system and the high-priority research that should be implemented by NASA and other interested parties in government, industry, and academia to expedite development of such a system. In order to assess NASA's vision for an RSSA system and to develop a national research agenda consisting of high-priority research projects, a challenge assessment was conducted in four fundamental system element development areas.

- *Concept of Operations and Risk Prioritization*. A clear concept of operations (CONOPS) is needed to define the scope of an RSSA, to understand how it would work, and to establish the framework for other areas of research. The system's capabilities will need to increase in sophistication as the NAS[6] continues to evolve and improve, while also accommodating continued growth in conventional air traffic and a wide range of new entrants. This report identifies three classes of new entrants that are of particular interest to the development of an RSSA system: UAS,[7] on-demand mobility,[8] and the increasing pace of commercial space operations.
- *System Monitoring*. Aviation safety assurance begins with a monitoring function that observes the system state by fusing varied and complex data from a multitude of sensors.[9] Issues of interest include identifying, characterizing, and collecting high-quality data. Additionally, data regarding operator performance cannot currently be collected in a timely fashion, or at all, in part because of privacy and related concerns.[10]
- *System Analytics*. Sophisticated algorithms and computational architectures will play a central role in the assessment function by interpreting and analyzing the state of the NAS and identifying elevated risk states, which then form the basis for mitigating actions to maintain safe operations. The large volume and heterogeneity of NAS data and the need to align and fuse data from multiple sources make it particularly difficult to develop algorithms, especially machine learning algorithms, that can identify and characterize existing and emergent risk states.

[5] In the context of this milestone, "hazardous events" also refers to hazardous trends and conditions.

[6] The NAS is "the common network of U.S. airspace; air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information and services; rules, regulations, and procedures; technical information; and manpower and material." FAA, 2013, *Integration of Civil Unmanned Aircraft Systems [UAS] in the National Airspace System [NAS] Roadmap*, Washington, D.C., https://www.faa.gov/uas/media/uas_roadmap_2013.pdf. Some NAS facilities are jointly operated by the FAA and the Department of Defense. The NAS includes all aircraft operating in U.S. airspace, both foreign owned and domestic.

[7] An "unmanned aircraft" is, as the name implies, an aircraft that has no onboard pilot. In this report unmanned aircraft are assumed to have no humans on board either as flight crew or as passengers. A UAS is an unmanned aircraft and its associated elements, including ground control and communications equipment.

[8] "On-demand mobility" (ODM) is an emerging concept for commercial aviation that would feature small aircraft providing on-demand transportation for individuals or small groups of passengers within urban areas, over relatively short intercity distances, and in some cases over longer distances for transportation to or from small and underserved airports. (Although some ODM concepts focus on ground transportation, this report refers to ODM exclusively in terms of aviation.)

[9] Data fusion involves correlation and synthesis of data from heterogeneous data sources with different formats, timing, accuracy, and other characteristics.

[10] In the aviation community, the term "operator" is used to refer both to individual human operators (e.g., pilots and air traffic controllers) or to the organizations that operate aircraft (e.g., airlines and government agencies). This report follows the same convention. Each time "operator" appears in the report, the specific meaning should be clear based on the context.

- *Mitigation and Implementation*. The ability to mitigate elevated risk states on a much faster time scale than existing safety management systems is limited. As aviation system complexity increases, so does the risk of unintended consequences due to system actions and recommendations. Success requires that human operators trust system outputs, which include alerts, decision support, and independent actions. Accepted approaches for verification, validation, and certification of real-time system solution sets are lacking.

OVERARCHING VISION COMMENTARY

Decades of continuous efforts to address known hazards in the NAS and to respond to issues illuminated by analysis of incidents and accidents have made airlines the safest mode of transportation. The task of maintaining a high level of safety for commercial airlines and other operators is complicated by the dynamic nature of the NAS.[11] The number of flights by commercial transports is increasing, air traffic control systems and procedures are being modernized to increase the capacity and efficiency of the NAS, increasingly autonomous systems[12] are being developed for aircraft and ground systems, and small aircraft—most notably UAS—are becoming much more prevalent. As the NAS evolves to accommodate these changes, aviation safety programs will also need to evolve to ensure that changes to the NAS do not inadvertently introduce new risks. In this context, the vision that NASA holds for an RSSA system is well founded.

A potentially confusing facet of NASA's RSSA research lies in the descriptor "real time." A common understanding of "real time" is that it describes events that occur at the same time or nearly so. Some elements of an RSSA system would indeed occur in real time, just as the Traffic Collision Avoidance System (TCAS) operates in real time to continuously monitor an aircraft's position and velocity vector relative to the terrain and to other aircraft to immediately alert pilots when the risk of a collision exceeds a programmed threshold. Other elements of an RSSA system, however, could operate over a period of minutes, hours, or even days to look at operational trends over these time scales to identify risks that cannot be identified in real time.

Additionally, a safety assurance system, as defined by the International Civil Aviation Organization (ICAO), "consists of processes and activities undertaken by the service provider to determine whether the safety management system (SMS) is operating according to expectation and requirements." An SMS is more comprehensive in that it uses "a systematic approach to managing safety including the necessary organization structures, accountabilities and policies and procedures." To successfully achieve NASA's vision, the latter will be required.

The committee's vision of an *in-time* aviation safety management system appears in Box S.1. This description does not specify the use of any particular programmatic approach for achieving the vision. Chapter 5, however, notes that an approach with interim deliverables would facilitate development of a consensus in the aviation community to support IASMS research. The approach envisioned by NASA for development of an RSSA is structured to provide such deliverables.

The committee's vision for an IASMS is summarized in the following recommendation:

Recommendation. *In-time Aviation Safety Management*. The concept of real-time system-wide safety assurance should be approached in terms of an in-time aviation safety management system (IASMS) that continuously monitors the national airspace system, assesses the data that it has collected, and then either recommends or initiates safety assurance actions as necessary. Some elements of such a system would function in real time or close to real time, while other elements would search for risks by examining trends over a time frame of hours, days, or even longer.

[11] In this report, "commercial transports" refers to aircraft operated by regional and major passenger airlines as well as cargo airlines.

[12] Increasingly, autonomous systems lie along the spectrum of system capabilities that begin with the abilities of current automatic systems, such as autopilots and remotely piloted (nonautonomous) unmanned aircraft, and progress toward highly sophisticated systems that would enable, for example, UAS that could operate independently within civil airspace, interacting with air traffic controllers and other pilots just as if a human pilot were on board and in command (National Research Council, 2014, *Autonomy Research for Civil Aviation: Toward a New Era of Flight*, The National Academies Press, Washington, D.C.)

BOX S.1
Vision of an In-time Aviation Safety Management System

1. An IASMS will continuously monitor the NAS to collect data on the status of aircraft, air traffic management (ATM) systems, airports, weather, and so on, and then assess that data, as follows:

   a. Assess data on a second-by-second, minute-by-minute, and hour-by-hour basis to detect or predict elevated risk states based on rapid changes in system status. (Different elements of a safety assurance system will operate on different time scales.) Data of interest include the status and performance of vehicle systems, ground systems, operators, and weather. However, the system would not be designed to predict or respond to emergencies caused by catastrophic equipment failures, such as an uncontained engine failure or a landing gear collapse.
   b. Assess data over periods of days to detect risks based on longer-term trends.
   c. Detect and predict elevated risk states that arise from a confluence of factors, none of which by itself would be noteworthy.
   d. Assess data in the context of a thorough understanding of (1) the nominal performance of systems and operators, (2) historical data regarding both the occurrence and consequences of off-nominal situations, and (3) the fault tolerance of the NAS and its key elements.
   e. Assess system outputs over long periods of time to identify emergent risks that in some cases should be added to the list of risks that the system is designed to check for.

2. An IASMS will be focused on risks that require safety assurance action in-flight or prior to flight. Preflight safety assurance action may include a decision to postpone or cancel a flight until, for example, flight conditions change or equipment is repaired. An IASMS will not be designed to recommend safety assurance actions that would occur over a period of weeks, months, or longer, such as changes to pilot training programs, operational procedures, equipment design, or the content of scheduled maintenance checks. The output of an IASMS, however, may be useful to those who are responsible for these longer-term areas of interest.
3. Safety assurance actions generated by an IASMS may take the form of recommendations that operators take action. In some cases when urgent action is required, IASMS may be designed to initiate safety assurance actions on their own.

HIGH-PRIORITY RESEARCH TOPICS

In order for an IASMS to properly function in accordance with the intended vision, research is required in each of the four system elements described above: CONOPS and risk prioritization, system monitoring, system analytics, and mitigation and implementation. For each element, existing technologies and analytical capabilities cannot handle, in-time, the vast amount of data and information needed by an IASMS.

Research priorities are identified based on the understood difficulty of completing each item and the urgency with which they should be initiated so that the research output will be available in a manner that supports the intermediate milestones identified by NASA.

The committee identified 10 high-priority research projects that it recommends for consideration by agencies and organizations in government, industry, and academia with an interest in developing an IASMS for the NAS. All 10 are judged to be both difficult and urgent; if they were not, they would not have been designated as a high priority. As indicated in the following, two of the high-priority research projects address an IASMS concept of operations and risk prioritization, two address data collection for system observation, three address system analytics, and three address mitigation and implementation.

For most of the research projects, meeting the needs of an IASMS will likely require a mix of new technologies, improvements to existing technologies, and the adaptation of existing technologies developed for other applications. Each research project, as applicable, will need to determine the appropriate mix for that project.

The research project IASMS Concept of Operations and National Airspace System Evolution is judged to be of the highest priority (see Chapter 6). The report does not otherwise address the relative priority of the high-priority research projects, because execution of most of the projects is most likely to be successful if they proceed in an iterative and integrated fashion that accounts for the many interactions among the different projects in Chapters 2 to 5.

IASMS CONCEPT OF OPERATIONS AND RISK PRIORITIZATION

IASMS Concept of Operations and National Airspace System Evolution

This research project would develop a detailed concept of operations for an IASMS using a process that considers multiple possible system architectures, evaluates key trade-offs, and identifies system requirements. This would (1) establish the framework upon which all other IASMS research is conducted, (2) identify the near-term potential of IASMS research to enhance the safety of the NAS and to engender stakeholder support for and trust in an IASMS, and (3) facilitate updates to the CONOPS as the NAS evolves.

Developing a detailed CONOPS will be extremely difficult and time consuming because an IASMS will be a complex and dynamic system of systems and because of the many factors to be considered and the difficulty of assessing the trade-offs and interactions among them. This research is urgent because of the complexity of achieving IASMS goals and because it will establish the framework upon which all other research projects flow. Developing a detailed IASMS CONOPS will also define timelines for infrastructure investment strategies that would most efficiently support development of an IASMS.

Identifying and Prioritizing Risks

This research project would develop processes to identify and prioritize risks that are relevant to an IASMS and that threaten the safety of the current and evolving NAS. This would lead to approaches for identifying emerging risks and for prioritizing known and emerging risks that fall within the scope of the IASMS CONOPS.

The traditional approach to risk assessment is based on an evaluation of the probability of occurrence and the consequence of an event. The highest risks occur when the consequences of an event are the most severe and the probability of it occurring is the highest over some period of time. An ongoing process of identifying and prioritizing risks that an IASMS will address is important because additional risks will emerge. These new risks will arise due to changes in operations in the NAS, technological advances, increased connectivity, the implementation of next-generation airspace procedures such as delegation of separation, and other exogenous and internal threats. Also, as the safety of various elements of the NAS improves and as the probability threshold for a risk to be mitigated lowers, the number of elevated risk states that should be considered for mitigation will increase. Because any mitigation approach will introduce some cost into the system, risk prioritization is needed to facilitate development of an affordable IASMS.

This research project will be difficult to complete largely because of the uncertainties associated with identifying emerging risks. This research is urgent because it is essential to the development of an IASMS CONOPS scope.

SYSTEM MONITORING

Data Fusion, Completeness, and Quality

This research project would develop methods to automatically collect, fuse, store, and retrieve data from different sources and with different formats, timing, accuracy, and other characteristics. The range of IASMS capabilities that can be successfully implemented will be limited by the completeness of the data available, by its quality and

consistency, by the ability to fuse it in the time scales of interest, by the ability to store it for future use, and by the relative cost and value of obtaining additional or higher-quality data sources as required.

This research will be difficult to achieve given the substantial advances that are needed to develop the ability to define, acquire, understand, fuse, and store the data required to support planned IASMS capabilities. This project is urgent because it is fundamental to the success of an IASMS risk identification and prioritization process and because some components will likely take years to complete.

Protecting Personally Identifiable Information

This research project would develop methods of de-identifying and/or protecting sensitive data in a way that does not preclude effective data fusion. This would help achieve the vision for an IASMS by developing systems that will permit the automated fusing of large data sets without compromising the identification of the operator. For information to be used for in-time monitoring and assessment and to be stored for future use, advances in technology (and changes to regulatory policy) are needed to address operators' concerns regarding unauthorized disclosure of identifiable data. To meet the needs of an IASMS, de-identification methods will need to operate quickly and without loss of key operational safety data.

This research will be difficult to complete because the source data will be generated from unique and sometimes proprietary systems. This research project is urgent because of the time that it will take to develop improved methods for de-identifying and protecting data and to then develop a broad consensus among stakeholders—including operational personnel, unions, and the leadership of airlines, other operators, the Federal Aviation Administration (FAA), and original equipment manufacturers—that these methods are adequate.

SYSTEM ANALYTICS

In-time Algorithms

This research project would develop robust and reliable algorithms that can assess large volumes of heterogeneous data of varying quality to simultaneously identify and predict elevated risk states of many different types and that are fast enough to meet in-time requirements.

This research project would be difficult to complete because of the growing complexity of the NAS and because of the large and growing number and variety of aircraft operating in the NAS, including new entrants. In addition, this research project faces significant uncertainties regarding the ability to acquire all of the data needed to monitor the NAS, to assess the system state, and to detect elevated risk states. This research project is urgent because in-time algorithms will form the core of the monitoring, detection, prediction, and mitigation tasks of the IASMS.

Emergent Risks

This research project would develop approaches for continually mining historical data for detecting previously unknown anomalies and their evolution, to characterize emergent risks, and to update the IASMS risk assessment algorithms.

As with the preceding In-time Algorithms research project, this research project will be difficult to complete because of the growing complexity of the NAS and because of the large and growing number and variety of aircraft operating in the NAS, including new entrants. This research is urgent because it will take a long time to develop the new classes of offline data-driven methods,[13] machine learning and data mining algorithms, and analysis and prediction techniques that will be needed for each functional element (monitor, assess, and mitigate) of the IASMS to address adequately the hazards posed by emergent risks.

[13] "Offline analysis" refers to analysis of stored data as opposed to online analysis of streamed data in real time or near-real time.

Computational Architectures

This research project would support the design of data repositories and computational architectures that support online detection of elevated risk states and offline analysis to detect and characterize emergent risks and to update the IASMS risk assessment algorithms. Existing computational architectures lack the ability to handle large volumes of heterogeneous data and dynamic analytics workflows to support in-time analysis.

This research project will be difficult to complete because research and development focused on other applications will not meet the unique needs of an IASMS in terms of scope; spatial and temporal complexities; the need for timely processing of large volumes of streaming and stored heterogeneous data with varying levels of quality and frequency; and the need to provide a reliable, fault tolerant, and secure system that degrades gracefully when adverse situations (e.g., regional power failures) and malicious threats are launched against the system. This research is urgent because data repositories and computational architectures will provide the backbone of the IASMS operational system and are therefore needed early in the IASMS research effort.

MITIGATION AND IMPLEMENTATION

In-time Mitigation Techniques

This research project would, for the high-priority risks that fall within the scope of the IASMS CONOPS, identify those risks for which adequate mitigation techniques do not currently exist and develop approaches and technologies necessary to implement timely mitigation.

This research project will be difficult to complete because of the need for new instrumentation, advanced analytic methods, and sophisticated prediction capabilities that take into account the increasing complexities and uncertainties in the evolving NAS, particularly with respect to new entrants. This research project is urgent because the success of an IASMS is dependent on near- and long-term mitigation schemes to maintain the safety and efficiency of the NAS and because of the long time it will take to achieve project goals.

Trust in IASMS Safety Assurance Actions

This research project would identify factors specific to human trust in IASMS safety assurance actions. IASMS will rely on systems that are growing in functionality and decision-making capabilities. Many factors, such as the frequency and complexity of operator interactions with the system, will need to be understood and addressed in order to foster operator trust in the system and to create the proper workload balance between the operator and a system so that the operator does not become overloaded. Change management processes will be critical when the system is deployed. The examination of the preceding factors, however, will need to occur at a much earlier stage than typical change management processes to assist in shaping the CONOPS, design, and implementation of an IASMS.

This research project will be difficult to complete because creating an IASMS that operators will trust, and therefore use, will require a thorough understanding of the potential capabilities, nuances, and emergent properties of IASMS. The research is urgent because operator trust is a relatively new field, and this research project therefore does not have a large body of work to use as a resource. In addition, the results of this research project will be most effective if they are available early enough in the IASMS development process in order to support the design and development of IASMS.

System Verification, Validation, and Certification

This research project would develop practical methods for verifying, validating, and certifying an IASMS. A system as complex as an IASMS, which can influence immediate operations, will need to be certified before it becomes operational. Although research in this area is already under way to support related applications, such as certification of a UAS traffic management (UTM) system and autonomous cars, existing research will not meet the

unique needs of an IASMS because an IASMS will be much more complex than a highly automated/autonomous aircraft, and it will need to monitor and assess the operational safety of all existing and new entrants that will be operating in the NAS, encompassing the existing air traffic management (ATM) systems as well as UTM systems.

This research project will be difficult to complete because development of certification standards for an IASMS will require a new approach to certification that promotes rapid and yet safe changes to the system. This research project is urgent because of the expected long lead time involved in creating viable verification, validation, and certification (VV&C) processes that can be standardized and applied to other ATM systems or to develop an alternate approach to VV&C.

ECONOMIC CHALLENGE

The report identifies 13 technical challenges that are addressed by the recommended high-priority research projects, discussed above. In addition, there is one economic challenge, as detailed below.

Operators' Costs and Benefits

Operators' perception of the cost-to-benefit ratio of an IASMS may be so high that it will impede its implementation. Some aviation safety programs, such as the Aviation Safety Action Program (ASAP), could be implemented without new equipage. Many of the future data sources needed for the successful adoption of a fully functional IASMS, however, will require new and sophisticated onboard equipment along with the adoption of ground infrastructure and data processing capability. Airline operations in the NAS are already extremely safe—and given the limited financial resources of airlines and other operators—the ability to adopt new and potentially costly investments in a new safety system such as an IASMS will not easily pass the traditional cost-to-benefit ratio for adoption. If that is the case, widespread use is unlikely to occur unless and until regulatory mandates are issued.

1

Introduction

Decades of continuous efforts to address known hazards in the national airspace system (NAS)[1] and to respond to issues illuminated by analysis of incidents and accidents have made commercial airlines the safest mode of transportation. The task of maintaining a high level of safety for commercial airlines is complicated by the dynamic nature of the NAS. The number of flights by commercial transports[2] is increasing; air traffic control systems and procedures are being modernized to increase the capacity and efficiency of the NAS; increasingly autonomous systems[3] are being developed for aircraft and ground systems, and small aircraft—most notably unmanned aircraft systems (UAS)[4]—are becoming much more prevalent. As the NAS evolves to accommodate these changes, aviation safety programs will also need to evolve to ensure that changes to the NAS do not inadvertently introduce new risks.

Maintaining the safety of the NAS as it evolves will require a wide range of safety systems and practices, many of which are already in place. This report focuses on an aviation safety system that could detect and mitigate high-priority safety issues as they emerge and before they become hazards. In particular, the report defines the challenges to establishing such a system and the high-priority research projects that should be implemented to expedite its development.

[1] The NAS is "the common network of U.S. airspace; air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information and services; rules, regulations, and procedures; technical information; and manpower and material." FAA, 2013, *Integration of Civil Unmanned Aircraft Systems [UAS] in the National Airspace System [NAS] Roadmap*, Washington, D.C., https://www.faa.gov/uas/media/uas_roadmap_2013.pdf. Some NAS facilities are jointly operated by the FAA and the Department of Defense. The NAS includes all aircraft operating in U.S. airspace, both foreign owned and domestic.

[2] In this report, "commercial transports" refers to aircraft operated by regional and major passenger airlines as well as cargo airlines.

[3] Increasingly, autonomous systems lie along the spectrum of system capabilities that begin with the abilities of current automatic systems, such as autopilots and remotely piloted (nonautonomous) unmanned aircraft, and progress toward highly sophisticated systems that would enable, for example, UAS that could operate independently within civil airspace, interacting with air traffic controllers and other pilots just as if a human pilot were on board and in command (National Research Council, 2014, *Autonomy Research for Civil Aviation: Toward a New Era of Flight*, The National Academies Press, Washington, D.C.).

[4] An "unmanned aircraft" is, as the name implies, an aircraft that has no onboard pilot. In this report unmanned aircraft are assumed to have no humans on board either as flight crew or as passengers. A UAS is an unmanned aircraft and its associated elements, including ground control and communications equipment.

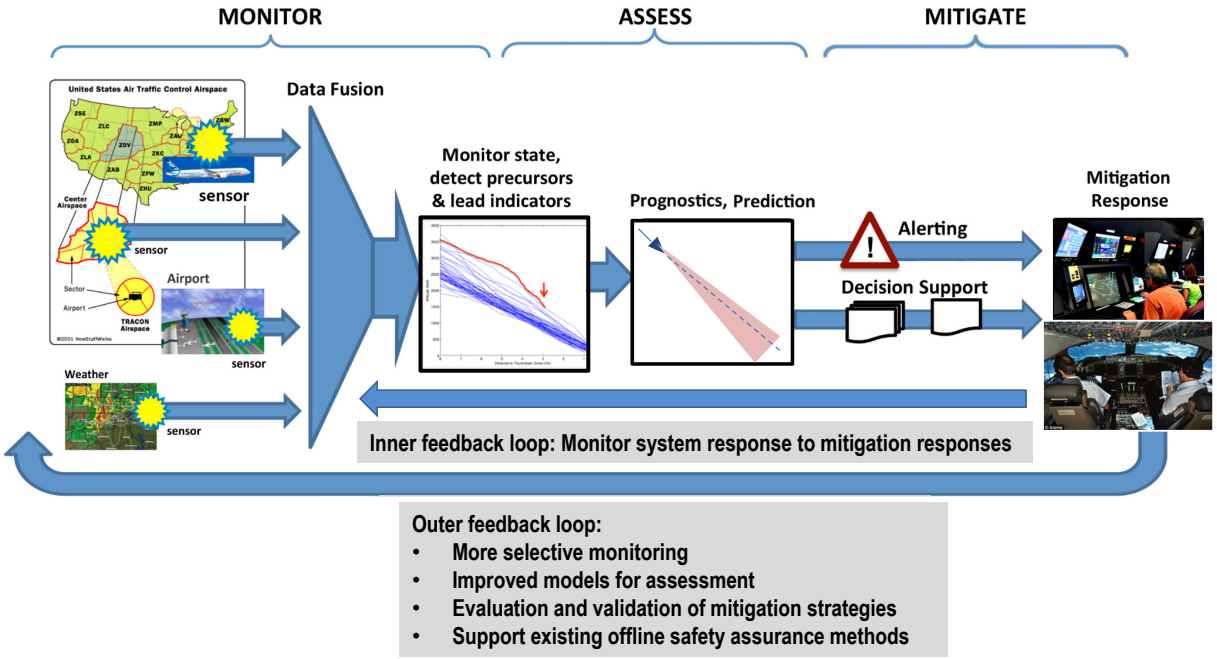

FIGURE 1.1 Simplified depiction of NASA's concept for a real-time system-wide safety assurance (RSSA) system. SOURCE: Briefing by J. Nowinski at the first meeting of the Aviation Safety Assurance Committee, January 23, 2016, Washington, D.C., p. 4 (modified).

A REAL-TIME AVIATION SAFETY ASSURANCE SYSTEM

Real-time system-wide safety assurance (RSSA) is one of six focus areas for NASA's aeronautics program. NASA envisions that an RSSA system (see Figure 1.1) would provide a continuum of information, analysis, and assessment that supports awareness and action to mitigate risks to safety. NASA's research plans state that development of an RSSA system will necessitate automating safety assurance of air transportation system components, integrating component-level systems, and reducing the safety assurance cycle time until real-time safety assurance is achieved at the system-of-systems level. The safety assurance system envisioned by NASA will combine air traffic and onboard aircraft technologies as well as air traffic system automated data mining capabilities into a system for continuous safety monitoring and threat prediction.[5] This system is expected to maintain or exceed the current level of air traffic safety[6] while accommodating global increases in air travel and rapid introduction of new technologies.[7] The system would not be expected to directly address issues related to design, development, training, or maintenance because the detection of problems in these areas and the process of implementing corrective actions falls outside the short time horizon of an RSSA. Other systems are already in place to address these aspects of aviation safety. The outer feedback loop in Figure 1.1 would allow for integrated development over time as the system guides the development of improvements in the capabilities for monitoring, assessing, and mitigating safety risks.

[5] NASA, 2015, *NASA Technology Roadmaps TA 15: Aeronautics*, NASA, Washington, D.C., https://www.nasa.gov/sites/default/files/atoms/files/2015_nasa_technology_roadmaps_ta_15_aeronautics_final.pdf.

[6] Throughout this report, "air traffic safety" generally refers to the safety of aircraft both in the air and on the ground.

[7] NASA, 2015, *NASA Technology Roadmaps TA 15: Aeronautics*.

NASA envisions that the process of developing a comprehensive and fully functional RSSA system would include three intermediate milestones:[8]

- *Domain-Specific[9] (Real-time) Safety Monitoring and Alerting Tools (2015-2025).* Expanded system awareness through increased access to safety-relevant data and initial integration of analysis capabilities; improved safety through initial real-time detection and alerting of hazards at the domain level and decision support for limited, simple operations.[10]
- *Integrated Predictive Technologies with Domain-Level Application (2025-2035).* NAS-wide availability of more fully integrated real-time detection and alerting for enhanced risk assessment and support of initial assured human and machine decision support for mitigation response selection for more complex operations.
- *Adaptive Real-time Safety Threat Management (2035-2045).* Fully integrated threat detection and assessment that support trusted methods for dynamic, multi-agent planning, evaluation, and execution of real-time risk mitigating response to hazardous events.[11]

These milestones provide a reasonable estimate of the long time that it would take to develop a fully functional RSSA.

IN-TIME AVIATION SAFETY MANAGEMENT SYSTEM (IASMS)

One potentially confusing facet of NASA's RSSA research lies in the descriptor "real-time." A common understanding of real time is that it describes events that occur at the same time or nearly so. For example, the operator of a remotely piloted vehicle is controlling the aircraft in real time, and if the aircraft is equipped with a camera and video link, the operator can monitor the area around the aircraft in real time. Some elements of an RSSA system would occur in real time, just as the Traffic Collision Avoidance System (TCAS) operates in real time to continuously monitor an aircraft's position and velocity vector relative to the terrain and to other aircraft to immediately alert pilots when the risk of a collision exceeds a programmed threshold. Other elements of an RSSA system, however, could operate over a period of minutes, hours, or even days to look at operational trends over these time scales to identify risks that cannot be identified in real time. This report therefore refers primarily to an IASMS instead of an RSSA to avoid potential misunderstandings regarding the temporal scope of the safety system addressed herein.

The Federal Aviation Administration (FAA) already requires that U.S. commercial airlines develop and implement a safety management system (SMS) (see Box 1.1), which will address operational safety risks associated with air travel. The FAA's SMS requirements do not specify a time frame over which those risks arise, are identified, and are mitigated. An IASMS, on the other hand, would continuously monitor the NAS to rapidly assess and mitigate safety risks.

The committee's vision for an IASMS is as follows:

1. An IASMS will continuously monitor the NAS to collect data on the status of aircraft, air traffic management (ATM) systems, airports, weather, and so on, and then assess that data, as follows:

[8] Briefing by J. Nowinski at the first meeting of the Aviation Safety Assurance Committee, January 23, 2016, Washington, D.C., p. 6.

[9] One example of a "domain-specific tool" would be a tool that monitors the NAS and determines the system state as it applies to a specific class of aircraft operating in the airspace near a specific airport. After such a tool is demonstrated and validated at that airport, continued development could expand its applicability to other classes of aircraft and other airports.

[10] In the context of this milestone, "limited, simple operations" are intended by NASA to refer to, for example, tools with limited automated decision-making and mitigation capabilities that could be demonstrated and validated in low-risk operations, such as those involving small UAS operating in unpopulated areas.

[11] In the context of this milestone, "hazardous events" also refers to hazardous trends and conditions.

BOX 1.1
Safety Management Systems

In 2015 the Federal Aviation Administration (FAA) directed commercial airlines to develop a fully functional safety management system (SMS) and to have that plan approved by the FAA no later than March 2018.[a] These systems will provide a formal, structured management approach to control operational safety risks. The use of SMS can be generally interpreted as applying a quality management approach to control safety risks. Similar to other management functions, safety management requires planning, organizing, communicating and providing direction. To be effective, each organization's approach to safety management should take into account the distribution of responsibilities as well as its operational safety processes.[b]

The FAA requires that the SMS being established by airlines include four elements:

- A safety policy that defines the general principles upon which the SMS will be built and operated and defines a strategy for achieving acceptable levels of safety within the organization;
- Safety risk management that identifies and analyzes risks;
- Safety assurance using data-driven evaluation methods to control risks; and
- Safety promotion that incorporates training of and communication with staff.

Safety planning and the implementation of safety management procedures are key steps in defining the processes that will be used to mitigate and contain operational safety risks. Once these controls are ready, quality management techniques can be utilized to ensure that they achieve the intended objectives and, where they fail, to improve them. This is accomplished by deployment of safety assurance and evaluation processes that in turn provide for a continuous monitoring of operations and for identifying areas of safety improvement.[c]

Effective safety management systems use risk and quality management methods to achieve their safety goals and to enable continuous improvement in the effectiveness of SMS. An IASMS would complement rather than duplicate the functions of an SMS.

[a] FAA, 2015, *FAA Advisory Circular 120-92B, 120-92B: Safety Management Systems for Aviation Service Providers*, Washington, D.C., https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1026670.

[b] SKYbrary, 2017, "Safety Management," last modified September 22, 2017, https://www.skybrary.aero/index.php/Safety_Management.

[c] SKYbrary, 2017, "Safety Management System," last modified September 22, 2017, https://www.skybrary.aero/index.php/Safety_Management_System.

a. Assess data on a second-by-second, minute-by-minute, and hour-by-hour basis to detect or predict elevated risk states based on rapid changes in system status. (Different elements of a safety assurance system will operate on different time scales.) Data of interest include the status and performance of vehicle systems, ground systems, operators, and weather. However, the system would not be designed to predict or respond to emergencies caused by catastrophic equipment failures, such as an uncontained engine failure or a landing gear collapse.
b. Assess data over periods of days to detect risks based on longer-term trends.[12]
c. Detect and predict elevated risk states that arise from a confluence of factors, none of which by itself would be noteworthy.

[12] The limited time horizon of an IASMS will allow it to complement rather than duplicate the efforts of other aviation safety systems such as those addressed in the Safety Data section that follows.

d. Assess data in the context of a thorough understanding of (1) the nominal performance of systems and operators, (2) historical data regarding both the occurrence and consequences of off-nominal situations, and (3) the fault tolerance of the NAS and its key elements.
e. Assess system outputs over long periods of time to identify emergent risks that in some cases should be added to the list of risks that the system is designed to check for.

2. An IASMS will be focused on risks that require safety assurance action in-flight or prior to flight. Preflight safety assurance action may include a decision to postpone or cancel a flight until, for example, flight conditions change or equipment is repaired. An IASMS will not be designed to recommend safety assurance actions that would occur over a period of weeks, months, or longer, such as changes to pilot training programs, operational procedures, equipment design, or the content of scheduled maintenance checks.[13] The output of an IASMS, however, may be useful to those who are responsible for these longer-term areas of interest.
3. Safety assurance actions generated by an IASMS may take the form of recommendations that operators take action. In some cases when urgent action is required, IASMS may be designed to initiate safety assurance actions on their own.

The preceding description of the committee's vision does not specify the use of any particular programmatic approach for achieving the vision. Chapter 5, however, notes that an approach with interim deliverables would facilitate development of a consensus in the aviation community to support IASMS research. The approach envisioned by NASA for development of an RSSA is structured to provide such deliverables.

The NAS includes many different classes of airspace, each of which has specific requirements for various types of aircraft and operations. Flight operations in most airspace must take place under the direction of air traffic controllers. Accordingly, the FAA's automation and surveillance capabilities are focused on controlled airspace rather than uncontrolled airspace, which predominantly exists at very low altitudes (less than 400 ft). As noted in Chapter 2, the UAS traffic management (UTM) system is being developed to facilitate operations of UAS. It remains to be seen how a future UTM system will be designed, operated, and integrated into the existing ATM system. It also remains to be seen what aircraft types and what types of operations in different classes of airspace will be encompassed by an IASMS; that will be determined as the concept of operations (CONOPS) for an IASMS is developed (see Chapter 2).

Figure 1.1 is consistent with this report's vision for an IASMS, although the outer feedback loop would have the additional task of identifying emergent risks. As with a conventional safety SMS, the tasks in the outer feedback loop would operate on long time scales of months or longer. For example, it will take some time to develop, validate, and incorporate improved models into an IASMS.

SAFETY DATA

The NAS includes a wide variety of aircraft, including commercial transports, general aviation aircraft, rotorcraft, military aircraft, and UAS. While the aviation community strives to ensure the safety of all aircraft operations, there is a particular emphasis on commercial airlines given that the number of flights by commercial transports—and the number of passengers and flight crew aboard those flights—far exceeds those for all other types of aircraft.[14] The impressive safety of U.S. commercial airlines is due in part to the fact that the aviation industry and federal government are voluntarily investing in the right safety enhancements to reduce the fatality risk of travel by commercial airlines in the United States. There is a long-standing safety culture in aviation that is currently supplemented

[13] Although scheduled maintenance checks would be outside the temporal scope of an IASMS, it could recommend conducting maintenance on a particular aircraft system prior to the aircraft departing on its next flight or during flight (e.g., by recommending a system reset).

[14] Although the number of UAS flight operations will exceed the number of commercial transport operations in the foreseeable future, aviation safety in terms of human safety will continue to be centered on commercial transport operations for the indefinite future. Nevertheless, as discussed in Chapter 2 the scope of an IASMS will include both general aviation aircraft and UAS.

by industry working together in the Commercial Aviation Safety Team (CAST), which describes its history and operations as follows:[15]

> Two government reports on aviation safety provided the framework for the formation of CAST. The White House Commission on Aviation Safety and Security report released in February 1997 challenged the government and industry to reduce the accident rate 80 percent over ten years. The National Civil Aviation Review Commission report followed up in December 1997 with a recommendation that the FAA and industry work together to develop a comprehensive integrated safety plan to implement many existing safety recommendations and develop performance measures and milestones to assess progress in meeting safety goals. The Commission also recognized that the global nature of aviation demanded that aviation safety needed to be addressed worldwide, not just in the United States. The FAA and the industry determined that their safety advocacy work was complementary and CAST was formed in 1998.[16]

CAST was established with two goals: to reduce the U.S. commercial airline fatal accident rate by 80 percent over a 10-year period ending in 2007, and to work with airlines and international aviation organizations to reduce the worldwide commercial airline fatal accident rate.

The work of CAST, along with new aircraft, regulations, and other activities, reduced the fatality risk per million departures for commercial airlines in the United States by 83 percent from 1998 to 2008.[17]

CAST has evolved, and the group is moving beyond the historic approach of examining past accident data toward a more proactive approach focusing on detecting risk and implementing mitigation strategies before accidents or serious incidents occur. It aims to transition to prognostic safety analysis, and to reduce U.S. commercial fatality risk by a further 50 percent from 2010 to 2025. The increasing number of flights requires greater emphasis on acquiring, sharing, and analyzing aviation safety data. Using incident data, CAST is examining emerging and changing risks to identify prevention strategies.

Given that there are so few commercial airline accidents—and few common causes for those that do occur—more data points are needed. Voluntary reporting programs, such as the Aviation Safety Action Program (ASAP) and the Flight Operations Quality Assurance (FOQA) program, give airlines and government insight into millions of operations so that potential safety issues and trends can be identified. The Aviation Safety Information Analysis and Sharing (ASIAS) program ties together the safety databases across the industry and is integrated into the CAST process. ASAP, FOQA, and ASIAS all feature nonpunitive reporting so that operators (both individuals and organizations) can provide frank and complete data without concern that the FAA will take action against operators based on the data (see Chapter 3). These programs have matured to the point that the FAA can now look at data from air carriers representing over 80 percent of U.S. commercial airline operations to search for emerging risks. The FAA has increased the number of databases ASIAS can access; expanded ASIAS to include maintenance/air traffic information; increased membership by adding regional air carriers; and increased community stakeholders to include operators[18] of general aviation and military aircraft, including helicopters.[19]

ASIAS resources include both public and nonpublic aviation data. Public data sources include, but are not limited to, ATM data related to traffic, weather, and procedures. Nonpublic sources include de-identified data from air traffic controllers and aircraft operators, including digital flight data and safety reports submitted by flight crews and maintenance personnel. ASIAS has the ability to query millions of flight data records and de-identified textual reports to facilitate directed studies, assessments of safety enhancements, monitoring of known risks, and

[15] Commercial Aviation Safety Team (CAST), "Fact Sheet, Commercial Aviation Safety Team," December 2011, http://www.cast-safety.org/pdf/cast1201.pdf.

[16] CAST, 2011, "Background," http://www.cast-safety.org/apex/f?p=180:1:27980477329992::NO::P1_X:background.

[17] SKYbrary, 2017, "Commercial Aviation Safety Team (CAST)," last modified February 6, 2017, https://www.skybrary.aero/index.php/Commercial_Aviation_Safety_Team_(CAST).

[18] In the aviation community, the term "operator" is used to refer both to individual human operators (e.g., pilots and air traffic controllers) and to the organizations that operate aircraft (e.g., airlines and government agencies). This report follows the same convention. Each time "operator" appears in the report, the specific meaning should be clear based on the context.

[19] FAA, 2016, "Fact Sheet—Commercial Aviation Safety Team," April 12, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=18178.

discovery of emergent risks. ASIAS has also established key safety benchmarks so that individual operators may compare their own safety performance against the industry as a whole.[20]

CAST uses ASIAS information by chartering working groups for in-depth analysis of precursors to the top accident categories in commercial transports. Safety enhancements are then identified to reduce such accidents and to prioritize and coordinate plans for implementing and, finally, monitoring actual effectiveness. Although most participants are from the United States, CAST promotes new safety initiatives by government and industry globally. Accident rates and causes vary by region and do not lend themselves to replicated solutions. With that in mind, CAST coordinates with the International Civil Aviation Organization (ICAO), the Flight Safety Foundation, the International Air Transport Association, the European Aviation Safety Authority, Transport Canada Civil Aviation, and other organizations, many of which have adopted CAST safety enhancements that are appropriate for different regions of the world or at a global scale.[21]

The General Aviation Joint Steering Committee is an industry-government organization dedicated to improve safety in general aviation, which lags far behind the safety of commercial transports.[22] The steering committee has partnered with CAST and is coordinating the implementation of certain CAST Safety Enhancements in general aviation. In addition to that, several members of the steering committee such as FOQA and ASAP have joined ASIAS and are contributing voluntary safety information. As of July 2017, ASIAS had 56 general aviation operators contributing safety information.

CAST and the aviation safety systems described above operate over relatively long time frames. It typically takes months for data collection systems such as ASIAS and FOQA to accumulate and disseminate data to airlines and regulators, and it takes more months or years for these data to be assessed, for issues to be identified, for solutions to those issues to be developed, and for those solutions to be promulgated as new or modified procedures, practices, and regulations. An aviation safety assurance system, such as an IASMS, that operates over a much shorter time frame would complement these existing systems to provide a more comprehensive approach to maintaining and improving aviation safety.

PRIORITIZATION PROCESS

This report identifies 14 key challenges that will be the most difficult to overcome in developing and demonstrating advanced technologies and capabilities to achieve the committee's vision for an IASMS. The discussion of each challenge begins with a summary statement that is followed by a summary of the reasoning for identifying that area as a key challenge. All but one of the challenges focus on technology issues; that one addresses economic issues (see Chapter 5).

The report also identifies 10 high-priority technology research projects that should be included in a national effort to support the development of an IASMS.[23] The selection of the projects was based on the committee's consensus of the difficulty of completing each project and the urgency with which the research project should be

[20] U.S. Government Accountability Office (GAO), 2015, *Aviation Safety: Proposals to Enhance Aircraft Tracking and Flight Data Recovery May Aid Accident Investigation, but Challenges Remain*, GAO-15-443, Washington, D.C., http://www.gao.gov/assets/670/669754.pdf.

[21] CAST, 2011, "Fact Sheet, Commercial Aviation Safety Team," December, http://www.cast-safety.org/pdf/cast1201.pdf.

[22] There were 219 fatal general aviation accidents in the United States with 347 fatalities in 2016, resulting in 8.4 fatal accidents per million operating hours. By comparison, from 2010 to 2014, inclusive, there were 11 fatalities caused by accidents by U.S. commercial airlines, resulting in 0.1 fatalities per million operating hours. FAA, 2017, "Fact Sheet—General Aviation Safety," October 24, https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=21274; U.S. Department of Transportation, Bureau of Transportation Statistics, 2016, "U.S. Air Carrier Safety Data," Table 2-9 in *National Transportation Statistics 2016*, https://www.bts.gov/sites/bts.dot.gov/files/legacy/NTS_Entire_2017Q1.pdf.

[23] All of the high-priority research projects address technology issues. The scope of the study does not include identifying research projects that are focused, for example, on policy or economics. Nonetheless, in some cases the results of the technology research projects will be useful for those who have the responsibility for addressing policy and economics.

initiated so that its results will be available in a timely fashion.[24] These two criteria (difficulty and urgency) reflect several associated considerations:

- The extent to which the current state of the art must be advanced;
- The time and resources needed to make those advances; and
- The time-phased application of research project results to the overall scheme of developing and deploying ever-more-capable IASMS.

The committee has grouped the challenges and research projects into one of four areas, each of which is discussed in one of the next four chapters:

- Chapter 2: IASMS Concept of Operations and Risk Prioritization
- Chapter 3: System Monitoring
- Chapter 4: System Analytics
- Chapter 5: Mitigation and Implementation

Chapter 6 completes the report by presenting the committee's findings and recommendations that summarize the 14 key challenges and 10 high-priority research projects. Chapter 6 also addresses organizational roles and resources.

All of the high-priority research projects are judged to be both difficult and urgent; if they were not, they would not have been designated as a high priority. For most of the research projects, meeting the needs of an IASMS will likely require a mix of new technologies, improvements to existing technologies, and/or the adaptation of existing technologies developed for other applications. Each research project, as applicable, will need to determine the appropriate mix for that project.

The success of the research projects is hindered by the many unknowns regarding the scope of the IASMS. For example, requirements for the nature and quality of the IASMS data are still unknown, the policies and mechanisms for collecting IASMS data have not yet been determined, and the stakes involved in the performance of an IASMS are tremendously higher (because lives are at stake) than with most other applications. The output of the research projects in Chapter 2 will assist greatly in reducing uncertainties faced by the other research projects. Each research project, as applicable, will need to determine the appropriate mix of technologies: new, improved, and adapted from other applications.

The research project, IASMS Concept of Operations and National Airspace System Evolution, is judged to be of the highest priority (see Chapter 6). The report does not otherwise address the relative priority of the high-priority research projects because execution of most of the projects is most likely to be successful if they proceed in an iterative and integrated fashion that accounts for the many interactions among the different projects in Chapters 2 to 5. An iterative, integrated approach would also (1) allow advances in one area to support advances in other areas, (2) enable each research project to benefit as more detailed information becomes available, and (3) improve the quality of the complex trade-offs that will help guide the goals of each research project.

[24] The prioritization process described here is modeled after the prioritization process described in the first study in this series, each of which addresses the subject of one of the six strategic thrusts established by NASA's Aeronautics Research Mission Directorate. That first report focused on assured autonomy for aviation transformation and is titled *Autonomy Research for Civil Aviation: Toward a New Era of Flight* (National Research Council, 2014, The National Academies Press, Washington, D.C.).

2

IASMS Concept of Operations and Risk Prioritization

A clear CONOPS for an IASMS is needed to understand how the system will operate, to define the issues that an IASMS will address, and to identify key technical and policy issues. Trying to develop an IASMS that can address a wide range of potential risks is problematic because each additional risk that is added to the scope of an IASMS increases both the cost of development and the complexity of the system. A process for prioritizing risks is therefore needed to limit the scope of an IASMS to potential risks that are most likely to occur and potentially have the most severe consequences if they do occur. A traditional prioritizing process can be used that relies on historic data from the operation of conventional aircraft. This approach, however, would not consider the potential impact of emerging risks associated with new entrants.[1] For example, new entrants will generate new issues such as a possible increase in the level of uncertainty in NAS operations, the possibility that operators will not demonstrate an appropriate level of trust in the increasingly autonomous systems; and the impact of unauthorized UAS operations and the increasing pace of commercial space operations on the safety and efficiency of the NAS.

This chapter identifies three key challenges and two high-priority research projects:

- Challenges
  - — IASMS Concept of Operations
  - — Identifying and Prioritizing Risks
  - — National Airspace System Evolution
- Research Projects
  - — IASMS Concept of Operations and National Airspace System Evolution
  - — Identifying and Prioritizing Risks

CHALLENGES

IASMS Concept of Operations

Challenge Summary Statement: A clear concept of operations (CONOPS) for an IASMS is needed to define the scope of such a system and to understand how it would work.

[1] This report identifies three classes of new entrants that are of particular interest to the development of an IASMS: unmanned aircraft systems (UAS), on-demand mobility (ODM) aircraft, and commercial space launches, all of which are discussed later in this chapter.

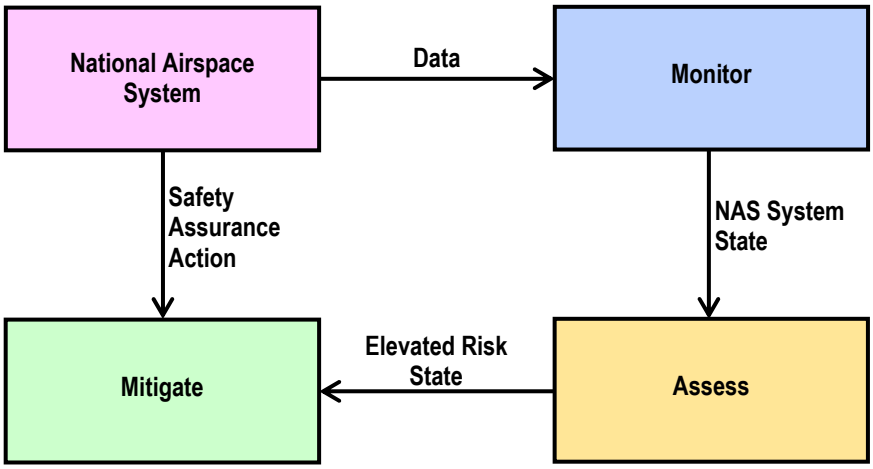

FIGURE 2.1 Functional elements and flow of information of a suggested high-level generic CONOPS for an IASMS.

Developing a detailed CONOPS for an IASMS will be a key challenge for four reasons. First, the CONOPS establishes the framework upon which all other research projects flow. Therefore, the development of the CONOPS is foundational to all other research. Second, by its nature, an IASMS is a complex and dynamic system of systems operating on varying time scales. As such, the CONOPS establishes a blueprint for system architecture and identifies interdependencies between operating subsystems. Third, the CONOPS defines the operational parameters inherent in IASMS including system authority, time constants, scope of risk, range of operations, and technological trade-offs. Last, an IASMS CONOPS will need to accommodate an evolving NAS that includes ongoing improvements to the NAS, new entrants that are already known—such as UAS, on-demand mobility (ODM),[2] and commercial space launch and reentry operations—as well as unforeseen new entrants and other issues.

The functional elements and flow of information of a suggested high-level generic IASMS CONOPS are shown in Figure 2.1. Conceptually, a monitoring system observes and characterizes the system state by collecting, fusing, and assessing data from a variety of sensors.[3] The system state is continuously assessed to identify hazards and characterize associated risks, thereby detecting elevated risk states. When an elevated risk state is detected or predicted, a mitigation process is triggered to implement a safety assurance action that reduces the identified risk level.

A number of issues and requirements are clear from the generic CONOPS. First, system effectiveness will depend greatly on the extent to which the monitor, assess, and mitigate functions are tailored to address specific risks or classes of risks. It is therefore necessary to establish a process to identify and prioritize those risks that merit a corresponding investment in an IASMS. It is also necessary to develop a much more detailed CONOPS to guide the development of an IASMS. Developing a detailed CONOPS will be complex and time consuming because of the difficulty of producing accurate, quantified projections of the state of the NAS, the availability of relevant data, the capabilities of computational systems, and so on; because of the many factors to be considered; and because of the difficulty of assessing the trade-offs and interactions among them. Key factors include the following:[4]

[2] ODM is an emerging concept for commercial aviation that would feature small aircraft providing on-demand transportation for individuals or small groups of passengers within urban areas, over relatively short intercity distances, and in some cases over longer distances for transportation to or from small and underserved airports. (Although some ODM concepts focus on ground transportation, this report refers to ODM exclusively in terms of aviation.)

[3] Data fusion involves correlation and synthesis of data from heterogeneous data sources with different formats, timing, accuracy, and other characteristics. See Chapter 3 for more information on data fusion.

[4] System scope is listed first because it is the most important of the factors in the list. The other factors are listed alphabetically.

- System scope in terms of:
  - — Aircraft types, including new entrants
  - — Data requirements
  - — Known and emergent risks
  - — Operations in different classes of airspace
  - — Time scales for each functional element (monitor, assess, and mitigate) of the generic CONOPS
  - — Users
- Ability to collect required data
- Architecture
- Costs and benefits
- Effectiveness
- Growth in air traffic
- Human performance limitations and human-machine roles
- NAS evolution
- System authority
- Technical capabilities
- Uncertainties associated with each functional element of the generic CONOPS
- Verification, validation, and certification (VV&C)

A concept of operations that encompasses all of the above factors would be very complex, perhaps approaching the complexity of the concept of operations of the NAS itself, given that the scope of IASMS will encompass a large portion of the NAS. In addition, it is likely that the functional elements of an IASMS will need to be tailored to some degree for different aircraft types, different risks, different operations in different classes of airspace, and so on, that fall within the scope of the system.

Identifying and Prioritizing Risks

Challenge Summary Statement: Because the universe of all potential risks is large and each risk addressed adds some cost and complexity to the system, it will be important to have an approach and process to prioritize and focus on those risks that will have the most impact on system safety issues that fall within the scope of the IASMS.

Identifying and prioritizing risks that an IASMS will address will be a key challenge because of the wide variety of potential risks, the difficulty of assessing many risks, and the extent to which an IASMS can mitigate those risks. As the safety of various elements of the NAS improves, and as the probability threshold for a risk to be mitigated lowers, the number of elevated risk states that should be considered for mitigation will increase. Because any mitigation approach will introduce some cost into the system, risk prioritization is needed to facilitate development of an affordable IASMS.

There are many factors to consider when prioritizing risks. These include traditional assessments of consequence and probability, as well as relevant hazards (Have the hazards that underlie risks of interest been identified and analyzed?[5]); detectability (Is the risk understood? Are the data available? Are there monitoring approaches to detect elevated risk states?); mitigation effectiveness (Are there viable options for reducing the risk levels?); cost; undesirable secondary effects (e.g., the introduction of new risks); and societal risks (see below).

The traditional approach to risk assessment is based on an evaluation of the probability of occurrence and the consequence of an event. This approach is illustrated by the sample risk assessment matrix in Figure 2.2. As shown, the highest risks occur when the consequences of an event are the most severe and the probability of the event occurring is the highest over some period of time. Risks posed by a given event are reduced as action is taken to reduce the consequences of the event and/or to reduce the probability that the event will take place. For example,

[5] FAA, 2012, *Safety Risk Management Policy*, FAA Order 8040.4, April 30, https://www.faa.gov/documentLibrary/media/Order/8040.4A%20.pdf.

RISK ASSESSMENT MATRIX					
		Severity			
		Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Probability	Frequent (A)	High	High	Serious	Medium
	Probable (B)	High	High	Serious	Medium
	Occasional (C)	High	Serious	Medium	Low
	Remote (D)	Serious	Medium	Medium	Low
	Improbable (E)	Medium	Medium	Medium	Low
	Eliminated (F)	Eliminated			

SEVERITY CATEGORIES		
Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental damage, or monetary loss equal to or exceeding $10 million.
Critical	2	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1 million but less than $10 million.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100,000 but less than $1 million.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100,000.

SEVERITY CATEGORIES			
Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item.	Continuously experienced.
Probable	B	Will occur several times in the life of an item.	Will occur frequently.
Occasional	C	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	D	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.

FIGURE 2.2 Sample risk assessment matrix, severity categories, and probability levels. SOURCE: U.S. Department of Defense, 2012, *Department of Defense Standard Practice: System Safety*, MIL-STD-882E, Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base, Ohio, http://www.system-safety.org/Documents/MIL-STD-882E.pdf, pp. 11-12.

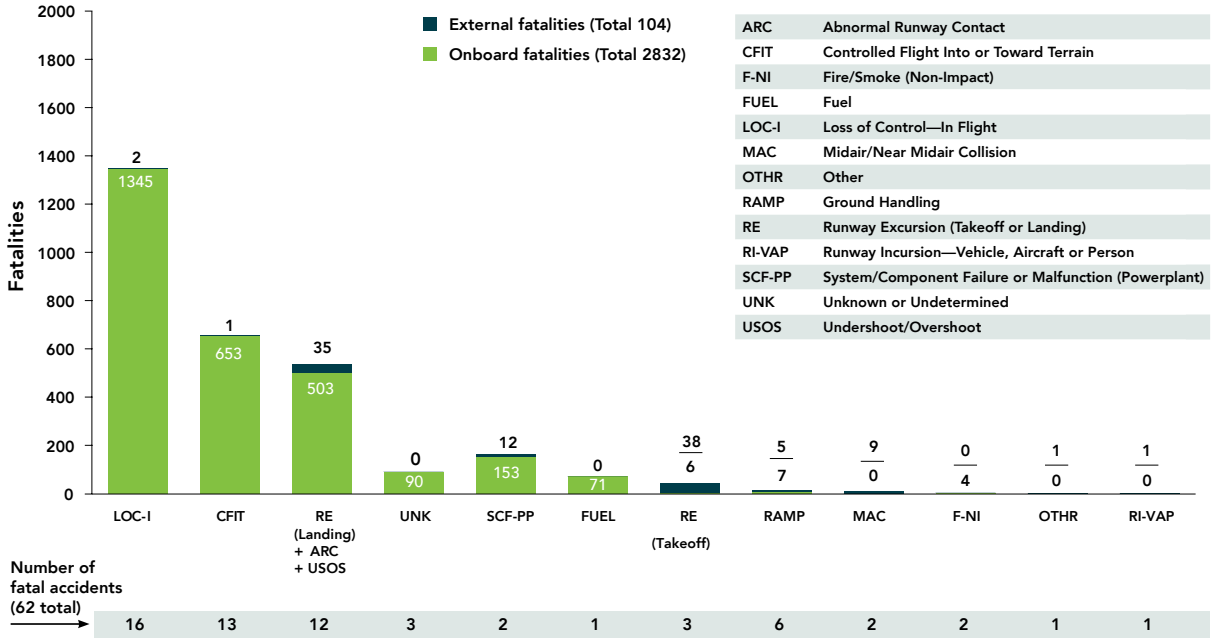

FIGURE 2.3 Fatalities associated with known risk areas, Worldwide Commercial Jet Fleet, 2007 through 2016. SOURCE: Boeing Corporation, 2017, *Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations, 1959-2016*, Boeing Commercial Airplanes, Seattle, Washington, http://www.boeing.com/resources/boeingdotcom/company/about_bca/pdf/statsum.pdf, p. 22. Copyright 2007 Boeing.

the risks posed by in-flight failures of gas turbine engines have been greatly reduced in recent decades by design improvements that have made engine failures exceedingly rare. The higher reliability of gas turbine engines has also reduced the consequences of an engine failure by reducing the likelihood that another engine will fail before an aircraft can make an emergency landing. Investigations of accidents and incidents and the methodologies used for those investigations can also contribute to risk assessments.

Several classes of risk are relevant to the process of identifying and prioritizing risks. These include the following:

- *Known Risks*. The highest-priority risks are known risks that are still present in the system, that have a relatively high probability of occurring, and that have the potential for the most severe consequences. In commercial transports this would include loss of control, controlled flight into terrain, and runway excursions, because they cause the most fatalities in commercial jet operations (see Figure 2.3).[6] These categories are all widely understood to be important risks to the safety of aviation, but there are specific manifestations of risk within each of these categories that have not been well characterized and for which preventive action is not yet fully effective. Each of these three risk areas is clearly a high priority, and they have been the focus of substantial aviation safety research for many years. Investigations of past incidents and accidents are also available to provide insight into known risks and to guide relevant research. It will be essential—and perhaps difficult—to show how an IASMS can help mitigate risks in these areas.

[6] Breaches in physical security have also caused many aviation fatalities, but physical security is generally addressed as a hazard apart from safety and aviation safety systems.

- *Emerging Risks*. As the NAS evolves, new risks will emerge due to changes in operations (e.g., UAS, ODM, and growth in air traffic), technological advances (e.g., increasingly autonomous systems), increased connectivity, the implementation of next-generation airspace procedures (e.g., delegation of separation), and other exogenous and internal threats (e.g., cyberattacks and instability of human operators).
- *Societal Risks*. In some cases, a risk may suddenly become a high priority due to societal concerns. This most commonly occurs after a high-profile accident with severe consequences that attracts public and legislative attention to a particular risk.[7]

Some risk factors are common to many of the risks described above. Hazardous weather, for example, contributes to many accidents that are classified as controlled flight into terrain, loss of control in-flight, or runway excursions. For conventional aircraft, hazardous weather is a known risk. For UAS, however, hazardous weather is an unknown risk because the safety risk of UAS operations in hazardous weather has yet to be quantified, especially with regard to small UAS used in new applications. The impact of hazardous weather on the safety of UAS is of particular concern for UAS operating in densely populated areas or in the vicinity of manned aircraft. Small UAS will tend to be more susceptible than larger aircraft to hazardous weather because of their light weight and because most UAS operators have less aviation experience and training than the pilots of manned aircraft.

In some cases, an emergent risk could mimic one or more known risks. A successful cyberattack, for example, could manifest itself as an accident associated with loss of control, runway excursion, or some other known risk area. Most NAS air and ground systems are not designed to operate during sophisticated cyberattacks. A common approach to securing these systems is to limit (or eliminate) connectivity to the outside world. There are still weaknesses, however, that could enable a successful cyberattack. For example, the Aircraft Communications Addressing and Reporting System (ACARS) provides key navigation data to on-board flight management systems, but the messages are not encrypted nor do they have authentication protocols. In addition, navigation, communication, and surveillance operations in the NAS are migrating to digital and network-based operations, and this may introduce new cyber vulnerabilities that are relevant to an IASMS. Accordingly, an IASMS will need to be designed with cybersecurity in mind. The only cybersecurity issues that fall within the scope of an IASMS research program, however, are those that are unique to the operation of an IASMS. For example, there is no need for an IASMS research program to develop more secure communications protocols or firewalls, because both of these areas apply to a wide array of applications and organizations, and tremendous resources are already devoted to research in these areas. Rather, issues of particular interest to an IASMS are detection and mitigation techniques for cyber threats that could bring down or compromise the integrity of NAS communications, navigation, and surveillance networks.

Likewise, an accident caused by human instability in which a pilot commits suicide by flying a passenger aircraft into the ground could be classified as a controlled flight into terrain accident. The corrective action for preventing such accidents, however, is far different than the corrective action to prevent unintended controlled flight into terrain accidents.[8] An advanced IASMS might be able to detect off-nominal physiological features associated with human instability in real time (see Chapter 3: "Collecting Data on the Performance of Human Operators" in the Challenges section and "Protecting Personally Identifiable Information" in the Research Projects section). If that is not possible, however, an effective IASMS would be able to detect and, if possible, take corrective action in response to adverse changes in the state of an aircraft or other elements of the NAS that are caused by human instability, other known or emergent safety risks, or attacks associated with a breach in physical security.

[7] For example, consider the history of the Traffic Collision Avoidance System (TCAS). The FAA began development of an airborne collision avoidance system in 1978 after a midair collision over San Diego with 144 fatalities. The FAA began to mandate the installation of collision avoidance systems in 1986 after a midair collision over Cerritos, California, with 82 fatalities. Many other countries began to mandate the installation of a collision avoidance system in 1996 after a midair collision over New Delhi with 351 fatalities. See Eurocontrol, "History and Future of Airborne Collision Avoidance," http://www.eurocontrol.int/articles/history-future-airborne-collision-avoidance, accessed December 8, 2017.

[8] Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, 2016, *Final Report: Accident on 24 March 2015 at Prads-Haute-Bléone (Alpes-de-Haute-Provence, France) to the Airbus A320-211 registered D-AIPX, operated by Germanwings*, March, https://www.bea.aero/uploads/tx_elydbrapports/BEA2015-0125.en-LR.pdf.

National Airspace System Evolution

Challenge Summary Statement: The capabilities of an IASMS will need to increase in sophistication as the NAS continues to evolve and improve, while also accommodating changes in conventional air traffic and new entrants, particularly with regard to the following:

- Growth in air traffic;
- Increased uncertainty from new entrants (e.g., UAS, on-demand mobility aircraft, and commercial space launch and reentry operations) and emergent risks;
- Trust in increasingly autonomous UAS and associated traffic management systems;
- Unauthorized UAS operations; and
- Increasing pace of commercial space operations.

Evolution of the NAS includes changes in both internal factors (e.g., aircraft, the ATM system, technologies, and operational procedures) and external factors (e.g., demographics, education, media, and cultural norms). Developing an IASMS that can accommodate the ongoing evolution of the NAS will be a key challenge because of technical difficulties in supporting the development of an increasingly complex IASMS. In addition, new capabilities implemented in the NAS, such as an upgraded IASMS, will be required to meet or exceed the extremely high levels of accuracy, reliability, speed, performance, and overall safety that current systems demonstrate and that the public expects, especially with respect to airlines. Also, growth in traditional air traffic and new entrants will create a need for an IASMS with more sophisticated capabilities related to data gathering, analysis, risk detection, and risk mitigation on the time scale of interest to an IASMS.

The NAS has evolved progressively from its rudimentary beginning in the 1920s. The system's initial focus was to deploy the best available navigation techniques to enhance efficiency, safety, accuracy, and reliability. As traffic increased, the system focused primarily on aircraft separation assurance to prevent collisions and enhance broad public acceptance of a safe and reliable air transportation network. Prior to World War II, the low density of air traffic permitted the use of procedural separation based on direction, time, and speed control. In the 1950s, however, the growth in traffic and available technology required the introduction of positive separation through the use of radar and real-time communication between pilots and air traffic controllers. As traffic density increased further and with the advent of commercial transports powered by jet engines in the late 1950s and early 1960s, the NAS was augmented with more capable radars, and defined airways or track systems were increasingly used to ensure safe separation between aircraft. NAS airspace classifications were also established to regulate operations within different regions, each of which is defined in terms of geography and altitude. Airspace classification schemes subsequently evolved to recognize and accommodate advances in the capabilities of aircraft and air traffic control systems. As growth in air traffic continued and technology evolved, satellite navigation systems were developed and deployed in the late 1980s and early 1990s, and GPS-based aircraft separation, using the Automatic Dependent Surveillance-Broadcast (ADS-B) system was deployed beginning in 2010.[9] Over the past 20 years, high-precision satellite-based systems have been replacing some ground-based navigation and radars.

The Next Generation Air Transportation System (NextGen) program was formulated in 2004 as a multiagency effort led by the FAA to modernize and improve the efficiency of the NAS over a period of approximately 25 years. NextGen is and will continue to be a major driver of improvements to the NAS. The NextGen program consists of a series of initiatives, which have included the System Wide Information Management (SWIM) program (see Chapter 3), ADS-B (see above), and trajectory-based operations (see Chapter 4).

As the NAS approaches 2020, satellite-based communication, navigation, and surveillance systems are expected to predominate as an increasing number of ground-based systems are phased out. Digital, lightweight satellite systems are much more precise and have greater capacity and, therefore, will be able to accommodate

[9] Automatic Dependent Surveillance-Broadcast (ADS-B) is a GPS satellite-based replacement for our current ground-based radar surveillance network. Like radar, the ADS-B sensor system provides a presentation of an aircraft's position, direction, and speed to an air traffic controller. Unlike radar, it can also provide this information to other aircraft equipped with an ADS-B system to enhance cockpit situational awareness, aircraft separation, and safety assurance.

an increase in traffic by both conventional aircraft and new entrants (see below). Most UAS will operate at lower altitudes than commercial transports, but some will operate in airspace shared with manned aircraft. A new traffic system referred to as UAS traffic management (UTM) will be needed to assure safe separation. Early versions of a UTM system are expected to be compatible with the ATM system. As the UTM system matures, it is expected to be interoperable with and ultimately to merge seamlessly with the existing NAS. This evolution will require preplanning of standards and technology to ensure forward compatibility and integration.

Each of the five areas listed in the preceding challenge summary statement is discussed in more detail in the following sections.

Growth in Air Traffic

Air travel provided by commercial airlines over the next 20 years is projected to increase by more than 60 percent in terms of revenue passenger miles. Over the same period air traffic in the NAS is projected to increase by 30 percent as measured by the number of aircraft handled at en route centers.[10] The discrepancy between growth in revenue passenger miles and en route flight operations arises from several factors:[11]

- The average size of aircraft used by airlines (especially regional airlines) is increasing.
- The average load factor is increasing (that is, the percentage of empty seats is decreasing).
- Air traffic by general aviation aircraft is growing more slowly than commercial transports.
- Air traffic by air taxi services is decreasing.

When looking at the next 20 years, however, the number of flight operations handled by en route centers will tell only part of the story. There will be a corresponding increase in the number of airport operations during takeoff, approach, landing, and on the ground. In addition, the FAA projects that the number of small UAS operated by hobbyists will increase by a factor of 3 in the next 5 years and the number of small UAS engaged in commercial operations will increase by a factor of 10.[12] The number of small UAS and their capabilities are increasing so quickly that it is impossible to make a reliable estimate of UAS characteristics, their range of applications, and the volume of UAS flight operations over longer periods of time. It is also difficult to reliably estimate the full scope of demands that UAS, large or small, will place on the NAS. The vast majority of small UAS will not be launched from airports, nor will they operate under the control of en route centers. Nevertheless, at some point a significant number of UAS will be operating in airspace shared with manned aircraft—and that number will surely grow over time.

In the future, ODM could also become a significant factor in terms of air traffic, and commercial space launch and reentry operations (discussed below) could increasingly interfere with the availability of airspace for normal operations. As with UAS, predicting the impact of ODM and commercial space operations on air traffic over the long term is problematic at best.

Increased Uncertainty from New Entrants and Emergent Risks

Predicting the safety risks that new entrants pose to themselves and other elements of the NAS is difficult because of uncertainties about their characteristics, missions, operational modes, and prevalence and how those factors will change over time. The safety risks of aircraft currently operating in the NAS are fairly well known based on historical data on missions, operational modes, normal operations, incidents, and accidents. Existing models and simulations provide additional insight into how these aircraft operate in the NAS, and increasingly sophisticated models are under development. Changes in the design of conventional aircraft and ATM systems

[10] The FAA's en route centers manage the flight of aircraft operating under instrument flight rules (i.e., excluding flight operations by general aviation aircraft operating under visual flight rules).

[11] FAA, 2017, *Aerospace Forecasts Fiscal Years 2017 to 2037*, March, https://www.faa.gov/data_research/aviation/aerospace_forecasts/, pp. 1 and 27.

[12] FAA, 2017, *Aerospace Forecasts Fiscal Years 2017 to 2037*, p. 1.

and related operational procedures introduce some uncertainties, but safety assessments of those changes can be guided by substantial insight into the workings of the NAS as it now exists. The situation with new entrants such as UAS is obviously quite different. There is no direct historical record of their characteristics, missions, operational modes, prevalence, and other factors that influence safety risks. Neither is there a substantial historical record of accident and incident investigations. These elements can still be projected, but the basis for these projections and the results thereof will inherently have much more uncertainty than projections of existing aircraft and systems.

Another source of uncertainly derives from a potential clash of cultures between the traditional aviation community and the UAS community. For example, pilots, air traffic controllers, and airlines are justifiably very focused on preventing as many aircraft accidents as possible to prevent the loss of life and substantial economic costs. In contrast, operators of small UAS are justifiably more risk tolerant because there are no people at risk on a UAS, the risk of causing fatalities on the ground is much lower, and the cost of the vehicle is much lower. In some cases UAS are considered to be expendable, and UAS are sometimes a better choice for hazardous missions to avoid the risk that a manned aircraft could crash with attendant loss of life. These different perspectives of the traditional aviation community and the UAS community will be important to consider in developing UAS systems to prevent elevated risk states, especially with respect to the operation of UAS and manned aircraft in the same airspace.

Trust in Increasingly Autonomous UAS and Associated Traffic Management Systems

The 2014 report *Autonomy Research for Civil Aviation: Toward a New Era of Flight*[13] documents the current and future development of increasingly autonomous systems for UAS, manned aircraft, and ATM and the many challenges associated therewith. This issue is particularly important with respect to UAS because they are rapidly advancing in capabilities, their numbers and range of applications are growing so quickly, and the regulatory and certification barriers to the introduction of new technologies on UAS are so much lower than they are for manned aircraft and ATM systems. Currently, there are no or minimal certification and operations standards for small UAS. Greater understanding is needed with respect to creating a process to certify and/or license increasingly autonomous UAS hardware, software systems, and operators. Reporting requirements for UAS operations are insufficient, and those that do exist have not been organized in coordination with efforts to inform either standards development or traffic management procedures to provide safety assurance.

The level of trust in increasingly autonomous systems is directly related to operators' belief that these systems will perform at acceptable levels of reliability and safety. Initial efforts to enable the integration of UAS into the NAS focused on the goal that UAS demonstrate a level of safety that is equivalent to manned aircraft. It is not viable, however, to use traditional, deterministic design-based standards with advanced, increasingly autonomous systems that incorporate adaptive and/or nondeterministic systems (see Box 5.1 in Chapter 5). The need to resolve issues associated with integration of UAS has accelerated FAA's transition to performance-based standards.[14]

Unauthorized UAS Operations

As noted above, the number of UAS operations is rapidly increasing. Unauthorized UAS pose a threat to other aircraft, especially in the vicinity of airports. If mitigation of this threat is included in the CONOPS, it will be a difficult requirement to satisfy, particularly for small UAS, because air traffic controllers cannot detect, identify, track, and control small UAS. There are many ways in which a UAS may be unauthorized to participate in particular airspace. UAS will likely be limited by altitude restrictions or airspace class, based on their weight. These restrictions cannot take into account the flight envelope of every UAS, and UAS operators may fly their aircraft into restricted airspace, intentionally or unintentionally. Some classes of airspace may have aircraft equipage

[13] National Research Council, 2014, *Autonomy Research for Civil Aviation: Toward a New Era of Flight*, The National Academies Press, Washington, D.C.

[14] The FAA is in the process of transitioning its regulations and guidance from prescriptive "must" statements to performance standards based on the outcome or capability of an aviation system. This methodology, when combined with a risk-based management approach to safety improvements, recognizes that there may be multiple acceptable methods and technologies that could satisfy a regulatory objective rather than a single government-specified action or design approach.

requirements, such as ADS-B. If UAS enter such airspace without the proper equipment, this could cause significant safety risks for the manned aircraft. For example, one solution would be to mandate that UAS be equipped with ADS-B as one requirement for operations above 400 ft. Meeting this requirement would be facilitated by ongoing efforts that are reducing the cost of lightweight, low-power ADS-B systems suitable for small UAS. Development of standards related to equipage, performance, communications, and procedures would also be helpful.

Increasing Pace of Commercial Space Operations

The market for commercial space services is growing, and the pace of launches is expected to increase significantly over the next decade.[15] Reducing the impact of more frequent launches will require changes in how the NAS accommodates space operations, including launch or reentry failures, which in turn will affect design of the functions of an IASMS. Due to the relatively slow pace of commercial space operations to date, simple and conservative methods are used to manage related risk. Specifically, large aircraft hazard areas are created for each launch. These areas encompass airspace that could be affected by a launch or reentry, including cases where the space vehicle fails and generates a debris field. Large hazard areas are justified given that spacecraft launch and reentry have a much higher accident rate than civil aviation. Even so, the large size of these areas interferes with many aviation operations. As the pace of commercial space operations increases, better surveillance data on space operations may become available, and debris modeling may also improve. Nevertheless, it will be challenging to develop the ability to use smaller and more dynamic aircraft hazard areas necessary to reduce the impact of commercial space operations. Specific issues involve the development of real-time decision support tools and, if desired, the capability for some types of spacecraft to operate with aircraft-like separation requirements.

Aerospace traffic management is currently a joint FAA-Air Force function, where the FAA is responsible for safe handling of aircraft traffic around a launch or reentry operation, and the Air Force is responsible for ensuring that operation does not conflict with other currently operating spacecraft. This distribution of responsibility could also change in the future.

RESEARCH PROJECTS

IASMS Concept of Operations and National Airspace System Evolution

Research Project Summary Statement: Develop a detailed concept of operations for an IASMS using a process that considers multiple possible system architectures, evaluates key trade-offs, and identifies system requirements.

This research project would help achieve the vision for an IASMS by establishing the framework upon which all other IASMS research is conducted, by identifying the near-term potential of IASMS research to enhance the safety of the NAS and to engender stakeholder support for and trust in an IASMS, and by facilitating updates to the CONOPS as the NAS evolves. Ongoing research addresses some specific elements, such as UTM, that are needed to implement an IASMS. Additional unique and specific research is needed to develop an overall strategy and CONOPS for an IASMS. Developing a detailed CONOPS will be difficult and time consuming because an IASMS will be a complex and dynamic system of systems and because of the many factors to be considered and the difficulty of assessing the tradeoffs and interactions among them (see below). This research project is urgent because of the difficulty of achieving its goals and because it is needed in the very early stages of IASMS development. A detailed IASMS CONOPS will also define timelines for infrastructure investment strategies that would most efficiently support development of an IASMS. Even so, the execution of this and many other research projects will likely proceed in an iterative fashion (1) as advances in one area support advances in other areas, (2) as more detailed information becomes available for various factors, and (3) as the ability to conduct complex

[15] FAA, Office of Commercial Space Transportation, 2017, *The Annual Compendium of Commercial Space Transportation*, https://www.faa.gov/about/office_org/headquarters_offices/ast/media/2017_AST_Compendium.pdf.

trade-offs involving all of the factors matures. For example, this research project will help define data requirements in terms of completeness and quality. Then, as advances are made in the ability to collect comprehensive, high-quality data in areas of particular interest, the results of trade-offs among various factors may change, which could justify modifications to the CONOPS.

Additional background information related to this research project appears in "IASMS Concept of Operations" in the Challenges section earlier in this chapter. Of particular note is the list of factors that will need to be considered in development of a detailed CONOPS:[16]

- System scope in terms of:
  - — Aircraft types, including new entrants
  - — Data requirements
  - — Known and emergent risks
  - — Operations in different classes of airspace
  - — Time scales for each functional element (monitor, assess, and mitigate) of the generic CONOPS
  - — Users
- Ability to collect required data
- Architecture
- Costs and benefits
- Effectiveness
- Growth in air traffic
- Human performance limitations and human-machine roles
- NAS evolution
- System authority vis-à-vis human performance capabilities and limitations
- Technical capabilities
- Uncertainties associated with each functional element of the generic CONOPS
- Verification, validation, and certification

The project will include elements that are specific to individual aviation domains, including ATM systems, commercial airlines, general aviation, ODM aircraft, UAS, and commercial space operations. A detailed CONOPS will articulate linkages to other domains to ensure synergies to leverage research and to prevent overlapping research efforts.

A key goal of this research project will be to understand the characteristics of an ideal IASMS and to thereby provide additional information for refining the list of key challenges and high-priority research projects. Many of the factors listed are associated with other high-priority research projects identified in this report. Accordingly, the output of many of the research projects that are under way concurrently with the development of the CONOPS will likely support the development of the CONOPS. Of all the high-priority research projects identified in this report, this research project is recommended to be of the highest priority (see Chapter 6).

Identifying and Prioritizing Risks

Research Project Summary Statement: Develop processes to identify and prioritize risks that are relevant to an IASMS and that threaten the safety of the current and evolving NAS.

This research project would help achieve the vision for an IASMS by developing approaches for identifying and prioritizing known and emerging risks that fall within the scope of the IASMS CONOPS. This research project will be difficult to complete largely because of the uncertainties associated with emerging risks. This research is urgent because it is essential to the development of an IASMS CONOPS (see above). Additional background information related to this research project appears in the discussion of the corresponding challenge earlier in this chapter.

[16] System scope is listed first because it is the most important of the factors in the list. The other factors are listed alphabetically.

The process of identifying risks will include consideration of known risk areas, such as loss of control and controlled flight into terrain (see Figure 2.3), that have been identified through traditional accident and incident analysis. More importantly, this research project would provide the basis for identifying emergent risks as the NAS evolves (see "National Airspace System Evolution," in the Challenges section earlier in this chapter). Toward that end, this research project would investigate the use of IASMS data and large-scale data analysis to monitor for systemic or anomalous changes to the NAS. The research project would also ensure that once changes have been identified they can be assessed for risk potential in a way that enhances the currently labor-intensive and subjective approaches that rely largely on assessments by subject matter experts. The risk assessment approach developed by this research project would explicitly or implicitly include a prioritization of risks consistent with standard risk matrix representations (see Figure 2.2). The research project would consider whether there are appropriate mitigation processes that could be enabled by an IASMS. It would also support the development of viable and effective methods for the timely detection and mitigation of elevated risk states for particular risk areas. The research project could investigate many different potential approaches, ranging from relatively simple methods based on exceedance criteria to more complex model-based methods, conformance methods, and statistical methods.

3

System Monitoring

The first step in the operation of an IASMS is a monitoring function that observes and characterizes the system state by collecting, fusing, and assessing data from a variety of sensors (see Figure 1.1 in Chapter 1). The scope and accuracy of an IASMS are thus directly related to the completeness and quality of the data that are available for an IASMS to observe the NAS and determine its system state. This chapter describes challenges for system observation and recommends research projects to address them.

System observation challenges include identifying, characterizing, and collecting data to be used for the intended scope of the IASMS, as established by its CONOPS; see Chapter 2). While some timely and accurate data sources exist, particularly for commercial transports, not all operational parameters are readily observed in a timely and accurate fashion. Some parts of the system are not observable at all, or only with significant effort and cost (e.g., small UAS) operating in unauthorized airspace), while others are not easily observed due to privacy or other policy considerations (e.g., pilot performance). The data from various sources differ in quality. The quality of data may also vary with time as sensors or system conditions change. Last, correlation and fusion of data sources can be challenging due to variations in key parameters, such as timing accuracy and latency, for data collected from different sources.

Resolving these challenges requires research in several key areas. A set of data needs to be identified and assembled via existing or new sources to enable sufficient system observations. Data sources need to be evaluated and monitored for quality and then fused to enable observations that meet the needs of an IASMS at a cost consistent with the value that the data provides. In addition, appropriate measures are needed to protect the privacy and proprietary concerns of data providers and/or the individuals being observed.

This chapter identifies three key challenges and two high-priority research projects:

- Challenges
  - — Data Completeness and Quality
  - — Data Fusion
  - — Collecting Data on the Performance of Human Operators
- Research Projects
  - — Data Fusion, Completeness, and Quality
  - — Protecting Personally Identifiable Information

CHALLENGES

Data Completeness and Quality

Challenge Summary Statement: Successful and efficient implementation of an IASMS requires identification, characterization, storage, and retrieval of the required data subject to availability, completeness, quality, and cost considerations.

Meeting the requirements of an IASMS for complete, high-quality, and affordable data will be a key challenge because some required data are not available and/or cannot be fused in the time frame of interest to an IASMS; some are not systematically stored or are not retrievable; some are expensive to obtain; some are burdened by accessibility and use constraints due to proprietary or privacy concerns; and some are not consistently available with sufficiently high quality, particularly with regard to accuracy and timeliness. While data acquisition is a general-purpose issue for any NAS decision support system, an IASMS has unique requirements for data availability, quality, and timeliness that need to be addressed early in system development because the success of an IASMS is highly dependent on the data used.

A comprehensive IASMS would observe all operations and entities that impact safety risks of interest to an IASMS, both in real time and over some period of history.[1] This is not currently possible because available data sources do not completely cover the needed observations. For example, there is little historical data on new entrants to the NAS, particularly UAS, ODM aircraft, and the increasing pace of commercial space launch and reentry operations. Unlike commercial transports, for which there exists an extensive historical record of normal operations, incidents, and accidents, no such record exists for new entrants. This will be an issue for developing algorithms to detect relevant safety issues. It is also not yet possible to acquire data on new entrant operations in real time or close to real time. While some space operations provide telemetry data, most do not, and while they may be surveilled by Department of Defense (DoD) radar systems, that information is not currently available to the FAA for air traffic control purposes. Standards and data streams do not yet exist for UAS operational data reporting and storage, and some UAS missions are inherently unpredictable because they typically do not follow a fixed flight plan. Likewise, general aviation aircraft do not necessarily file a flight plan if operating under visual flight rules, and surveillance data on general aviation aircraft are only available under a limited set of conditions. New data sources such as ADS-B will likely be needed to bridge existing gaps in observational data.

The means for data collection (as well as for command and control operations) in real time typically involves wireless links from aircraft to terrestrial or satellite-based systems as well as ground system-to-ground system networks. An IASMS could also take advantage of aircraft-to-aircraft communications systems that could become more prevalent in the future. Key factors regarding the collection of data from each of these sources include availability, latency, update rates, integrity, security, formats, avionics standards, implementation and service costs, spectrum regulation, and bandwidth utilization.

A successful IASMS will be trustworthy and capable of effectively detecting elevated risk states (that is, the system will experience few false negatives), and it will have very low false alarm rates (that is, few false positives). This could be quite difficult to achieve, since an IASMS will attempt to detect and assess the risk of rare events—and it will be especially difficult unless the quality of input data can meet the needs of an IASMS CONOPS. Many existing data feeds, however, such as the feed from the FAA's System-Wide Information Management (SWIM)[2] system, are composed of data from many sources of varying quality. The utility of these data in supporting an IASMS CONOPS is limited unless it is possible to determine the source and the quality

[1] The actual scope of the observations conducted by an IASMS will be determined by the CONOPS.

[2] The FAA's SWIM system is an NAS-wide information system that supports development of the FAA's Next Generation Air Transportation System (NextGen) modernization program. SWIM will generate standard data streams and interfaces for use within the NAS and by other members of the aviation community. SWIM is intended to replace legacy point-to-point system interfaces with a modern service-oriented architecture, thereby providing a common set of connections and data components. As of September 2017, SWIM streams are available for traffic flow management data, terminal radar data, flight plan data, and airspace data. As the system matures, it will also provide weather forecast data. Additional information on SWIM is available at https://www.faa.gov/nextgen/programs/swim (accessed December 8, 2017).

of each individual datum and to monitor for changes that would affect the accuracy and reliability of the data. Furthermore, the accuracy and reliability of the data must be explicitly quantified, such that for each risk of interest it is possible to determine key statistics, such as the probabilities of detection and of false alarms. For example, the SWIM Traffic Flow Management System provides a large set of flight data and flow information, including flight planning data, aircraft positions, airport and route status, and predeparture flight status information. Flight position data come either from en route radar, which provides accurate and reliable data, or from oceanic position reports, which provide data that are less accurate, less reliable, and less consistent in terms of quality. Data on the altitude of individual aircraft come from on-board sensors and thus vary in quality depending upon the accuracy of a particular aircraft's on-board altitude measurement system. Some other data are self-reported by airlines, and the timeliness and reliability of these data vary across airlines and in some cases vary over time as airlines update their data collection and reporting systems. Future enhancements to the traffic flow management system will include position reports generated by the ADS-B system, and this will improve the accuracy, reliability, and consistency of position data, but ADS-B data will not necessarily be available for all flight tracks.

The sources and quality of data provided collected by an IASMS need to be understood and tracked over time to determine the quality of IASMS outputs. In addition, some data feeds will need to be stored in a retrievable way, which will be necessary to enable an IASMS to continuously analyze data over the last few days or weeks as necessary to detect elevate risk states that may arise over these time frames. Data storage and retrieval capabilities would also enable running data quality analyses, so that IASMS can determine when a specific data source was either unavailable or degraded for some reason (e.g., because data were being collected from a backup system with lower accuracy).

There is also a value proposition involved in selecting data for system observation. Some data sources are readily available in real time and easy to access. This is the case with data that can be accessed via SWIM feeds. In other cases, data that would be useful for an IASMS, such as position reporting for small UAS, may not be available or the data may be too difficult or too expensive to collect and access. The cost and availability of data will be an important consideration when developing an IASMS CONOPS and prioritizing the risks to be included within the scope of an IASMS (see Chapter 2). Put another way, it is important to identify which data are not necessary or worthwhile to collect.

Data Fusion

Challenge Summary Statement: To accurately detect safety risks, an IASMS will need to correlate and synthesize data from heterogeneous data sources with different formats, timing, accuracy, and other characteristics.

Developing the data fusion capabilities needed by an IASMS will be a key challenge because, while systems exist to assemble and fuse safety-related data weeks or months after operations are complete, the IASMS will require data to be fused in a much more timely fashion. The performance of an IASMS would be enhanced or in some cases enabled by the fusion of data that are not collected by current systems (e.g., human performance data).

Observations needed to detect an elevated risk state in the NAS will require data from many different sources. These sources will vary in accuracy and latency, they may overlap in coverage (e.g., multiple surveillance sources), and they may require correlation (e.g., flight plans and surveillance reports). An IASMS will need flight data, such as aircraft state and trajectory data, as well as nonflight data, such as human performance measurements or voice communications between controllers and pilots and in the cockpit and among the members of a single flight crew.[3]

Methods for fusing flight data for commercial transports are mature, as this is done today in both real-time and post-event analyses. For example, the SWIM Traffic Flow Management System synthesizes data from multiple surveillance sources, schedules, flight plans, and weather forecasts to generate information on current aircraft state and predicted aircraft trajectory. Aircraft position and velocity data are known or estimated, but other parameters

[3] Recording voice communications within the cockpit and making them available to an IASMS raises privacy issues that are addressed in the next section and in "Protecting Personally Identifiable Information," in the Research Projects section later in this chapter.

that may be of importance to an IASMS, such as bank angle or vertical speed, are not known well or at all. Trajectory intent is also imperfectly known, as flights are not always following a cleared flight plan, as is the case when controllers clear pilots to deviate around severe weather as the pilots deem necessary. To achieve IASMS goals, it may be necessary to fuse data from additional sources, such as from ADS-B reports or voice recognition of controller-pilot voice communications.

More data sources are available for post-event analysis than for in-time analysis. Some data cannot be obtained in a timely fashion (e.g., flight recorder data). Also, noncausal[4] post-processing algorithms can be used to produce more accurate flight state data.

As previously noted, comprehensive flight data are not available for flights operating under visual flight rules, for UAS operations, or for commercial space flights. Data fusion is thus also more difficult, and real-time (or near-real-time) modeling and prediction may be necessary to predict or infer vehicle status and intent based on the limited data available and in the time frame of interest for an IASMS.

Data fusing can also raise sensitivity considerations, particularly with regard to storage. Archiving data and making them available for post-event processing may lead to identification of safety issues that are sensitive to some aviation system stakeholders. Data fusion may also reveal sensitive non-safety-related information, such as details of a carrier's business objectives or proprietary design features of an aircraft. This risk is increased when data are stored and are made available for post-event analysis.

Collecting Data on the Performance of Human Operators

Challenge Summary Statement: Data regarding operator performance that are essential to achieving the full potential of the envisioned IASMS cannot be collected in a timely fashion or at all, in part because of privacy and related concerns.

Providing an IASMS with sufficient, timely data on the performance of operators will be a key challenge because of privacy and related concerns. Much of the data necessary to perform in-time safety analysis are associated with the actions and performance of an individual pilot, controller, or other member of the aviation industry. Individuals will be reluctant to agree to disclose performance data that could jeopardize their livelihood, subject them to regulatory or company sanctions, or violate their personal privacy. Similarly, information held by private companies and airlines, including data on the performance of their staff, will be difficult to obtain due to potential liability issues.

There are currently in place systems to improve operator safety performance, and these systems have greatly contributed to aviation safety. These systems are part of airline safety management systems and include FAA-approved programs like the Aviation Safety Action Program (ASAP) to facilitate reporting of safety problems by employees and the Flight Operations Quality Assurance (FOQA) program to capture and disseminate flight monitoring data. These programs provide the foundation of the Aviation Safety Information Analysis and Sharing (ASIAS) program (see Chapter 1).

To mitigate the concerns of operators regarding privacy, enforcement actions, and liability and to thereby encourage the submission of data that would otherwise be unobtainable, the U.S. Congress provided the FAA with the authority to protect from public disclosure information provided under an approved program such as the preceding.[5] This has been extremely successful in obtaining safety information and maintaining the confidentiality of information. Similar protections may be necessary for information provided by individual and corporate operators to NASA for research purposes and ultimately to the entity entrusted with operating the IASMS. Without such legal protections and trust, valuable safety information may not be available for analysis, which could limit the full potential of an IASMS.[6]

[4] In real time, only data on events that have already occurred can be used. In post-event processing, this restriction is not present (e.g., future positions of a flight can be used in refining the "present" position).

[5] Protection of Voluntarily Submitted Information, 49 USC 40123, 1996.

[6] There are analogous privacy, liability, and security concerns in automotive data management, especially as the industry moves toward high-volume vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-cloud-to-vehicle (V2C2V) communications. Research devoted to solving automotive problems may also provide solutions for analogous aviation data management issues.

Current systems such as those listed above are not designed to collect and assess data in the short time frames of interest to an IASMS. Because many accidents and incidents can be traced to human error (individual or collective) or miscommunication, it is important to identify states and conditions that indicate an elevated risk state that involves human error and/or miscommunication. Key issues include how to identify those factors that contribute to elevated risk states related to human performance (e.g., high emotion, fatigue, or inattention, etc.) and how to develop noninvasive data collection methods that will be acceptable to operators, particularly regarding privacy concerns.

Operators sometimes face high levels of stress. The combination of factors such as insufficient rest, hazardous weather, illness, emotional state (e.g., because of the death of a family member), and concerns about their competency to handle operational requirements (especially for inexperienced general aviation pilots on solo flights) can affect an operator's ability to focus or contend with an urgent situation.[7] This highlights the importance of understanding preexisting emotional or cognitive issues that might affect task performance as well as the need for timely data on the state of individual operators.

Currently, there is a significant body of work that quantifies and assesses the performance of pilots. This work is primarily limited to controlled environments, such as a laboratory or simulator, and it includes information gathered via post-flight and post-accident reports. In many studies, data on the internal state of pilots is based on qualitative self-reports of the subject's cognitive and emotional state, such as perceived stress levels and situational awareness. Subjects may have difficulty describing their internal states, and there is also a risk that subjects may under- or over-report their emotional and cognitive processes depending on real or perceived consequences.[8] Much of this work focuses on the final results of a mission or on the completion of a challenging task. Metrics indicating the internal state of the operators in real time or near-real time are far less mature.

The ability to rapidly identify, quantify, and evaluate human-system performance offers a significant advantage in increasing operational safety and efficiency.[9] This information can directly aid the operator's actions and performance through appropriate and well-timed feedback, and it can inform other operators in the NAS of impending issues and conflicts.

RESEARCH PROJECTS

Data Fusion, Completeness, and Quality

Research Project Summary Statement: Develop methods to automatically collect, fuse, store, and retrieve data from different sources and with different formats, timing, accuracy, and other characteristics.

This research project would help achieve the vision for an IASMS because the range of capabilities that can be successfully implemented in an IASMS will be limited if available data are inadequate in terms of completeness, quality, consistency, the ability to fuse them in the time scales of interest, the ability to store them for future use, or the relative cost and value of obtaining additional and/or higher quality data. This research project will be difficult to complete given the substantial advances that are needed to define, acquire, understand, fuse, and store the data required to support planned IASMS capabilities. This project is urgent because it is fundamental to the success of an IASMS and because some components will likely take years to complete. Additional background information related to this research project appears in "Data Completeness and Quality" and in "Data Fusion" in the Challenges section earlier in this chapter.

---

[7] Many general aviation pilots have little flight experience. In contrast the flight crews of all commercial transports include at least one pilot who holds an airline transport pilot certification, which is the highest level pilot certification. This disparity in pilot experience is one factor that contributes to the high accident rate of general aviation relative to airlines. AOPA Air Safety Institute, 2017, *26th Joseph T. Nall Report, General Aviation Accidents in 2014*, Washington, D.C., https://www.aopa.org/training-and-safety/air-safety-institute/accident-analysis/joseph-t-nall-report.

[8] A.K. Webb, A.L. Vincent, A.B. Jin, and M.H. Pollack, 2014, Physiological reactivity to nonideographic virtual reality stimuli in veterans with and without PTSD, *Brain and Behavior* 5(2):e00304, doi: 10.1002/brb3.304.

[9] K.R. Duda, Z. Prasov, S.P. York, J.J. West, S.K. Robinson, and P.M. Handley, 2015, "Development of an Integrated Simulation Platform for Real-Time Task Performance Assessment," *2015 IEEE Aerospace Conference*, pp. 1-9, doi:10.1109/AERO.2015.7118974.

One thrust of this research project would be to establish a picture of current and projected data completeness: What data are likely to be available? What data are needed but are unlikely to be available given current trends in research? What research and changes in policy would enable the collection of necessary data? This research project would begin the slow process of developing operators' support for providing data that are proprietary, sensitive, and/or technically difficult to obtain. This will require consensus in the aviation community that the safety benefit of the information is great enough to convince operators that releasing the data is in the best interest of all aviation users, including themselves. Even then, in some cases it may be difficult to obtain requisite data due to changes in the NAS. For example, there are many envisioned UAS mission profiles in which UAS would operate within airspace shared by manned aircraft. Some UAS will be equipped with increasingly autonomous systems and some will have significantly different flight performance characteristics than manned aircraft. As a consequence the data required to assure safety of some UAS operations are not yet well understood.

Another thrust of this research project would be to (1) gain a complete and quantitative understanding of IASMS input data characteristics, and (2) develop algorithms and processes for monitoring, fusing, and updating this understanding over time as data quality changes and new data sources are added. This would include analyses of the accuracy, timeliness, and reliability of existing and projected input data as well as establishing relationships with the original data providers to anticipate changes. While this is particularly critical for establishing the accuracy of and developing trust in time-critical IASMS functions, it is also important that the quality of stored data be known and recorded so that it can be improved after the operations of interest have concluded, thereby improving the utility of post-operations analyses. Shortcomings in some data, such as gaps in receiving data from a particular source, will likewise need to be recorded and their implications understood. It would also be useful to advance existing capabilities to solve for incomplete data. Existing studies of the quality of NAS data from different sources will be useful to this research project, but the specific needs of IASMS functions will likely require additional studies and algorithm development. The difficulty of the research project will vary across the different data types and sources IASMS will collect. Analyses of data quality requirements will determine which IASMS functions are feasible, and they will provide a basis for setting alerting thresholds that result in a high probability of detecting elevated risk states and a low probability of false alarms.

Protecting Personally Identifiable Information

Research Project Summary Statement: Develop methods of de-identifying and/or protecting sensitive data in a way that does not preclude effective data fusion.

This research project would help achieve the vision for an IASMS because it would enable the timely and automated fusing of large data sets to help overcome the concerns of operators regarding privacy and related concerns. Additional background information related to this research project appears in "Collecting Data on the Performance of Human Operators," in the Challenges section earlier in this chapter.

For information to be used for in-time monitoring and assessment and to be stored for future use, advances in technology (and changes to regulatory policy) are needed to address operators' concerns regarding unauthorized disclosure of identifiable data. Research in this area has advanced the state of the art of text mining of narrative data when disparate data are combined from numerous sources, but current approaches greatly increase the potential for identifying the individual source of specific data. To overcome the concerns of operators and thereby enable an IASMS to achieve its full potential, de-identification of data will need to be done quickly and without the loss of critical operational safety data. This research project will be difficult to complete because source data will be generated from unique and sometimes proprietary systems. It is likely to be particularly difficult to convince pilots and other operators to agree to the monitoring of their cognitive and emotional states, their decision-making capacity, and their sense of spatial orientation for those who are in the risk mitigation decision chain. This research is essential because information concerning time of day, aircraft type, registration numbers, along with many other identifiable sources of information would be particularly valuable to an IASMS, and in many cases key operational and safety data will not be available from other sources.

This research project is urgent because of the time that it will take to develop improved methods for de-identifying and protecting data and to then develop a broad consensus among stakeholders (including operational personnel, unions, and the leadership of airlines, other operators, the FAA, and original equipment manufacturers) that these methods are adequate. This research project could assess the value to each stakeholder of collecting operator data so that all stakeholders understand the value of collecting and storing relevant data in terms of improving the safety of the NAS. For example, the research project could work with stakeholders to identify potentially unsafe conditions that could effectively be addressed using data on operator performance to identify data of particular interest and when it should be collected. Monitoring operators en route is contentious in part because of operators' concerns about recording personal discussions on topics not directly related to operations (even though such communications are not prohibited). It may be less difficult, however, to achieve consensus regarding the collection of selected data in critical parts of the flight regime, such as, for example, upon arming of the instrument landing system when only flight operational communications should be discussed. It will also be important to assure that an IASMS has adequate cybersecurity protection in order to safeguard personally identifiable information. Cybersecurity is also important to assure the operation of the system as a whole, however, so it need not be included in this particular research project.[10]

[10] See "Identifying and Prioritizing Risks," in the Challenges section in Chapter 2, for more information on cybersecurity.

4

System Analytics

The generic IASMS CONOPS presented in Figure 2.1 depicts the key role that the assessing function plays in interpreting and analyzing the state of the NAS and identifying elevated risk states, which then form the basis for mitigation to maintain safe operations. The assessing function will be enabled by sophisticated analytics functions and algorithms that (1) identify and characterize known risk states in the time frame of interest to an IASMS and (2) examine large volumes of stored flight and ground operations data with anomaly detection methods to identify and characterize emergent risks and to update IASMS risk assessment algorithms.

Developing in-time algorithms for identifying and predicting elevated risk states presents many challenges. The lack of a well-defined CONOPS for IASMS (see Chapter 2) makes it hard to define the scope of the in-time algorithms, to define algorithm performance requirements, and to develop verification and validation (V&V) methods for the developed algorithms. The large volume and heterogeneity of NAS data (from commercial transports, UAS, commercial spacecraft, and general aviation aircraft) and the need to align and fuse data from multiple sources (from ground and air operations, ADS-B systems, pilot communications from individual aircraft, and reports of weather conditions throughout the NAS) make it particularly difficult to develop new or improved algorithms, especially machine learning algorithms, and/or make new applications of existing algorithms in order to identify and characterize risk states. Overcoming many of the other challenges addressed in Chapters 2 and 3 will also create demands for more capable analytical systems.

The complexity and size of the NAS implies that a large number of factors can influence system safety. Identifying and characterizing elevated risk states will require developing sophisticated machine learning algorithms that can operate on heterogeneous data of varying quality. Furthermore, the continually evolving NAS will require development of advanced anomaly and hazard detection algorithms that can operate on large volumes of historical operations data to characterize and predict emergent risks and to reprioritize known risks.

In-time safety assessment for a large number of risk factors will require the development of computational architectures for data input and output devices, processing capabilities, and storage that can work with high-volume and high-speed streaming of data from multiple sources. The FAA's SWIM architecture (see Chapter 3), if scaled up to include more distributed architectures and networked repositories, will have the potential to support in-time elevated risk identification and offline anomaly detection algorithms for characterizing emergent risks.[1]

[1] "Offline analysis" refers to analysis of stored data as opposed to online analysis of streamed data in real time or near-real time.

This chapter identifies three key challenges and three high-priority research projects:

- Challenges
  - In-time Algorithms
  - Emergent Risks
  - Computational Architectures
- Research Projects
  - In-time Algorithms
  - Emergent Risks
  - Computational Architectures

CHALLENGES

In-time Algorithms

Challenge Summary Statement: Existing algorithms for identifying and predicting elevated risk states lack the ability to integrate the diversity of data sources of varying quality anticipated for an IASMS.

Developing the algorithms for an IASMS will be a key challenge because the NAS will experience large increases in air traffic by commercial transports and new entrants, such as UAS, whose interactions with manned aircraft are still being investigated. Moreover, the introduction of trajectory-based operations for commercial transports will change the role of ATM systems from tactical to more strategic decision making that will be distributed and partially automated.[2] This will introduce new issues for the algorithms and analytics developed for monitoring, detection, and mitigation of known and emergent risks.

Whereas the traditional role of an IASMS would be to focus on known, high-priority risks, significant changes in airspace operations could result in a reprioritization of known risks and the introduction of new risks. The likelihood of some known risks (see Figure 2.3) may decrease significantly with the introduction of new devices (e.g., ADS-B) and increased automation, but new high-priority risks will likely emerge, and risk prioritization will continue to evolve with changes in operations and as new information becomes available (see "Identifying and Prioritizing Risks," in the Challenges section of Chapter 2).

The large number of relevant factors and the interactions among them will complicate the process of studying and analyzing some high-priority risks. For example, factors related to midair/near midair collisions include trajectory-based operations, interactions between UAS and manned aircraft, the impact of environmental conditions such as turbulence and weather on flight and ground operations, and the cognitive and emotional states of operators.

The challenges in Chapter 3, Systems Monitoring, are also relevant to this challenge. In-time algorithms will require large volumes of heterogeneous, multimodal data, and the ability to process them in in a timely fashion so that an IASMS can monitor ground and air operations and identify and characterize the current state of NAS. Data quality and completeness as well as data fusion will impose requirements on the data-driven state identification methods regarding the ability to process data from multiple sources of varying levels of uncertainty to determine their impact on the reliability of the assessment function as it detects elevated risk states. Key factors related to uncertainties include accuracy, timeliness, completeness, availability, and reliability of the data. Research into uncertainty management and risk analysis methods will enable the detection of elevated risk states and the generation of alarms with low false-alarm rates. For example, in-time monitoring, hazard detection, safety analysis, and

[2] The implementation of NextGen improvements in navigation, communications, surveillance, and automation will enable the ATM system to adopt trajectory-based operations. This will enable the more efficient use of the NAS in the air and on the ground at airports. Full implementation of trajectory-based operations will require operators to install Automatic Dependent Surveillance-Broadcast (ADS-B) and other new equipage on their aircraft (Federal Aviation Administration, 2016, *The Future of the NAS*, Washington, D.C., https://www.faa.gov/nextgen/media/futureOfTheNAS.pdf.

prediction algorithms for an IASMS will need to operate in an anytime[3] manner, and this will require algorithms to account for the different sources of uncertainty and to compute the contextualized risk associated with hazards in dynamically evolving situations.

Developing algorithms to address human performance states is a particularly difficult issue because there is little understanding of the comprehensive set of cognitive and emotional states and conditions of individual humans and their interactions in distributed environments that provide an understanding of normal behavior. In contrast, there is significant understanding and maturity of the laws of physical processes that lead more directly to assessing normalcy in those systems. Individual human responses, behaviors, cognitive states, and emotional states cannot yet be measured or predicted reliably or accurately. If sufficient data are identified and collected on human performance (see Chapter 3), then quantifying and evaluating these data on a relevant time scale is one factor that is needed for an IASMS to achieve its full potential.

Emergent Risks

Challenge Summary Statement: The complexity of the evolving NAS will result in anomalies with unknown root causes, making it hard to develop algorithms that analyze and predict the effects of emergent risks before accidents or incidents occur.

Emergent risks associated with the growth in air traffic by commercial transports, UAS, on-demand mobility, and commercial space operations are discussed in "National Airspace System Evolution," in the Challenges section of Chapter 2. The challenge discussed here is related to the effect of emergent risks on requirements for IASMS analytics to support the discovery and analysis of the effects of emergent risks and to guide the design and development of mitigation procedures to address newly identified risks.

Developing the ability to analyze and predict the threat posed by emergent risks will be a key challenge because the threat posed by emergent risks could increase in frequency and severity as the NAS evolves. Factors related to this challenge include the difficulty of interpreting and tracking the evolution of previously unknown anomalous situations in historical data, especially when they involve complex operational scenarios. In general, analysis schemes will be needed for multidimensional, time series data. These data will be generated by monitoring the state and trajectories of multiple aircraft. The quality of some key data segments may be highly uncertain in that to some extent they may be inaccurate, misleading, missing, or misaligned. Furthermore, the nominal modes of operation of the NAS are not fully known, especially with respect to new entrants. This makes it difficult to differentiate anomalous situations from nominal situations and to establish the root causes of the former with any degree of certainty. As a result, it will also be difficult to establish and validate elevated risk states resulting from emergent risks and to study their longer-term consequences on the operations of the NAS. The form of data relevant to emergent risks and their features may be hard to identify, and the operational data available may be incomplete.

Computational Architectures

Challenge Summary Statement: Existing computational architectures lack the ability to handle large volumes of heterogeneous data and dynamic analytics workflows, both of which are necessary to detect elevated risk states, to detect and characterize emergent risks, and to update the IASMS risk assessment algorithms.

Computational architectures typically focus on data sources, storage, computing mechanisms, and the presentation and delivery of results to the user. Developing the computational architectures needed by an IASMS

[3] Anytime algorithms are required to produce the best results they can within a given time bound for computation. In other words, they produce a result even if they are interrupted before completion (S. Zilberstein, 2017, Using anytime algorithms in intelligent systems, *AI Magazine* 17(3):73).

will be a key challenge because these architectures will deal with big data[4] acquired from a variety of sources, some of which may be stored (such as past aircraft trajectories, or runway configurations). Much of this will be streaming (e.g., data related to current aircraft locations, weather conditions, and pilot-to-pilot and pilot-to-air traffic controller communications). Analysis of these data to identify the occurrence of known hazards (e.g., loss of control) in real time as well as over periods of hours or days to look for anomalies and emerging risks presents many difficulties. Parallel computing architectures, perhaps in the form of extensions and derivatives of the current Hadoop[5] infrastructure (such as Apache Hama[6]), will have to be developed for processing of streaming and stored data.

As the ATM system evolves, it is unclear how data collection methods and systems can scale up to collect the very large volumes of heterogeneous, multimodal data that are going to be generated from multiple sources and multiple regions in the airspace. These include different commercial airlines, UAS operators, ground operations systems, environmental data such as weather conditions and turbulence, and operational data from the ATM system. A key part of this challenge will be how to scale up the current data exchange standards established in the SWIM program to accommodate the collection and distribution of the large volumes of heterogeneous, multimodal data from operations of the NAS, especially as the system evolves. The centralized SWIM architecture may need to be revamped to set up a shared, distributed computational architecture that includes networked repositories and computational systems to support online IASMS analytics operations that cover ground operations and the airspace.

Another key element of this challenge is the need for computational architectures to support multiple data sources and consumers of various components of the data. This raises additional issues, including the need for infrastructure for data abstraction, alignment, and integration. In addition, advanced software that interconnects various elements of the architecture is needed to build analytics workflows that can be configured for a variety of data sources and algorithms described above. Configuration and reconfiguration of computational workflows would also benefit from the ability to incorporate new analytics components to enable newer functionalities. Another necessary element would be a management layer in the architecture to ensure the seamless execution of both online and offline analytic tasks.

---

[4] One can separate big data and "regular-size" data based on the presence of a set of characteristics commonly referred to as the four V's: volume, variety, velocity, and veracity. The *volume* of data collection is pervasive across industries including finance, manufacturing, retail, health, security, technology, and NAS operations. Furthermore, in the vocabulary of big data, petabytes and exabytes have now replaced terabytes. To put these volumes into perspective using the classic grains of sand analogy: if a megabyte is a tablespoon of sand, a terabyte is a sandbox 2 feet wide and 1 inch deep, a petabyte is a mile-long beach, and an exabyte is a beach extending from Maine to North Carolina. The *variety* comes from structured, semistructured, and unstructured data accumulated from multiple sources, and includes traditional transactional data, user-generated conversations, sensor-based data, and spatial-temporal data. The *velocity* of data creation is a hallmark of big data, and it has important implications for "real-time" predictive analytics in various application areas, ranging from finance to health. Simply put, analyzing "data in motion" presents new challenges because the desired patterns and insights are moving targets, which is not the case for static data. *Veracity* pertains to the credibility and reliability of different data sources, which may have varying degrees of noise, corruption, and incompleteness. In addition, aligning large volumes of time-series data from heterogeneous sources can be a challenge, as is deriving deep semantic knowledge from a combination of these data sources (A. Abbasi, S. Sarker, and R.H. Chiang, 2016, Big data research in information systems: Toward an inclusive research agenda, *Journal of the Association for Information Systems* 17(2):1-32).

[5] Hadoop (created by Doug Cutting and Mike Cafarella in 2005) makes it possible to run applications on systems with thousands of commodity hardware nodes, and to handle thousands of terabytes of data. Its distributed file system facilitates rapid data transfer rates among nodes and allows the system to continue operating in case of a node failure. This approach lowers the risk of catastrophic system failure and unexpected data loss, even if a significant number of nodes become inoperative. Consequently, Hadoop quickly emerged as a foundation for big data processing tasks, such as scientific analytics, business and sales planning, and processing enormous volumes of sensor data, including from Internet of Things sensors. It is part of the Apache project sponsored by the Apache Software Foundation. (See TechTarget, "Hadoop," in "Essential Guide: Managing Hadoop Projects: What You Need to Know to Succeed," last updated September 2016, http://searchcloudcomputing.techtarget.com/definition/Hadoop?.)

[6] K. Siddique, Z. Akhtar, E.J. Yoon, Y.S. Jeong, D. Dasgupta, and Y. Kim, 2016, Apache Hama: An emerging bulk synchronous parallel computing framework for big data applications, *IEEE Access* 4:8879-8887.

RESEARCH PROJECTS

In-time Algorithms

Research Project Summary Statement: Develop robust and reliable algorithms that can assess large volumes of heterogeneous data of varying quality to simultaneously identify and predict elevated risk states of many different types, and that are fast enough to meet in-time requirements.

This research project would help achieve the vision for an IASMS, because IASMS will be dealing with a new and evolving environment for flight management operations, which could create situations where a lack of knowledge about how hazards evolve may hamper detection and decision making. Addressing this shortfall will require development of advanced machine learning methods to analyze large volumes of heterogeneous data and find anomalous patterns and precursors to hazards. Another requirement will be the development of interfaces with operators that can succinctly inform them of both impending hazards and corrective action to mitigate the hazards. Additional background information related to this research project appears in the discussion of the corresponding challenge earlier in this chapter.

This research project will be difficult to complete because of the growing complexity of the NAS and because of the large and growing number and variety of aircraft operating in the NAS, including new entrants. In addition, this research project faces significant uncertainties regarding the ability to acquire all of the data needed to monitor the NAS, to assess the system state, and to detect elevated risk states. This research project is urgent because in-time algorithms will form the core of the monitoring, detection, prediction, and mitigation tasks of the IASMS.[7]

Advances in supervised, semi-supervised, and unsupervised machine learning algorithms will be needed to reliably characterize known hazards and to discover new hazards, all while taking into account the multidimensional operational space of aircraft, their flight trajectories, human performance states, key inputs to human performance, and environmental factors.

Predictive algorithms will be needed to follow evolving situations and to prognosticate the occurrence of adverse events that can degrade safety. In addition, software tools will need to be able to conduct what-if analyses to support ground control and air traffic control to study the effects of safety assurance actions being applied in evolving hazardous and anomalous situations.

For both state identification and state prediction, this research project will need to consider the confluence of factors arising from aircraft operations and trajectories, interactions between UAS and manned aircraft, the density of air traffic, and weather conditions. Even when any one of these by itself does not imply an elevated risk state, some combination of these factors could indicate that hazards exist. Eventually, system analytics and data mining methods will need to be extended to support V&V methods both to assure that an IASMS will operate safely and to determine appropriate operational boundaries.[8]

This research project will address approaches to V&V to the extent that new methods will be needed to ensure the correctness of advanced algorithms. The complexity of this problem may necessitate the development of test beds, such as the Shadow Mode Assessment Using Realistic Technologies for the National Airspace System (SMART-NAS) project.[9] The high dimensionality and the uncertainty in the data will necessitate verification schemes that are based on stochastic and Monte Carlo simulation methods.

IASMS algorithms must be robust and reliable given the variability in the quality and completeness of the available data. An operational IASMS will, of course, rely to a large extent on streaming operational data. Much of that data is not currently being collected, and so this research project (and some others) will need to rely on data produced by models and simulations. Data storage schemes and computational processing architectures for

[7] As shown in Figure 2.1, the generic CONOPS defines a process whereby (1) operational data is extracted from the NAS and fed into a risk monitoring system that determines the system state; (2) the system state is continuously assessed for elevated risk states; and (3) when an elevated risk state is detected, a mitigation process is triggered to implement a safety assurance action that reduces the identified risk level.

[8] For more information on VV&C, see both "System Verification, Validation, and Certification" sections in the Challenges and Research Projects sections in Chapter 5.

[9] NASA's SMART-NAS test-bed provides simulation and testing support for NASA's air traffic management research.

big data, as discussed above, will also play an important role in this research. These algorithms will form the core of the in-time IASMS assessment and mitigation functions, and they are essential from maintaining the effectiveness of an IASMS as the NAS evolves.

Emergent Risks

Research Project Summary Statement: Develop approaches for continually mining historical data for detecting previously unknown anomalies and their evolution to characterize emergent risks and to update the IASMS risk assessment algorithms.

This research project would help achieve the vision for an IASMS because well-defined metrics to characterize safety margins and risk thresholds need to be established along with the ability to track these metrics as the NAS evolves. Although research in this area is already under way to study anomalies and emergent risks for individual aircraft, existing research will not meet the unique needs of an IASMS because of the complexity of an IASMS in terms of the scale, the heterogeneity, and the uncertainties in characterizing the airspace and time frame of interest to an IASMS. This research project will be difficult to complete because of the growing complexity of the NAS and because of the large and growing number and variety of aircraft operating in the NAS, including new entrants. This research is urgent because it will take a long time to develop the new classes of offline data-driven methods, machine learning and data mining algorithms, and analysis and prediction techniques that will be needed for each functional element (monitor, assess, and mitigate) of the IASMS to address adequately the hazards posed by emergent risks. Additional background information related to this research project appears in the discussion of the corresponding challenge earlier in this chapter.

Large amounts of historical data from air and ground operations over long periods of time are required to assess emergent risks. New and sophisticated data preprocessing methods are needed to clean, curate, and achieve established norms for data quality before the data are provided to IASMS analytics and machine learning algorithms. Furthermore, growth in the number and variety of new entrants, especially UAS; data integration and alignment; and feature extraction will be increasingly difficult.

This research project is not intended to conduct what-if analyses that explore a list of risks posed by researchers. Those analyses will be conducted by the research project on identifying and prioritizing risks (see Chapter 2). Rather, this project will be a data-driven effort that seeks to identify unknown near-term risks that are growing in magnitude and should therefore be considered for inclusion within the scope of an IASMS.

Existing semi-supervised and unsupervised learning methods that can operate on large amounts of complex historical data are needed to support discovery and characterization of anomalous operations and potentially unforeseen circumstances that may lead to elevated risk states. An important consideration for successful application of unsupervised algorithms is the application of feature selection to reduce the dimensionality of the space by removing redundant and irrelevant features. This will make the anomaly detection algorithms computationally efficient with outputs that are more robust in terms of false positives and false negatives, both of which need to be reduced. The anomaly detection methods developed to address emergent risks may also prove to be useful in providing new insights into the causes of known hazards. These anomaly detection methods will require the involvement of human experts to aid in the interpretation of anomalies and to initiate analyses to find root causes. Once the risks of anomalies have been characterized, the experts may direct updates to the in-time risk detection and identification algorithms.

Computational Architectures

Research Project Summary Statement: Support the design of data repositories and computational architectures that support online detection of elevated risk states and offline analysis to detect and characterize emergent risks and to update the IASMS risk assessment algorithms.

This research project will provide the core infrastructure that will provide the basis for the algorithms used for online and offline elements of an IASMS. With the explosion of big data applications across business, engineering,

medicine, and scientific research, distributed cloud architectures and accompanying computational architectures are being developed and deployed. This research project will be difficult to complete because research and development focused on other applications will not meet the unique needs of an IASMS in terms of scope and spatial and temporal complexities; the need for timely processing of large volumes of streaming and stored heterogeneous data with varying levels of quality and frequency; and the need to provide a reliable, fault-tolerant, and secure system that degrades gracefully when adverse situations (e.g., regional power failures) and malicious threats are launched against the system. This research is urgent because data repositories and computational architectures will provide the backbone of the IASMS operational system and are therefore needed early in the IASMS research and development effort. Additional background information related to this research project and to big data as it applies to an IASMS appears in the discussion of the corresponding challenge earlier in this chapter.

Computational architectures for IASMS face a scaled-up version of the big data challenge. This includes the need to effectively organize and extract relevant information from large volumes of frequently changing streaming data generated by multiple, heterogeneous, and autonomous sources in the NAS. In addition, there is the need for in-time analysis using statistical and machine learning techniques developed for risk identification and prioritization. Simultaneously, the architecture will have to support offline analysis of large volumes of stored heterogeneous data of varying quality and frequency for detection of previously unknown hazards and emergent risks. The potentially large number of airlines and other operators, the need to control UAS and manned aircraft in the same airspace, the lack of data collection standards and requirements (which will make data fusion more difficult), and the lack of well-defined repositories present significant difficulties in advancing research on computational architecture to support IASMS algorithm development, decision making, and visualization of complex data for flight and ground operations. Modern commercial transports have substantial on-board processing and data storage capacities, and this could facilitate the availability of data needed by an IASMS. It is not anticipated, however, that the computational architecture will rely on on-board systems because of the proprietary nature of those systems and the high cost of modification.

Many of the organizations that are most involved in the development and use of big data have been developing technologies in other domains to address the problems of in-time processing and analysis of large data streams. Even so, the extent to which these approaches can be applied to an IASMS remains to be seen.

One goal of this research project will be to develop technology-independent reference architectures and categorization of related implementation technologies and services to enable the development of a big data architecture suitable for an IASMS. Such an architecture will need to research a four-layered abstraction model to explore complex and evolving relationships among data. The four layers are the physical layer, the data layer, the computing layer, and the data analytics layer.[10] Research related to the physical layer will include approaches for handling streaming and stored data, it will be scalable to assure redundancy and fault tolerance, and it will allow data transfer at high rates and efficient support for computation. Research related to the data layer will address core functionalities, such as data organization, to enable information exchange and fusion and to ensure that all distributed storage devices can support common goals while facilitating fast access and retrieval of the data in both the streaming and stored models of operation. Research related to the computing layer will address the needs for data modeling and query, and it will develop tools that facilitate retrieval of structured and nonstructured data while also supporting advanced computational architectures, such as Spark[11] and Storm[12] and their future evolutions to

[10] The four-layer architecture is a widely used, generic template used in big data applications. However, some researchers and practitioners have proposed a different four-layer scheme, such as (1) data source, (2) data storage, (3) data processing/analysis, and (4) data output. See B. Marr, 2016, *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*, John Wiley & Sons, Hoboken, N.J.

[11] Apache Spark is an open-source cluster-computing framework for tackling big data problems. Spark provides programmers with an application-programming interface centered on a data structure called the resilient distributed dataset, a read-only multiset of data items distributed over a cluster of machines that is maintained in a fault-tolerant way. Spark supports a variety of systems, including Hadoop. See J.G. Shanahan and L. Dai, 2015, Large scale distributed data science using Apache Spark, pp. 2323-2324 in *Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Association for Computing Machinery, New York, N.Y.

[12] Apache Storm is an open-source, distributed, and scalable high-speed stream processing computational framework for applications such as real-time analytics, online machine learning, and continuous computation. See "Apache Storm," http://storm.apache.org, accessed December 8, 2017.

allow for data-intensive computing for statistical analysis and machine learning algorithms. Research related to the data analytics layer will provide the computational abstractions to support the analytics and mining functions for in-time and emergent risk analysis while also providing the textual and graphical interfaces to support effective human-machine interactions.

This research project will also develop visual and configurable schemes for generating workflows that support the data analysis tool chain: acquisition, data cleaning and alignment, preprocessing, curation, analytics and mining, and generation of actionable information to support automated as well as human-in-the-loop decision making. This project would also investigate secure repositories and computational architectures that scale with the four V's (volume, variety, velocity, and veracity) associated with big data applications.

5

Mitigation and Implementation

This chapter addresses issues related to the mitigation function of an IASMS and to the implementation of an IASMS once the necessary technologies and capabilities have been developed. As discussed in Chapter 1, an IASMS requires the ability to detect and mitigate elevated risk states on a much shorter time scale than existing safety management systems. The NAS is a complex and evolving system of systems, and as that complexity increases, the risk increases that the outputs of an IASMS (that is, the safety assurance actions) will in some situations have unintended consequences that create new and unanticipated safety risks. The effectiveness of an IASMS will be limited if operators do not trust the system's safety assurance actions, including alerts, decision support aids, and independent actions. It will be especially important for an IASMS to engender operators' trust as advanced IASMS are developed and given greater autonomy and authority. Aircraft operators represent an important potential source of data for an IASMS, but they will likely not support costly technical and infrastructure investments unless the safety benefits are worth the expense and as long as participating in an IASMS does not create a competitive disadvantage.

This chapter identifies five key challenges and three high-priority research projects:

- Challenges
  - — In-time Mitigation Techniques
  - — Unintended Consequences of IASMS Action
  - — Trust in IASMS Safety Assurance Actions
  - — System Verification, Validation, and Certification
  - — Operators' Costs and Benefits
- Research Projects
  - — In-time Mitigation Techniques
  - — Trust in IASMS Safety Assurance Actions
  - — System Verification, Validation, and Certification

CHALLENGES

In-time Mitigation Techniques

Challenge Summary Statement: Existing mitigation techniques are limited in their ability to respond to many risks in the short time frame of interest to an IASMS.

Developing mitigation technologies that can cover the scope of issues to be addressed by an IASMS will be a key challenge because of many factors, including the short time frame of interest to an IASMS (see Chapter 1), the many different types of operations in the NAS (see Chapter 2), and the wide variety of known and emergent risks (see Chapters 2 and 4).

An IASMS will be expected to mitigate elevated risk states associated with a wide variety of ground and air operations, such as arrival and departure sequencing, vectoring and hold operations, four-dimensional trajectories (latitude, longitude, altitude, and time), and balancing of capacity with demand across various regions of the NAS.[1] The response to some of these risks will require urgent action by operators to safeguard individual aircraft. In addition, anomalies and elevated risk states can in some cases propagate rapidly across various operations and aircraft, making it difficult to identify root causes and to mitigate elevated risk states in a timely fashion. Emergent risks are also of particular concern. For example, navigation, communication, and surveillance operations in the NAS are migrating to digital and network-based operations, and this may introduce new cyber vulnerabilities that could fall within the scope of an IASMS.

Timely mitigation techniques will need to account for human operators in the decision-making loop and provide sufficient information to them in a timely manner so that they can take the appropriate actions to mitigate the evolving risks and hazards. Consider Asiana Airlines flight 214, which on July 6, 2013, during an approach at San Francisco National Airport, struck a sea wall. At the time the instrument landing system's glide slope for the runway was out of service and so the flight crew was making a visual approach. The National Transportation Safety Board determined that the probable causes of the accident were the flight crew's mismanagement of the airplane's descent during the visual approach, the unintentional deactivation of the automatic airspeed control by the pilot flying the aircraft, the flight crew's inadequate monitoring of airspeed, and the flight crew's delayed execution of a go-around after they became aware that the airplane was below the minimum acceptable altitude and airspeed for the glide path. An IASMS could possibly have identified and responded to key factors that combined to increase the risk during this approach. Most importantly an IASMS could have identified that the aircraft approach continued below 500 feet of elevation even though Asiana Airlines requires that a stabilized approach be established by that point in the approach. Depending upon the control authority granted to an IASMS, the system could have initiated a go-around or advised the flight crew to initiate a go-around while still at a safe altitude. As it was, the flight crew did not initiate a go-around until the aircraft was at 100 feet, and they were unable to complete the maneuver before impacting the sea wall.[2]

Even in those situations where the IASMS has the authority to act independently in response to a particular elevated risk state, human operators may need to be informed of the risk and mitigating action so that they can judge whether to allow the IASMS to continue its response or to override the IASMS.

Unintended Consequences of IASMS Actions

Challenge Summary Statement: An IASMS could inject new risks into the NAS due to unintended consequences of actions that it recommends or initiates.

---

[1] The IASMS Concept of Operations and National Airspace System Evolution research project will generate detailed guidance regarding requirements for system mitigation.

[2] National Transportation Safety Board, 2014, *Descent Below Visual Glidepath and Impact with Seawall, Asiana Airlines Flight 214, Boeing 777-200ER, HL7742, San Francisco, California, July 6, 2013, Accident Report NTSB/AAR-14/01 PB2014-105984*, Washington, D.C., https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR1401.pdf.

Predicting and minimizing the unintended consequences that could arise from the safety assurance actions of an IASMS will be a key challenge because of the complexity of the NAS and the innumerable ways in which an IASMS could interact with various elements of the NAS. The overall safety analysis and operational approval of an IASMS will need to address the possibility of unintended consequences, and this may require synchronization between different human and/or automation agents in the system to avoid conflicting actions or recommendations between different agents in the system.

The importance of this challenge was illustrated by the Überlingen TCAS accident in 2002. This accident was a midair collision of two aircraft, Bashkirian Airlines Flight 2937 and DHL Flight 611, near Überlingen, Germany. The accident investigation identified two immediate causes for the accident.[3] First, the air traffic controller did not notice that the aircraft were on a collision course soon enough to maintain safe separation between the two aircraft. Thus, although he directed Flight 2937 to descend to avoid the collision, the projected path of the two aircraft still indicated that the risk of collision was so high that the Traffic Collision Avoidance System (TCAS) on each aircraft directed the flight crew to take action. In particular, the TCAS on Flight 2937 advised the pilot to ascend (countermanding the order from the air traffic controller), while the TCAS on Flight 611 advised the pilot to descend. The second immediate cause of the accident was that the pilot on Flight 2937 continued to descend even after receiving the TCAS warning to ascend. In other words, the pilot on Flight 2937 received conflicting advice from two agents, one human and one automated, each of which was not aware of the action being recommended by the other. Because of this lack of synchronization, and because the pilot erred in following the advice of the human agent instead of the automated agent, two aircraft and all 71 people aboard those two aircraft were lost.

Trust in IASMS Safety Assurance Actions

Challenge Summary Statement: The efficacy of an IASMS will be degraded if it is built without regard to the factors that influence operators' trust in the system.

Ensuring that operators develop trust in the safety assurance actions of an IASMS (e.g., system alerts, decision aids, and independent actions) will be a key challenge because the complex, multifaceted, dynamic, computational nature of the system may lead to safety assurance actions that are unfamiliar, unexpected, and/or run counter to operators' training and experience. While this section addresses trust with respect to the safety assurance actions, the issue of trust includes many other factors. Chapter 3 addresses other trust factors, such as the disclosure of personal or private information.

The issue of human trust in technology is growing in importance as new systems incorporate an increasing level of functionality and decision-making capabilities. This can be a significant barrier to the acceptance of some increasingly autonomous systems, such as advanced UAS, but this issue is not limited to unmanned vehicles. The number of other systems that provide capabilities such as process improvement and intelligent decision support are also on the increase, and IASMS certainly falls in the latter area.

Appropriate levels of trust are necessary to assure that operators use systems such as an IASMS to their full extent. This occurs when an operator's trust matches a system's capabilities. If an operator's trust of a system exceeds the system's capabilities, then the system could be misused. On the other hand, if an operator's trust falls short of the system's capabilities, then the system could be underused. Inappropriate trust materializes as a mismatch of expectations and eventually leads to operator overload, limited or no use of the system, and decreased system utility.[4]

Within the aviation community, interviews with operators confirm that, even if a system's capabilities are impressive and even if the system operates as the system developers and manufacturers intended, operators will limit their use of a system if they do not trust the system to act appropriately. In the best case, if operator accep-

[3] Bundesstelle für Flugunfalluntersuchung (BFU) (German Federal Bureau of Aircraft Accidents Investigation), 2004, *Investigation Report AX001-1-2/02*, BFU, Braunschweig, Germany, http://www.bfu-web.de/EN/Publications/Investigation%20Report/2002/Report_02_AX001-1-2_Ueberlingen_Report.pdf?__blob=publicationFile.

[4] J.D. Lee and K.A. See, 2004, Trust in automation: Designing for appropriate reliance, *Human Factors* 46(1):50-80.

tance is not addressed during the formation of the system, operators will use only a portion of the functionality. In the worst case, the operators will ignore the system. Both the functionality and the money spent on systems such as IASMS will be wasted if operators do not trust the system enough to use it or if they act in accordance with the system's output only when the system concurs with the action that operators have already decided to take.

Less complex technologies, such as anti-lock brakes on cars, were slow to gain operator acceptance due in part to the fact that the proper use of the braking system (which anti-lock brakes imposed under specified conditions) ran counter to operators' training and experience. This created a conflict of expectations between what the operators believed they could do versus what the technology could do. The acceptance of anti-lock brakes was mostly solved through increased familiarity with the technology and with positive experiences that accumulated over time. With an IASMS, however, its extraordinarily complex algorithms, its use of enormous amounts of data, and the wide variety of situations in which it may act, will make it difficult to engender the trust of operators solely through changes in training and experience with the use of the system.

An IASMS has the potential to draw conclusions and either recommend or initiate safety assurance actions that in some cases are unfamiliar, unexpected, and/or run counter to operators' prior training and experience. In some situations operators will have very little time to decide whether to trust the output of an IASMS, and in some of those situations it will be vital that the operator make the correct decision because the consequences of making a wrong decision could be catastrophic to the crew, their passengers, and to people on the ground.

System Verification, Validation, and Certification

Challenge Summary Statement: There is no accepted approach to verification and validation that leads to certification of a software system as complex as an IASMS, particularly if, as expected, the system includes adaptive and/or nondeterministic algorithms.

Verification, validation, and certification (VV&C) of an IASMS will be a key challenge because of shortcomings in regulatory requirements certification of an IASMS as it is currently envisioned; a lack of certification standards to provide guidance for complying with regulatory requirements; and a lack of verification and validation (V&V) technologies for an IASMS that would permit conformance to the requirements that are likely to appear in certification guidance.

"Verification" refers to the processes for ensuring that a given product, service, or system meets its specifications. "Validation" refers to the process for ensuring that the product will fulfill its intended purpose. V&V methodologies are typically underpinned by well-established scientific principles. VV&C are critical steps on the path to engendering the trust necessary for operators to accept the outputs of a complex system. This is especially important for an IASMS because the outputs of the system may not be intuitive to the operator.

V&V processes currently employed in aviation are geared toward obtaining quantitatively predictable outcomes based on known inputs or stimuli. In the case of an IASMS, requirements would be deconstructed from the overall IASMS into hardware and software. While challenging, there are several accepted approaches to certification of hardware. (See, for examples, DO-160C.[5,6]) In the case of traditional computer hardware, certification can also be achieved through service-life history.

FAA certification of software is performed through the methodologies detailed in DO-178C, Software Considerations in Airborne Systems and Equipment Certification, and in DO-278C, Software Standard for Non-Airborne Systems. The DO-178C/278C methodologies have been shown to provide reliable software that meets certification requirements with certainty.[7] While inputs to these software systems may be stochastic (from, for example, air data sensors), and stochastic analysis may be used for certification of mechanical aircraft parts, stochastic approaches are not used to certify software. The DO-178C/278C methodologies are time consuming and expensive to complete,

[5] DO-160C, which is published by RTCA, addresses environmental conditions and test procedures for airborne equipment.

[6] For a complete list of RTCA standards and other documents, see "Standards and Guidance Materials," https://www.rtca.org/content/list-available-documents, accessed December 28, 2017.

[7] National Research Council, 2007, *Software for Dependable Systems: Sufficient Evidence*, The National Academies Press, Washington, D.C.

and they do not apply to the adaptive, nondeterministic systems (see Box 5.1) that are likely to be incorporated into an advanced IASMS because of the following reasons:

- An IASMS software system will be very complex due to the varied and large number of inputs and the complexity of the algorithms.
- An advanced IASMS is expected to be adaptive because it will modify its response to a given input over time. That is, after an initial training phase an IASMS will continue to "learn" as a result of its operational experience in different situations. Therefore, the IASMS will tend to accommodate changes in the NAS, whether the changes are a result of operating in different geographic regions; seasonal variations in air traffic; and evolution of the NAS as systems, equipage, and procedures are updated, air traffic flows are rerouted, new entrants become more common, and so on. Current certification standards are incompatible with adaptive/nondeterministic systems because those standards demand and expect, among other things, that systems will consistently respond in the same way to a given situation. In order to be certified using current VV&C procedures, the adaptive features of an IASMS would need to be locked down after a training phase and before the VV&C process, thus negating the adaptability of the system. This would not, however, resolve this issue if the IASMS is also nondeterministic.
- Verification technologies for adaptive/nondeterministic systems are being developed by the Defense Advanced Research Projects Agency (DARPA), the Air Force Research Laboratory (AFRL), and NASA, among others. In addition, the National Highway Traffic Safety Administration is developing standards for autonomous cars that are consistent with the risk assessment matrix in Chapter 2 (see Figure 2.2). It may be possible to use the research coming out of these efforts to support IASMS research. An IASMS, however, is substantially more complex than the systems that are the focus of ongoing research, and additional research will be needed to support VV&C of an IASMS. This is particularly true with regard to development of methods for continuous certification or certification in block updates, which would facilitate improvements in an IASMS to accommodate changes in the NAS.

BOX 5.1
Adaptive/Nondeterministic Systems

Adaptive systems have the ability to modify their behavior in response to their external environment. For aircraft systems, this could include commands from the pilot and inputs from aircraft systems, including sensors that report conditions outside the aircraft. Some of these inputs, such as airspeed, will be stochastic because of sensor noise as well as the complex relationship between atmospheric conditions and sensor readings not fully captured in calibration equations. Adaptive systems learn from their experience, either operational or simulated, so that the response of the system to a given set of inputs varies and, presumably, improves over time.

Systems that are nondeterministic may or may not be adaptive. They may be subject to the stochastic influences imposed by their complex internal operational architectures or their external environment, meaning that they will not always respond in precisely the same way even when presented with identical inputs or stimuli. The software that is at the heart of nondeterministic systems is expected to enable improved performance because of its ability to manage and interact with complex world models, which involve large and potentially distributed data sets, and to execute sophisticated algorithms to perceive, decide, and act in real time.

Systems that are adaptive and nondeterministic demonstrate the performance enhancements of both. Many advanced increasingly autonomous systems are expected to be adaptive and/or nondeterministic.

SOURCE: National Research Council, 2014, *Autonomy Research for Civil Aviation: Toward a New Era of Flight*, The National Academies Press, Washington, D.C.

- Requirements need to be developed for IASMS that are based on a consensus among stakeholders with regard to system reliability, the ability to detect elevated risk states, an acceptable level of false positives, a clear definition of what constitutes a risk condition, and the ability to minimize the creation of new risks. This consensus will be the basis that regulators will use to address the certification of an IASMS.
- The level of intended impact of an IASMS (which could range, for example, from increasing the situational awareness of an operator to the initiation of safety assurance actions on its own authority) will likely determine the assurance level for the software design and V&V testing. Higher assurance levels result in higher costs for V&V.

In summary, there is tension between the nature of adaptive (learning) systems and the need to certify them. Impressive functionality can be implemented with adaptive capabilities, but this comes at a cost of not meeting certification requirements for a component of the NAS. Likewise, a deterministic IASMS could be certifiable, but that would also limit its advanced capabilities. A key part of the VV&C challenge will be to find a proper balance between functionality with the ability to certify an IASMS, recognizing that improving the latter would enable improvements to the former.

Operators' Costs and Benefits

Challenge Summary Statement: Operators' perception of the cost-to-benefit ratio of an IASMS may be so high that it will impede its implementation.[8]

The perceived cost-to-benefit ratio of implementing an IASMS could be a key challenge because operators will need to fund the purchase and installation of IASMS-specific equipment on their aircraft or other aviation systems.

Some aviation safety enhancements, such as those arising from the Commercial Aviation Safety Team (CAST) and Aviation Safety Action Program, can be implemented without new equipage. Many of the future data sources needed for the successful adoption of a fully functional IASMS, however, will require new and sophisticated aircraft equipage, such as upgraded avionics and sensors, as well as new ground infrastructure and data processing capabilities. Airline operations in the NAS are already extremely safe; based on current accident rates the probability that any individual airline will experience a catastrophic accident is extremely low, even over a time frame of decades. In addition, airlines and other operators have limited financial resources. Therefore, the higher the cost of developing and implementing an IASMS, the more difficult it will be to demonstrate a satisfactory cost-to-benefit ratio. The issue of cost is especially problematic with the general aviation community. Even though general aviation operations are much more hazardous than airline operations, the ability of general aviation aircraft owners to pay for new safety equipment is for the most part extremely limited. In addition, despite the higher accident rates for general aviation aircraft (see Chapter 1), the probability that any individual pilot will have an accident over a lifetime of flying is nevertheless quite low.

When operators believe that the cost of a safety system exceeds the expected benefit, widespread use is unlikely to occur unless and until regulatory mandates are issued. Consider the Aviation Collision Avoidance System, which was the predecessor to TCAS. These collision avoidance systems reduce the risk of collision for one aircraft only if other aircraft are similarly equipped. As a result, there was minimal benefit to early adopters. The issue of cost versus benefit for airborne collision avoidance systems in the United States was not resolved until the FAA issued a mandate following a midair collision in 1986 with 82 fatalities.

As noted in Chapter 2, however, the NAS is evolving into an increasingly complex system that will need to accommodate new entrants and address emergent risks associated with those new entrants and other factors. If as a result, the safety of the NAS is degraded, even in a minimal way, modernization and innovation in the NAS, including the accommodation of new entrants, could be significantly delayed, thus potentially hindering growth of the U.S. economy and international competitiveness. Developing a consensus to support IASMS research would be facilitated if the output of the recommended research projects, including interim deliverables, is expected to

[8] All of the challenges addressed previously in this report are focused on technical issues. This is the only nontechnical challenge.

improve system efficiencies and reduce operational costs as development of an IASMS proceeds, if interim benefits can be achieved with minimal investments by operators in new equipage, and if the cost of adoption is incorporated as a fundamental element in the development and implementation of an IASMS.

RESEARCH PROJECTS

In-time Mitigation Techniques

Research Project Summary Statement: For the high-priority risks that fall within the scope of the IASMS CONOPS, this research project would identify those for which adequate mitigation techniques do not exist and develop approaches and technologies necessary to implement timely mitigation.

Most risk mitigation techniques relevant to an IASMS that have been developed to date involve operators (primarily pilots and air traffic controllers) with some instrumentation support (e.g., collision avoidance systems). Much more is needed, however, to provide the sophisticated decision support systems needed by an IASMS. The research projects "IASMS Concept of Operations and National Airspace System Evolution" and "Identifying and Prioritizing Risks" in Chapter 2 identify those risks that will be included within the scope of an IASMS. For these risks, this research project will focus on enabling an IASMS to be aware of relevant airspace and ground operations, threat detection and assessment, and decision support systems. This research project will be difficult to complete because of the need for new instrumentation, advanced analytic methods, and sophisticated prediction capabilities that take into account the increasing complexities and uncertainties in the evolving NAS, particularly with respect to new entrants. This research project is urgent because the success of an IASMS is dependent on near- and long-term mitigation schemes to maintain the safety and efficiency of the NAS and because of the long time it will take to achieve project goals. Additional background information related to this research project appears in the discussion of the corresponding challenge earlier in this chapter.

The scope of this research project would encompass three areas of interest, as follows:

- Research on expanded awareness of airspace and ground operations would build on new system analytics methods for detecting and identifying known and emergent risks. This will require integrated studies of gate, ground, and air operations and how they interact to affect the overall state of the NAS. The study of environmental effects, such as air turbulence and weather, on air operations will also be critical factors for study. Data-driven methods, such as Bayesian analysis, may form the basis for reducing uncertainty, establishing root causes for observed risks, and then developing mitigation techniques to address the root causes.
- Research on integrated threat detection and assessment will develop prediction tools, simulation methods, and planning and scheduling tools that will form the basis for complex, distributed decision making to facilitate in-time risk mitigation.
- Research on decision support systems will address strategic decision making that an IASMS will need either to make recommendations to operators for corrective action or to initiate corrective action within the limits of its authority. The research will also consider the need for advances in operators' interactions with decision support systems. There are certain tasks that are clearly best handled by a human. Others are clearly best handled by an IASMS. Between these two extremes are tasks for which neither the human nor an IASMS is best suited. This research will address how a decision support system will determine for any particular situation whether a combination of the two or a selection of one or the other would be most beneficial.

This research will be of increasing importance as more and more tactical operations are automated with the evolution of the NAS. The goal of research in this area would be to provide tools that (1) provide performance precursors, (2) describe a causal chain of events to reduce temporal confusion, (3) improve situation awareness, and (4) monitor and reduce operators' stress.

Trust in IASMS Safety Assurance Actions

Research Project Summary Statement: Identify factors specific to human trust in IASMS safety assurance actions.

This research project would help achieve the vision for an IASMS because if operators do not trust the ability of an IASMS to recommend or take appropriate action, they will minimize the use of the system or ignore it entirely. Many factors, such as the frequency and complexity of operator interactions with an IASMS in various situations, will need to be understood and addressed in order to foster operator trust in the system. For example, operators may be particularly reluctant to trust an IASMS when the safety assurance actions recommended by the system are unfamiliar, unexpected, or run counter to operators' training and experience. One way to approach this challenge would be to implement the capabilities of an IASMS incrementally. This would make it easier for developers to ensure that each element of the operational system is trustworthy, and it would make it easier for operators to become familiar with and build trust in the system.

A better understanding of the factors that impact operator trust will also enable the proper balance of tasking between the operator and the IASMS so that the operator does not become overloaded. Change management processes will be critical when the system is deployed. The examination of the above factors, however, will need to begin at a much earlier stage than typical change management processes to assist in shaping the CONOPS, design, and implementation of an IASMS. Additional background information related to this research project appears in the discussion of the corresponding challenge "Trust in IASMS Safety Assurance Actions," earlier in this chapter.

An IASMS will rely on systems that are growing in functionality and decision-making capabilities. Change management processes will be critical at the point of deployment of the system. The examination of these factors will need to occur at a much earlier stage than typical change management processes to assist in shaping the CONOPS, design, and implementation of an IASMS.

Research on human trust in increasingly autonomous systems is under way to support other applications, such as advanced UAS. Even so, this research project will be difficult to complete because an IASMS will be so much more complex, for example, with regard to the very large number of variables that an IASMS will consider for each functional element of the IASMS CONOPS (i.e., monitoring, assessing, and mitigating). In addition, creating an IASMS that operators will trust and therefore use will require a thorough understanding of the potential capabilities, nuances, and emergent properties of an IASMS. The research project is urgent because operator trust is a relatively new field, and this research project therefore does not have a large body of work to use as a resource. In addition, this research project will be most effective if its results are available early in the IASMS development process.

This research project will identify stated, unstated, met, and unmet operator needs relevant to establishing trust in a highly complex system such as an IASMS. It will also identify metrics and methods to determine the level of operators' trust in and use of a complex system such as an IASMS, develop general principles that can be used in the design and development of IASMS, and identify evaluation metrics and methods to determine whether the IASMS adheres to those principles. The research project will involve scientists, operational personnel, unions, and the leadership of airlines, other operators, the FAA, and original equipment manufacturers.

System Verification, Validation, and Certification

Research Project Summary Statement: Develop practical methods for verifying, validating, and certifying an IASMS.

This research project would help achieve the vision for an IASMS because systems must be certified before they become operational. Although research in this area is already under way to support related applications such as certification of UTM and autonomous cars, existing research will not meet the unique needs of an IASMS because an IASMS will be much more complex than a highly automated/autonomous aircraft, and it will need to monitor and assess the operational safety of all existing and new entrants that will be operating in the NAS, encompassing the existing ATM systems as well as UTM systems.

This research project will be difficult to complete because development of certification standards for an IASMS will require a new approach to certification that promotes rapid and yet safe changes to the system, especially for an IASMS with adaptive/nondeterministic systems. Existing V&V procedures require months to years to complete, recertification is required if significant changes are made to configuration or core algorithms, and they do not apply to adaptive/nondeterministic systems, which will be incorporated in an advanced IASMS. This research is urgent because of the long time required to (1) create new VV&C processes that can be standardized and applied to other ATM systems (for example, via procedures established by RTCA and/or the European Organisation for Civil Aviation Equipment [EUROCAE][9]), or (2) develop an alternative approach to VV&C. Additional background information related to this research project appears in the discussion of the corresponding challenge earlier in this chapter.

An initial step in executing this research project could use emerging systems such as UTM as a prototype, since it is essentially a microcosm of the future ATM system. The benefit to focusing this research on emerging NAS systems couples with the urgency in that there are near-term needs in the marketplace for certifying these systems in an efficient manner to facilitate safe and low-cost operations. Without robust certification techniques, standards, and tool frameworks, it is unlikely that an IASMS will be readily incorporated in the NAS. Targeted tasks within this research project will include the following:

- Review agile test methods that can be applied to ATM test beds.
- Identify achievable and desirable target levels of safety for automated and agile test frameworks to validate.
- Identify alternatives to "code coverage" and "parametric analysis" (robustness testing) as described in DO-178C/DO-278C.
- Define the key criteria for which an IASMS should be tested. Development of a clear IASMS CONOPS (see Chapter 2) is a prerequisite for accomplishing this task.
- Develop advanced simulation capabilities that can accept comprehensive input test vectors and develop complex test scenarios.[10]
- Determine the most efficient VV&C test environment and whether the test system should use live data as well as simulated data as inputs.
- Develop updated methods and means for initial and ongoing quality assurance and configuration management relevant to a system with the complexity of an IASMS.
- Develop publications for standards development that can be adopted by operators and regulators.

[9] RTCA and EUROCAE are organizations in the United States and Europe, respectively, that support the development of aviation standards and regulations.

[10] A test vector typically involves a time-sequenced data set that is used to investigate the functionality of a system relative to a set of requirements and/or a CONOPS. Test vectors are intended to emulate an expected real-world scenario (either nominal or off-nominal) in order to explore system behavior.

6

Findings, Recommendations, and Organizational Roles and Resources

FINDINGS AND RECOMMENDATIONS

Recommendation. *In-time Aviation Safety Management*. The concept of real-time system-wide safety assurance should be approached in terms of an in-time aviation safety management system (IASMS) that continuously monitors the national airspace system, assesses the data that it has collected, and then either recommends or initiates safety assurance actions as necessary. Some elements of such a system would function in real time or close to real time, while other elements would search for risks by examining trends over a time frame of hours, days, or even longer.

Finding. *Challenges*. Successful development of an IASMS will require overcoming key technical and economic challenges:

- IASMS Concept of Operations and Risk Prioritization
  - — *IASMS Concept* of Operations. A clear concept of operations (CONOPS) for an IASMS is needed to define the scope of such a system and to understand how it would work.
  - — *Identifying and Prioritizing Risks*. Because the universe of all potential risks is large and each risk addressed adds some cost and complexity to the system, it will be important to have an approach and process to prioritize and focus on those risks that will have the most impact on system safety issues that fall within the scope of the IASMS.
  - — *National Airspace System Evolution*. The capabilities of an IASMS will need to increase in sophistication as the NAS continues to evolve and improve, while also accommodating changes in conventional air traffic and new entrants, particularly with regard to the following:
    - o Growth in air traffic,
    - o Increased uncertainty from new entrants (e.g., UAS, on-demand mobility aircraft, and commercial space launch and reentry operations) and emergent risks,
    - o Trust in increasingly autonomous UAS and associated traffic management systems,
    - o Unauthorized UAS operations, and
    - o Increasing pace of commercial space operations.

- System Monitoring
  - *Data Completeness and Quality*. Successful and efficient implementation of an IASMS requires identification, characterization, storage, and retrieval of the required data subject to availability, completeness, quality, and cost considerations.
  - *Data Fusion*. To accurately detect safety risks, an IASMS will need to correlate and synthesize data from heterogeneous data sources with different formats, timing, accuracy, and other characteristics.
  - *Collecting Data on the Performance of Operators*. Data regarding operator performance that are essential to achieving the full potential of the envisioned IASMS cannot be collected in a timely fashion or at all, in part because of privacy and related concerns.
- System Analytics
  - *In-time Algorithms*. Existing algorithms for identifying and predicting elevated risk states lack the ability to integrate the diversity of data sources of varying quality anticipated for an IASMS.
  - *Emergent Risks*. The complexity of the evolving NAS will result in anomalies with unknown root causes, making it hard to develop algorithms that analyze and predict the effects of emergent risks before accidents or incidents occur.
  - *Computational Architectures*. Existing computational architectures lack the ability to handle large volumes of heterogeneous data and dynamic analytics workflows, both of which are necessary to detect elevated risk states, to detect and characterize emergent risks, and to update the IASMS risk assessment algorithms.
- Mitigation and Implementation
  - *In-time Mitigation Techniques*. Existing mitigation techniques are limited in their ability to respond to many risks in the short time frame of interest to an IASMS.
  - *Unintended Consequences of IASMS Actions*. An IASMS could inject new risks into the NAS due to unintended consequences of actions that it recommends or initiates.
  - *Trust in IASMS Safety Assurance Actions*. The efficacy of an IASMS will be degraded if it is built without regard to the factors that influence operators' trust in the system.
  - *System Verification, Validation, and Certification*. There is no accepted approach to verification and validation that leads to certification of a software system as complex as an IASMS, particularly if, as expected, the system includes adaptive, nondeterministic algorithms.
  - *Operators' Costs and Benefits*. Operators' perception of the cost-to-benefit ratio of an IASMS may be so high that it will impede its implementation.

Recommendation. ***National Research Agenda.*** **Agencies and organizations in government, industry, and academia with an interest in developing an in-time aviation safety management system (IASMS) for the national airspace system (NAS) should execute a national research agenda focused on high-priority research projects in each of four areas, as follows:**

- **IASMS Concept of Operations and Risk Prioritization**
  - ***IASMS Concept of Operations and National Airspace System Evolution.*** **Develop a detailed concept of operations for an IASMS using a process that considers multiple possible system architectures, evaluates key trade-offs, and identifies system requirements.**
  - ***Identifying and Prioritizing Risks.*** **Develop processes to identify and prioritize risks that are relevant to an IASMS and that threaten the safety of the current and evolving NAS.**
- **System Monitoring**
  - ***Data Fusion, Completeness, and Quality.*** **Develop methods to automatically collect, fuse, store, and retrieve data from different sources and with different formats, timing, accuracy, and other characteristics.**
  - ***Protecting Personally Identifiable Information.*** **Develop methods of de-identifying and/or protecting sensitive data in a way that does not preclude effective data fusion.**

- **System Analytics**
  - — ***In-time Algorithms.*** **Develop robust and reliable algorithms that can assess large volumes of heterogeneous data of varying quality to simultaneously identify and predict elevated risk states of many different types and that are fast enough to meet in-time requirements.**
  - — ***Emergent Risks.*** **Develop approaches for continually mining historical data for detecting previously unknown anomalies and their evolution to characterize their emergent risks and to update the IASMS hazard detection algorithms.**
  - — ***Computational Architectures.*** **Support the design of data repositories and computational architectures that support online detection of elevated risk states and offline analysis to detect and characterize emergent risks and to update the IASMS risk assessment algorithms.**
- **Mitigation and Implementation**
  - — ***In-time Mitigation Techniques.*** **For the high-priority risks that fall within the scope of the IASMS CONOPS, identify those for which adequate mitigation techniques do not exist, and develop approaches and technologies necessary to implement timely mitigation.**
  - — ***Trust in IASMS Safety Assurance Actions.*** **Identify factors specific to human trust in IASMS safety assurance actions.**
  - — ***System Verification, Validation, and Certification.*** **Develop practical methods for verifying, validating, and certifying an IASMS.**

Finding. ***Highest Priority Research Project.*** **The research project on the IASMS Concept of Operations and National Airspace System Evolution is of the highest priority.**

Chapter 2 describes a generic IASMS CONOPS (see Figure 2.1). A much more detailed CONOPS is necessary to guide the development of IASMS. The IASMS CONOPS research project is critical primarily because it will establish the framework upon which all other IASMS research is conducted. In addition, it would identify the near-term potential of IASMS research to enhance the safety of the NAS and to engender stakeholder support for and trust in an IASMS. It would also facilitate updates to the CONOPS as the NAS evolves. Developing the CONOPS will be extremely complex and time consuming because of the many factors to be considered and the difficulty of assessing the trade-offs among them, which include the following:[1]

- System scope in terms of
  - — Aircraft types, including new entrants
  - — Data requirements
  - — Known and emergent risks
  - — Operations in different classes of airspace
  - — Time scales for each functional element (monitor, assess, and mitigate) of the generic CONOPS
  - — Users
- Ability to collect required data
- Architecture
- Costs and benefits
- Effectiveness
- Growth in air traffic
- Human performance limitations and human-machine roles
- NAS evolution
- System authority vis-à-vis human performance capabilities and limitations
- Technical capabilities
- Uncertainties associated with each functional element of the generic CONOPS
- Verification, validation, and certification

[1] System scope is listed first because it is the most important of the factors in the list. The other factors are listed alphabetically.

A key goal of this research project will be to understand the characteristics of an optimum IASMS and to thereby provide additional information for refining the list of key challenges and high-priority research projects. Many of the factors listed above are associated with other high-priority research projects identified in this report. Accordingly, the execution of this and many other research projects will likely proceed in an iterative fashion (1) as advances in one area support advances in other areas, (2) as more detailed information becomes available for various factors, and (3) as the ability to conduct complex trade-offs involving all of the factors matures.

ROLES AND RESOURCES

The allocation of organizational roles and resources associated with the development of an IASMS are similar in concept to the allocation of roles and resources described in the two prior reports in this series, each of which addresses the subject of one the six strategic thrusts established by NASA's Aeronautics Research Mission Directorate.[2] In particular, each of the recommended research projects would rely on academia, industry, and government agencies to play the same role that they normally play in the development of new technologies and products. Academia would generally participate in the projects at lower levels of technology readiness. Industry would focus on more advanced research and product development. Government agencies would support research and development—internally and/or through contracts with academia and industry—consistent with the mission objectives of the organization and the desired nature of a given organization's research portfolio in terms of risk, technical maturity, and economic potential. The FAA is leading the Next Generation Air Transportation System (NextGen) program, some elements of which pertain directly to the development of an IASMS.[3] The FAA has the expertise and facilities to serve as a test bed for technologies developed elsewhere, and it would be directly engaged in the development of certification standards and methodologies to enable the introduction of IASMS elements into the ATM system. In addition, some ATM equipment operated by the FAA may need to be modified. NASA would contribute primarily by supporting basic and applied research to support advanced development of systems by industry and the FAA. The Department of Defense (DoD) would monitor any changes to the ATM system that could impact the operation of military aircraft in civil airspace. In addition, each of the research projects could be addressed by partnerships involving multiple organizations in the federal government, industry, academia, and other international government agencies. For example, several European and Asian governments are developing data analysis programs similar to the FAA's Aviation Safety Information Analysis and Sharing (ASIAS) program (see Chapter 1). Both NASA and the FAA have existing cooperative research and development programs with their foreign counterparts. These could be expanded to share knowledge and the cost burden of new research and to maximize the benefit of unique capabilities by particular organizations.

In many cases, it would be beneficial to involve researchers with relevant expertise who might not have a history in addressing civil aviation issues. For example, state-of-the-art research and development related to algorithms for assessing complex data sets is not taking place in the context of civil aviation.

Executing all of the high-priority research projects described in this report would require significant resources. However, for many of the research projects substantial advances could be achieved using currently available resources, especially if those resources are aligned in accordance with the recommended high-priority research projects and if program planning and execution take maximum advantage of the synergies that exist among some of the research projects.

[2] National Research Council, 2014, *Autonomy Research for Civil Aviation: Toward a New Era of Flight*, The National Academies Press, Washington, D.C., and National Academies of Sciences, Engineering, and Medicine, 2016, *Commercial Aircraft Propulsion and Energy Systems Research: Reducing Global Carbon Emissions*, The National Academies Press, Washington, D.C.

[3] The Next Generation Air Transportation System (NextGen) Airborne Collision Avoidance System X (ACAS X) system would replace and improve the capabilities of the Traffic Collision Avoidance System (TCAS). Elements of the ACAS X system would accommodate the special needs of unmanned aircraft systems (UAS) and low-performance general aviation aircraft that lack collision avoidance systems.

Appendixes

A

Statement of Task

The National Academies of Sciences, Engineering, and Medicine will convene an ad hoc committee to create a national research agenda for the development of the suite of tools needed to support a prototype integrated safety monitoring and assurance system that detects, predicts, and prevents safety problems in the national airspace system (NAS) in real time, particularly with regard to the safety of commercial transports. The recommended research agenda will consist of a set of research projects, grouped by priority, to achieve this goal. In particular the committee will

1. Review the following:
   a. Current processes for providing real-time system-wide safety assurance for the NAS.
   b. Current goals and plans by government, industry, and academia regarding the advancement of tools, technologies, and processes that specifically address real-time system-wide safety assurance for the NAS, including ongoing research by NASA's Aeronautics Research Mission Directorate and that portion of the NASA Technology Roadmap for Aeronautics that specifically addresses system-wide safety assurance.
   c. Expectations regarding advances of broadly applicable technology that could be used to advance real-time system-wide safety assurance capabilities. Areas of interest include sensing, computing, communications, and analytics, as well as safety assurance technologies and capabilities for nonaviation applications.
   d. NASA's vision for advances in system-wide safety assurance over the near term, midterm, and far term.
2. Outline a national research agenda that will demonstrate the feasibility of real-time system-wide safety assurance of the NAS, as follows:
   a. Comment on NASA's vision for development of real-time system-wide safety assurance capabilities.
   b. Identify technical, economic, regulatory, and policy barriers to developing and demonstrating advanced technologies and capabilities to achieve the vision.
   c. Recommend a research agenda consisting of a set of recommended research projects, grouped by priority, to overcome the barriers and achieve the vision for real-time system-wide safety assurance. The agenda should be developed with due consideration of the resources and organizational partnerships required to complete the projects included in the agenda. The research agenda should, as appropriate, describe the potential contributions and roles of U.S. research organizations, including NASA, other federal agencies, industry, and academia.

B

Committee Member Biographies

KENNETH J. HYLANDER, *Chair*, is the past chairman of the Board of Governors at the Flight Safety Foundation (FSF), whose core mission is that of a leading independent, impartial, and international enabler of continuous aviation safety improvement. He is also a member of the board of directors of Monroe Energy, a medium-size oil refinery in Trainer, Pennsylvania, and a member of the Federal Aviation Administration (FAA) Research, Engineering, and Development Advisory Committee. His professional expertise lies mainly in the areas of airline engineering, safety, security, quality assurance, and operations. Previously, Mr. Hylander has served in executive positions with Delta Air Lines, Northwest Airlines, and United Airlines, where his responsibilities focused on the preceding areas. His awards include the FSF Presidential Citation, which was awarded for his efforts to ensure that a strong FSF will be able to continue its lifesaving work, and the William Littlewood Memorial Lecture, which was awarded by the Society of Automotive Engineers, Aerospace Division, in recognition of his contributions to aviation safety and engineering. He is also the winner of the Airlines 4 America (A4A) Nuts and Bolts Award in recognition for leadership in airline technical disciplines. He holds an M.B.A. from the University of California, East Bay, and a B.S.M.E. from the University of Rhode Island.

BRIAN M. ARGROW is professor of Aerospace Engineering Sciences, director of the Integrated Remote and In Situ Sensing Program, and director emeritus of the Research and Engineering Center for Unmanned Vehicles at the University of Colorado, Boulder (CU). Dr. Argrow has served as associate dean for education and is a CU president's teaching scholar. His research topics include small unmanned aircraft system design and airspace integration, dense and rarefied gas dynamics, sonic boom, and engineering education, with more than 100 research publications. He is a fellow of the Center for STEM Learning and a recipient of the W.M. Keck Foundation Award for Excellence in Engineering Education. Dr. Argrow co-chaired the first Symposium for Civilian Applications of Unmanned Aircraft Systems (CAUAS) and chaired the Association for Unmanned Vehicle Systems International (AUVSI)/American Institute of Aeronautics and Astronautics (AIAA) 2nd Workshop on Civilian Applications of Unmanned Aircraft Systems (CAUAS-2), the first major AIAA and AUVSI joint event. He is a fellow of the AIAA and is chair emeritus of the AIAA Unmanned Systems Program Committee. He served on the NASA Advisory Council's unmanned aircraft systems (UAS) subcommittee and several other NASA and NOAA advisory boards and committees. Dr. Argrow currently serves on the ASTM F38 Subcommittee for "Specifications for UAS Operations over People." Dr. Argrow is an alumnus of the DARPA/IDA Defense Science Study Group, and he received the Air Force Exemplary Civilian Service Award for his service on the Air Force Scientific Advisory Board. He

has a Ph.D. in aerospace engineering from the University of Oklahoma. He is a member of the Aeronautics and Space Engineering Board (ASEB) of the of the National Academies of Sciences, Engineering, and Medicine.

MEYER J. BENZAKEIN is the Wright Brothers Institute Professor in the Aerospace Engineering Department at the Ohio State University, where he is also the assistant vice president for Aerospace and Aviation in the Office of Research. Previous positions at Ohio State University include director of the Propulsion and Power Center and chair of the Aerospace Engineering Department. He entered academia after retiring from General Electric Aircraft Engines, where for 10 years he was responsible for research, design, technology development, and certification of new products. He led the research in computational aerodynamics, aeroacoustics, aeromechanics, and combustion. His research interests include analytical tools for improved quality and throughput for turbine engines, reduction of aircraft engine noise and emission, and management of technology programs. He is a member of the National Academy of Engineering (NAE), a fellow of the AIAA, and a fellow of the Royal Aeronautical Society. His awards include the Gold Medal of Honor from the Royal Aeronautical Society and the AIAA Reed Aeronautics Award. He has served on many industry and government advisory panels and received an honorary doctorate from the University of Poitiers, France, in 2006. He holds a Ph.D. in engineering mechanics from Wayne State University. He is a member of the ASEB, and he has served on many National Academies study committees, including the Committee on Propulsion and Energy Systems to Reduce Commercial Aviation Carbon Emissions, the Committee on Examination of the U.S. Air Force's Aircraft Sustainment Needs in the Future and Its Strategy to Meet Those Needs, and the Panel on Air and Ground Vehicle Technology.

GAUTAM BISWAS is the Cornelius Vanderbilt Professor of Engineering and a professor of computer science, computer engineering, and engineering management in the Electrical Engineering and Computer Science Department at Vanderbilt University. He is also a senior research scientist at the Institute for Software Integrated Systems at Vanderbilt University. He conducts research in intelligent systems with primary interests in hybrid modeling, simulation, and analysis of complex embedded systems, and their applications to diagnosis, prognosis, and fault-adaptive control. As part of this research, he has worked on fault diagnosis and fault-adaptive control for aircraft fuel transfer systems. He has also initiated new projects in health management of complex systems, which includes online algorithms for distributed monitoring, diagnosis, and systems-level prognosis. More recently, he has been working on data mining for diagnosis, and developing methods that combine model-based and data-driven approaches for anomaly detection and diagnostic and prognostic reasoning. For this work, in conjunction with researchers at Honeywell Laboratories, he received a NASA ARMD Technology and Innovation Group Award for vehicle-level reasoning system and data mining methods to improve aircraft diagnostic and prognostic systems. Dr. Biswas is currently leading a safety analytics project related to vehicular accidents and emergency response. He holds a Ph.D. in computer science from Michigan State University.

JOHN W. BORGHESE is vice president of Rockwell Collins Advanced Technology Center, where he has led the development of high-assurance systems for both safety-critical avionics systems and security-critical communication systems. Under his direction, the center develops innovative technology solutions that include avionics, communications, navigation, electronic warfare, safety systems research, and approaches to protect manned aircraft and UAS against cyber threats. Previously, Mr. Borghese served as vice president and general manager of Kaiser Aerospace and Electronics, a Rockwell Collins company, and as director of automatic test systems and avionics systems business at Allied-Signal (Honeywell). Throughout his career, he has held positions in general management, program management, business development, and engineering. Mr. Borghese is vice chair of the Aeronautics Committee of the NASA Advisory Council, and he is a private pilot. He earned a B.S. in electrical engineering from the University of Southern California and an M.B.A. from Boston University.

STEVEN J. BROWN is the chief operating officer for the National Business Aviation Association, where he oversees all of the association's activities relating to aircraft operations and flight department management issues, as well as the administrative, financial, and human resources functions. Previously, Mr. Brown served with the FAA as vice president of operations planning. He also served as associate administrator for air traffic services,

managing the 35,000 air traffic controllers, maintenance and software technicians, flight inspection pilots, and administrative personnel who are responsible for the day-to-day operation of the nation's airspace systems. He served as president of the National Aeronautic Association and as senior vice president of government and technical affairs at the Aircraft Owners and Pilots Association. His areas of expertise include aircraft operations, safety, and air traffic control. He holds an M.S. in industrial education from Texas A&M University, and he is a qualified accident investigator certified by the University of Southern California.

DANIEL K. ELWELL is the acting administrator of the FAA, where he is responsible for the safety, efficiency, and modernization of the air traffic control system. Formerly, he was the president of Elwell & Associates, LLC, an aviation consulting firm. He has also served as the senior vice president for safety, security, and operations at A4A, where he was responsible for leading the U.S. airline industry's efforts to advance safety and security while improving operational efficiency. Before joining A4A, Mr. Elwell was vice president of civil aviation at the Aerospace Industries Association; assistant administrator for policy, planning, and environment at the FAA; and a longtime U.S. Air Force and commercial airline pilot with over 6,000 hours of flight time in more than 10 different aircraft types. His areas of expertise include many aspects of commercial and general aviation operations and safety, including regulatory challenges, policy challenges, and the technological enhancements to surveillance and navigation systems that are currently in use or will be in the next 10 to 20 years. He has numerous Air Force commendations and citations with worldwide operational experience, including service in Operation Desert Storm. Mr. Elwell earned his pilot wings at Williams Air Force Base in Arizona after graduating from the U.S. Air Force Academy with a B.S. in international affairs. He has been a member of the National Academies Committee on Propulsion and Energy Systems to Reduce Commercial Aviation Carbon Emissions and the Aeronautics Research and Technology Roundtable.

ANTHONY F. FAZIO is president of Fazio Group International, an aviation safety and regulatory information consulting firm. The firm is affiliated with the U.S. Crest Group; the Groupement des Industries Françaises Aéronautiques et Spatiales, which is the French Aeronautics and Space Industries Association; and TSI Aviation Solutions. He also serves as an individual expert to the European Aviation Safety Agency for their Data 4 Safety data analysis and sharing program. Previously, Mr. Fazio served with the FAA in policy, regulatory, and international positions, including executive positions as director of rulemaking; director of the Africa, Europe, and Middle East office in Brussels; and director of accident investigation and prevention. In this last position he had program responsibility for the FAA's Aviation Safety Information Analysis and Sharing (ASIAS) program and the Commercial Aviation Safety Team (CAST). In his capacity as the government co-chair of the General Aviation-Joint Steering Committee, he expanded ASIAS's participation to the general aviation community. Mr. Fazio served as the designated federal official to the Safety Subcommittee of the Department of Transportation Future of Aviation Advisory Committee, and he was the FAA representative to the International Civil Aviation Organization (ICAO) Special Task Force on Safety Information Protection and Global Safety Information Exchange. His expertise includes domestic and international aviation safety and regulations. He has received the FAA Aviation Safety Organization Champion of Safety award. He holds an M.P.A. in public policy from the University of Maryland, College Park.

MICHAEL GARCIA is the director of systems engineering at Aireon, LLC. Dr. Garcia has overall responsibility for the technical specification, design, implementation, and performance of the Aireon space-based Automatic Dependent Surveillance-Broadcast (ADS-B) surveillance system. His responsibilities also include the oversight, coordination, and communication of technical and development activities with air navigation service providers, standards groups, subcontractors, and investors. Dr. Garcia has also contributed key technical analysis and presentations in support of the decision by the United Nations International Telecommunications Union to add a safety allocation in the radio regulations for reception of ADS-B data from Earth to space. Prior to joining Aireon, Dr. Garcia served as an associate principal engineer at Exelis while working on the FAA's ADS-B and Wide Area Multilateration programs. Several of his innovations have resulted in patents and publications of interest to the air traffic management industry. Dr. Garcia received his Ph.D. in electrical engineering from Duke University.

R. JOHN HANSMAN, JR., is the T. Wilson Professor of Aeronautics and Astronautics at the Massachusetts Institute of Technology (MIT), where he is also the director of the MIT International Center for Air Transportation. Dr. Hansman holds seven patents and has authored more than 250 technical publications. He has more than 5,800 hours of pilot in command time in airplanes, helicopters, and sailplanes, including meteorological, production, and engineering flight test experience. Dr. Hansman chairs the FAA Research, Engineering, and Development Advisory Committee as well as other national and international advisory committees. He is co-director of the Aviation Sustainability Center, which is a multi-university FAA Center of Excellence. He conducts research in the application of information technology in operational aerospace systems. He is a member of the NAE and a fellow of the AIAA. He has received numerous awards, including the AIAA Dryden Lectureship in Aeronautics Research, the Air Traffic Control Association's Kriske Air Traffic Award, and the FAA Excellence in Aviation Award. He earned his Ph.D. in physics, aeronautics, and meteorology from MIT. He has served on many National Academies committees, most recently the Committee of the Federal Aviation Administration Research Plan on Certification of New Technologies into the National Airspace System and the Committee on Review of the Enterprise Architecture, Software Development Approach, and Safety and Human Factor Design of the Next Generation Air Transportation System.

GERARDO D.M. HUETO is assistant director of safety and flight operations at the International Air Transport Association (IATA) Asia Pacific Office in Singapore. He leads the development and implementation of regional safety enhancement initiatives for air carriers, nations, and service providers in the region, leveraging information from the Flight Data Exchange program and ASIAS to focus on top regional risks. He also leads the effort to proactively identify emerging or future safety risks and evaluate possible risk management initiatives. Mr. Hueto is the industry co-chair of the ICAO Asia Pacific Regional Aviation Safety Team (APRAST). Prior to joining IATA he was chief engineer, aviation system safety at Boeing Commercial Airplanes. He coordinated Boeing's Aviation Safety initiatives with regulators and industry in the United States and worldwide. Mr. Hueto represented Boeing at the U.S. CAST and the steering committees of ICAO's regional safety initiatives in Asia and the Americas. He has served as industry co-chair for the Joint Implementation Measuring and Data Analysis Team for the U.S. FAA CAST; Aviation Team Looking Ahead at Safety for the U.S. FAA CAST; the ICAO Regional Aviation Safety Group-Pan America; and the ICAO Safety Reporting Group for APRAST. His areas of expertise include commercial aircraft manufacturing, airline operations, and safety. He is a recipient of the McDonnell Douglas Spirit of Excellence Award for the development of new nondestructive inspection technology. Mr. Hueto holds an M.S. in engineering management from the West Coast University and an M.S. in aeronautical engineering from the Universidad Nacional de La Plata, Buenos Aires, Argentina.

LAUREN J. KESSLER is a distinguished member of the technical staff at the Charles Stark Draper Laboratory, Cambridge, Massachusetts, where she has been the leader of the Intelligent Automated Systems and the Resilience and Fault Tolerance groups. She is currently co-leading the fault-tolerant flight computer software development for the DreamChaser unmanned shuttle. She has led efforts in automated hydrocarbon extraction rigs, Lunar Surface Systems multilevel autonomy software architectures, and Autonomous Precision Lunar Landing mission management, as well as the verification for the Orbital Express autonomous rendezvous and servicing satellite demonstration system. She was a key contributor to the unmanned underwater vehicle efforts, focused on the human operator engagement with the autonomous vehicles. Previously, Ms. Kessler was a lead engineer at Northstar and Avidyne for the development and certification of a general aviation next-generation Air Data/Attitude/Heading Reference System and a precision approach navigation device for the GPS-Wide Area Augmentation System. Her areas of expertise are centered on researching, architecting, and implementing human-in-the-loop and mission-critical systems, including war-gaming simulations, human-embedded autonomous systems, avionics, and human decision aides. Ms. Kessler was named a 2013 Woman-to-Watch in technology by Mass High Tech (*Boston Business Journal*), and she was a recipient of the AIAA Software Engineer of the Year award, along with NASA certificates of achievement. She is an AIAA associate fellow, a commercially rated helicopter pilot, and an advanced aviation ground instructor, and she serves in the Civil Air Patrol. She holds an M.S. in computer science from Boston University.

JOHN C. KNIGHT passed away during the course of the study. He was a professor emeritus of computer science at the University of Virginia. Prior to joining the University of Virginia, he was with NASA's Langley Research Center. His research interests included system safety, especially for aviation systems utilizing significant digital technology; mathematical proofs of software correctness; assurance using rigorous safety and security arguments; enhancing the security of binary programs through artificial diversity; and proofs of security properties of binary programs. Dr. Knight was the general chair of the 2000 International Symposium on the Foundations of Software Engineering (FSE 2000), the general chair of the 2007 International Conference on Software Engineering (ICSE 2007), and editor in chief of *IEEE Transactions on Software Engineering* from January 2002 to December 2005. Dr. Knight was the recipient of the 2006 IEEE Computer Society's Harlan D. Mills award and the recipient of the 2008 ACM Special Interest Group on Software Engineering's Distinguished Service award. Dr. Knight held a B.Sc. (Honors) in mathematics from Imperial College, London, and a Ph.D. in computer science from the University of Newcastle upon Tyne. Dr. Knight served as a member of the National Academies Committee on Trust in Cyberspace and the Committee on Review of the Enterprise Architecture, Software Development Approach, and Safety and Human Factor Design of the Next Generation Air Transportation System.

MICHAEL J. McCORMICK is an assistant professor of air traffic management at Embry-Riddle Aeronautical University. Previously, he retired as vice president of management services in the FAA's Air Traffic Organization. His portfolio included labor, contracts, fiscal budget, business services, communications, strategic planning, organizational effectiveness, administrative services, talent and resource policy, employee development, and diversity. He has also served as the FAA's executive director responsible for day-to-day operations of tower and approach control services. He was the FAA's director of safety and operations support, responsible for standardization, safety, and compliance of air traffic control procedures and operations in 292 FAA airport traffic control towers and approach controls centers and 245 contract towers. Mr. McCormick performed as the transportation attaché at the U.S. Embassy in Iraq. In this role Mr. McCormick advised and assisted with strategic planning and program synchronization of transportation systems to improve local services and ensure the flow of passengers and goods. He led subject matter experts who provided Iraqi government organizations with technical assistance and consultation in the rebuilding of infrastructure of aviation, rail, maritime ports, and roads and bridges. He was the first civilian air traffic controller at Baghdad International Airport, he has provided air traffic control services at Philadelphia International Airport, and he has managed the New York and Washington Air Route Traffic Control Center. He served as the Aviation Emergency Support Function Leader for the Federal Emergency Management Agency during incidents of national significance. He also served as the Department of Transportation representative to the U.S. National Search and Rescue Committee responsible for land, air, and maritime policy and procedures. His expertise includes air traffic control both as a controller and as a senior executive. Mr. McCormick has received the U.S. Secretary of Transportation Gold Medal; the U.S. Secretary of Transportation 9-11 Medal for his actions on September 11, 2001; the U.S. Department of Transportation War on Terrorism Medal; and the U.S. Ambassador Certificate of Merit for his service in Iraq. He holds a B.S. in aviation management from Southern Illinois University and an M.B.A. from West Chester University.

BONNIE SCHWARTZ is the UAS Airspace Integration Portfolio manager at the Air Force Research Laboratory (AFRL), Aerospace Systems Directorate, Power and Control Division. At AFRL, Ms. Schwartz leads multidisciplinary technology development efforts in UAS sense and avoid, terminal airspace operations, and surface operations, and she is the program manager of AFRL's vehicle-agnostic sense and avoid effort, which is conducting flight tests on board a surrogate UAS. Her areas of expertise include real-time information fusion and decision making for safe and efficient operation of UAS in the same airspaces and airbases as piloted aircraft and UAS surface operations, including autonomous taxi, air traffic control communication, navigation, and collision avoidance. She earned her M.S. in computer engineering from Wright State University, Dayton, Ohio.

CRAIG WANKE is a senior principal engineer at The MITRE Corporation's Center for Advanced Aviation System Development. He is also the innovation area lead for aviation and transportation research, responsible for selecting and directing MITRE's internal research and development program in aviation and transportation. During his

23 years at MITRE, Dr. Wanke has worked on a wide range of decision support capabilities for pilots, air traffic controllers, and, especially, traffic flow managers in the NAS. Several tools developed under this work were eventually acquired by the FAA and deployed to the NAS. Dr. Wanke's research interests include probabilistic decision making, optimization, traffic flow management, visualization of complex traffic flows, weather forecasting for traffic flow decision making, integration of unmanned vehicles into the NAS, building effective human-machine teams, and Agile system engineering and acquisition. He is an associate fellow of the AIAA. He has served as a member of the AIAA Guidance, Navigation, and Control Technical Committee, and he is currently an associate editor of the *AIAA Journal of Air Transportation*. Dr. Wanke earned his Ph.D. in aeronautical engineering from MIT.

C

Acronyms

ACARS	Aircraft Communications Addressing and Reporting System
ADS-B	Automatic Dependent Surveillance-Broadcast
AFRL	Air Force Research Laboratory
ARMD	Aeronautics Research Mission Directorate
ASAP	Aviation Safety Action Program
ASEB	Aeronautics and Space Engineering Board
ASIAS	Aviation Safety Information Analysis and Sharing
ATM	air traffic management
CAST	Commercial Aviation Safety Team
CONOPS	concept of operations
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FOQA	Flight Operations Quality Assurance
IASMS	In-time Aviation Safety Management System(s)
ICAO	International Civil Aviation Organization
NAS	national airspace system
NASA	National Aeronautics and Space Administration
NextGen	Next Generation Air Transportation System
ODM	on-demand mobility

RSSA	real-time system-wide safety assurance
SMART-NAS	Shadow Mode Assessment Using Realistic Technologies for the National Airspace System
SMS	safety management system(s)
SWIM	System-Wide Information Management
TCAS	Traffic Collision Avoidance System
UAS	unmanned aircraft system(s)
UTM	UAS traffic management
V&V	verification and validation
VV&C	verification, validation, and certification